CYBER ENDEAVOUR 2014

JUNE 24 – 26, 2014

"When the Lights Go Out"

FINAL REPORT

FOREWORD

The Cyber Endeavour 2014 Final Report is provided on behalf of the Department of Defense Information Operations Center for Research (DoD IOCfR), located at the Naval Postgraduate School, and the Army Reserve Cyber Operations Group (ARCOG), the co-sponsors of this event. This report synthesizes materials from our co-sponsors, panel members, and distinguished and special guest presenters. This report also includes open-forum discussions and comments offered by participants, on a non-attribution basis, increasing the richness and relevance of this report.

Cyber Endeavour 2014 was attended by an estimated 230 participants, panel members, and guest speakers. It provided an interactive, working level environment for leaders and operators to collectively discuss some of the more critical Cyber challenges and problems facing our nation and armed services and to identify potential solutions. Our theme for this year's event was **"When the Lights Go Out,"** with a focus on identifying the current status of our nation's cyber resiliency in order to further explore the Department of Defense's and its partner's roles in securing critical infrastructure-smart grid.

Cyber Endeavour 2014 also provided an operational environment for exercising offensive and defensive cyber techniques and practices during the Cyber X-Games which consisted of individual and team cyber-attack and cyber-defend competitions.

We would like to express their sincerest thanks to our keynote speaker, distinguished and special guest speakers, moderators, and panel members, participants, and volunteers who collectively helped make Cyber Endeavour 2014 and Cyber X-Games huge success. Our particular thanks and appreciation go out to the following corporate sponsors for their generosity and support.

- Mehta Tech, Inc (Platinum Sponsor)
- IBM (Platinum Sponsor)
- SynerScope (Platinum Sponsor)
- Endgame, Inc (Gold Sponsor)

This report will hopefully serve as an important reference document for you and your parent organizations, and to encourage you to continue the dialogue on "When the Lights Go Out."

Thank you, and hope to see everyone at Cyber Endeavour 2015!

TABLE OF CONTENTS

Foreword 2

Table of Contents 3

Section 1 – Cyber Endeavour 2014

June 24, 2014

Keynote Speaker 5

Office of the Undersecretary of Defense for Policy – Major General John Davis

Guest Speaker – Civilian Threat Briefing 9

Dr. John Weiss, Applied Control Solutions, LLC

Guest Speaker – Australian Cyber Policies and Rules of Engagement 11

GPCAPT Paul Wade, Defence Cyber Coordination Office, Australia

Panel 1 – Allied and Partner Nation Cyber Policies and Rules of Engagement 13

Dr. Steve Chan, MIT/IBM NSRC/Sensemaking PACOM Fellowship (Moderator)

Mr. Bob Griffin, IBM i2, IBM NSRC (Panel Member)

Mr. Ed Bryan, United Kingdom, IBM i2 (Panel Member)

Mr. Jan-Kees Buenen, Amsterdam, SynerScope (Panel Member)

Mr. Jim Hackett, Canada, Mehta Tech (Panel Member)

Guest Speaker – Pacific Command Scenario 17

Dr. Richard Berry, U.S. Pacific Command

Guest Speaker – National Intelligence Briefing (Cyber) 20

Mr. Sean Kanuck, Office of the Director of National Intelligence

Guest Speaker – DOE Cyber Security for Energy Delivery Systems R&D Initiatives 23

Dr. Carol Hawk, Department of Energy

June 25, 2014

Panel 2 – U.S. Roles, Responsibilities, and Capabilities (Government and Department of Defense) 26

Mr. Robert Spousta, Sensemaking/U.S. Pacific Command Doctoral Fellow (Moderator)

Mr. Randall Cieslak, SES, U.S. Pacific Command (Panel Member)

Col William Hutchinson, U.S. Cyber Command (Panel Member)

Mr. Ross Roley, U.S. Pacific Command (Panel Member)

Mr. Jeff Johnson, Naval District Washington (Panel Member)

Panel 3 – Cyber Intelligence 33

LTC Michael Smith, National Capital Region IO Center (Moderator)

Dr. Ernest Hampson, Battelle Memorial Institute (Panel Member)

COL Drew Ryan, Military Intelligence Readiness Command (Panel Member)

Mr. Elijah Owen, California Governor's Office of Emergency Services (STAC) (Panel Member)

Mr. Douglas Raymond, Endgame Inc (Panel Member)

Distinguished Guest Speaker – Cyber Analogies 37

Dr. John Arquilla, Department of Defense Analysis, Naval Postgraduate School

Panel 4 – U.S. Roles, Responsibilities, and Capabilities (Reserve Component and National Guard) 40

LTC Michael Smith, National Capital Region IO Center (Moderator)

MG Darryll Wong, Hawaii Adjutant General (Panel Member)

BG Gabriel Troiano, Commanding General, Military Intelligence Readiness Command (Panel Member)

Col William Hutchinson, U.S. Air Force Reserves (Panel Member)

Col Mark DiTrolio, Army Reserve Cyber Operations Group (Panel Member)
LTC Kelly Greenhaw, Joint Force Headquarters of California (Member)
Panel 5 – Training and Educating the Force 46
COL Michael Hildreth, Army National Guard (Moderator/Panel Member)
Dr. Cynthia Irvine, Center for Information Systems Security Studies and Research, NPS (Panel Member)
SFC Thomas Blackard, Army Reserve Cyber Operations Group (Panel Member)
COL Heather Meeds, National Guard Bureau (Panel Member)

June 26, 2014

Guest Speaker – Georgia/Ukraine Discussion – Analyzing Bear Behavior in the Wild 52
Mr. John Bumgarner, U.S. Cyber Consequences Unit
Guest Speaker – DHS Roles, Responsibilities, and Capabilities 54
Mr. Antonio "T" Scurlock, U.S. Department of Homeland Security (DHS) S&P/NPPD
Panel 6 – Ethics and Policies 56
Dr. Bradley Strawser, Department of Defense Analysis, NPS (Moderator/Panel Member)
Mr. Javier Santoyo, Symantec (Panel Member)
Dr. Dorothy Denning, Department of Defense Analysis, NPS (Panel Member)
Panel 7 – Public Private Partnerships 62
Ms. Alison Kuzmickas, Sensemaking/U.S. Pacific Command (Moderator)
Dr. Richard Berry, U.S. Pacific Command (Panel Member)
Dr. Steve Chan, MTI/IBM NSRC/Sensemaking PACOM Fellowship (Panel Member)
COL Margaret Roosma, Office of the Chief Army Reserve (Panel Member)
Mr. Bob Griffin, IBM i2 Group/IBM NSRC (Panel Member)
Dr. Kathleen Kiernan, KGH/Infragard/NPS (Panel Member)
Panel 8 – Smart Grid 71
Dr. Steve Chan, MTI/IBM NSRC/Sensemaking PACOM Fellowship (Moderator)
Mr. Randy Baldemor, State of Hawaii (Panel Member)
Mr. Michael Champly, State of Hawaii Public Utilities Commission (Panel Member)
Ms. Shari Ishikawa, Hawaiian Electric Companies (HECO) (Panel Member)
Mr. Jeffrey Katz, IBM (Panel Member)
Mr. Wesley Rhodes, IBM (Panel Member)
Mr. Jim Hackett, EVP, Mehta Tech (Panel Member)

Section 2 – Cyber X-Games

Cyber X-Games Overview 79
Cyber X-Games Results 80
Cyber X-Games Team Assessment (CMU/SEI) 82

Section 3 – Cyber Endeavour 2014 / Cyber X-Games Sponsors

Platinum Sponsors (Mehta Tech / IBM / SynerScope) 85
Gold Sponsor (Endgame) 86

KEYNOTE SPEAKER

Major General John Davis, Senior Military Advisor for Cyber to the Undersecretary of Defense for Policy

Major General John Davis welcomed Cyber Endeavour 2014 participants, then opened the conference with an overview of the major trends, drivers and dynamics within the Office Undersecretary of Defense for Policy that are shaping the way we think about policies, authorities and resources. Highlights of his presentation include:

Driver 1 – Teamwork and Partnerships

Cyber is a team sport. There are many organizations in the public and private sector that have very important roles and responsibilities, and no single organization has the resources, authorities, and capacity it needs to be successful in an environment of a very serious and growing threat. There are four different types of teams:

- Internal to the Department of Defense (DoD)
- Interagency (Cross Government)
- Public Private Sector
- Partner Nations

This is an environment of the collective, where it is necessary to establish and cultivate a broad range of relationships with internal partners within a complex environment. It is also an environment where there is no single organization in charge, and where it is important to identify who is involved and how they work together. The need to define these partnerships and relationships that led the Government and U.S. Federal Cybersecurity Operations Team to define their national roles and relationships as highlighted in Figure 1, which is commonly referred to as the "Bubble Chart." There were seventy-five (75) versions made of this chart before all parties agreed on how this works, and it was powerful and important just to get an agreement. There was also a realization by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Department of Defense (DoD) that they cannot be successful without this partnership. Of importance to the DoD were the discussions and relationship building that occurred and recognition that they had a role to defend the nation in all domains, including cyberspace, to include Presidential policy directed roles in defending the nation from a strategic cyber attack.

The DoD, and U.S. Cyber Command (USCYBERCOM) in particular, has a responsibility to operate and defend DoD networks. However they have to rely on things beyond DoD networks that include industry and other country networks and systems that they have a responsibility to secure and that are becoming increasingly vulnerable to a growing threat. This leads to DoD partnerships with other interagency partners in order to improve cyber security standards of critical infrastructure and Defense Industrial Base.

The DoD also needs to identity new ways to work with its international partners to help these countries get better at critical infrastructure protection and cyber security so they can live up to their alliance and military

contingency response options. Taking a "whole of government approach," the DoD helped key partners in the Gulf and Asia-Pacific region identity those critical infrastructure and key resources of common interest, helped these countries determine who is in charge of what in their government, encouraged them to treat cyberspace as an operational domain from a military perspective, helped them establish strategy and plans and authorities to hold right entities accountable, and provided other support under "Building Partner Capacity."

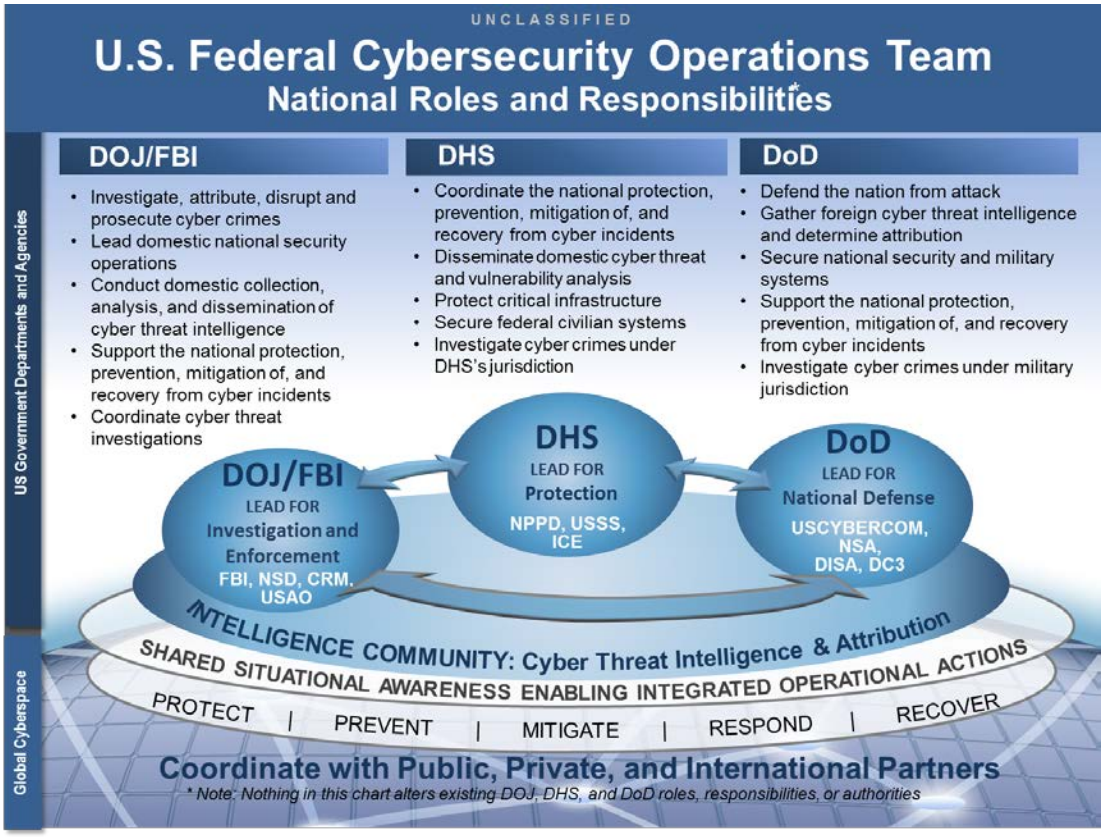

Figure 1 – Bubble Chart

One of the implications for the Services is the fact that "Cyber is born Joint," probably more than any other experience, with unique applications of Cyber at the tactical level. Training qualification certifications are where joint standards become critically important as these forces operate in a very complex, shared environment, which has implications on the "man, equip, and train roles" of the Services.

Driver 2 – Balance Between Opportunity and Risk

Our increasing reliance on Information Technology (IT) is shifting the scales in cyber security, and the DoD and Intelligence Community (IC) are ringing the alarm bell on the risk button. This is serious, this is real, and this has significant consequences associated with it. While a major cyber attack has not happened yet in the U.S., it is but a matter of time before it does happen. The role of government has been to try to get a balance between opportunity and risk, and industry and our international partners are beginning to understand. It also has obligations for ensuring an open, secure, and reliable cyber environment.

Important factors that go into the "Opportunity Bucket" include reflecting good American values, freedom of expression, personal privacy, innovation, and economic development. The U.S. also has to live up to its international obligations as a global leader in basically preserving the above, and also trying to preserve a

multi-stakeholder approach with Internet governance. Cyberspace is a multi-stakeholder, international industry, and the government is only one of many players, and actually one of the smaller players.
The government needs to continue asserting norms of responsible behavior, as there is increasingly reckless behavior materializing around the world that is worrisome. In international forums, it is argued that cyber is no different within the context of the law of international human rights, and most countries are coming to this realization, with the exception of a few nations such as Russia.

As for risks, there is no doubt the bucket is filling up and causing the scales to move. What was once an environment of mostly hackers, political agenda mischief, hactivism, criminals, identity theft, fraud, and even legitimate espionage, has now been shifted to highly disruptive and destructive types of events, such as the cyber attack on computer networks of Saudi Aramco with a self-replicating virus, or North Korea military cyber attacks involving military developed malware targeting banks and media companies.

What is worrisome and what is at risk is not just U.S. critical infrastructure and key resources. It is also global critical infrastructure and key resources to the proliferation of cyber weapons and associated implications for instability of states. Within DoD, it is imperative to make its critical infrastructure and key resources as secure as they can be, and what is worrisome to me are the "unintended consequences" as the landscape with government and non-government organizations is becoming a blurring mix of surrogates, criminal organizations and academic – research organizations, who are not just building stuff and handing over to the government. As the government increases its outsourcing trends in cyber, risks increase that there will be more mistakes and not an intentional act which will have implications to the DoD and rest of government. Standards and discipline are needed, and leadership and accountability must be brought into the equation by all, as there are things the government relies on that its does not control. There is a real need for measuring and reducing risks better than what is being done today.

Driver 3 – Clarity and Transparency

Historically, most of our sophisticated cyber capabilities grew out of DARPA, in the darkness of the hacker and criminal worlds, and in the legitimate intelligence activities for very good reasons.

If the government is going to develop uniform, military capability we need to shine more light on what we are doing, why we are doing it, and how we are going to control it. It requires a different model than we ever used in the past. Shining more light (not full disclosure) is achieved through increased transparency, and by being very accurate in what we are doing, especially our uniformed military, as the trend right now is greater uncertainty – we need to need to reduce uncertainty and instability or else someone is going to make a mistake. We see lots of things today, and we see a lot happening, but we do not understand its intent. This could lead to miscalculations. The DoD needs to be clear, explain what it is doing, what forces it is building, what capabilities it has and what is needed, and how it is carefully going to control that with significant oversight, command and control, and policy. The DoD wants to the people of the U.S. and world, and its friends and adversaries, to have a little clearer picture about this "uniformed military" and its efforts in the cyber domain. In doing so, it also enables the U.S. to be a little more effective in deterrence, which requires the increased exposure of U.S. cyber capabilities.

President Obama, in addressing West Point graduates, specifically addressed the need for increased transparency when it comes to U.S. counter-terrorism, as the alternative is increased terrorist propaganda,

international suspicion, loss of faith by our partners and our people, and reduced accountability of our government and leadership inability to strengthen the course of international order...all tenets directly applicable to cyber transparency.

There is increased transparency within the DoD as it pertains to forces, capabilities and processes, and DoD attempts to be clearer with friends and competitors by explaining the "whole of government approach." The DoD has been explaining its roles in defending the nation in all domains, and a cyber mission that includes:

- Securing its own cyber systems and networks
- Integrating Cyber into Combatant Commander contingency planning
- Defending the nation in cyberspace, to include countering a strategic cyber attack on our nation's critical infrastructure, an something causing harm to our national interests, economy, and public health and safety

There are also talks about developing "national mission forces" to counter a threat of significance before it has a chance to impact, or at least reduce the damage if it cannot be stopped. Combat mission teams are currently being developed, with a role of integrating Cyber in COCOM contingency plans and operations. There is also more discussion and recognition of Offensive Cyber Operations within the Combatant Commands. Cyber Protection Teams are being created that leverage government/industry knowledge and skills in building and securely operating critical infrastructure (most important systems and networks).

The DoD (and whole of government) wants the world to know about our capabilities, their intentions for their use in ways that does not pose disadvantage to us, and the degree to which these capabilities will be used for deterrence reasons...what a "responsible nation" like the U.S. is supposed to do.

Questions / Open Forum Discussion

1. **What are Undersecretary of Defense for Policy perspectives on the future of Defense (Cyber) Support to Civil Authorities?**
    - Resources (another driver) are a major impediment, as DoD has Cyber manpower shortages and mandated, prioritized missions
    - DoD is not deliberately building forces for, or have the capacity, to handle this mission
    - DoD can support this mission, however, with byproducts of other missions, to including sharing information
2. **A January 2013 Defense Science Board report described Cyber as an existential threat, but DoD has not responded to the report. Is Cyber and existential threat, and if so, is it receiving the sense of urgency in response to that threat?**
    - Cyber could be an existential threat, but do not want to exaggerate the threat
    - Cyber threats today could cause significant consequence to the nation, and why we are building forces and capabilities to respond to and counter this threat
    - DSB report built over a period of time, current conditions and defense standards/capabilities are in place and described at the end of report that addressed problems identified in earlier sections
    - There is a significant cyber threat, and cyber is a priority for the DoD (protected in budget)
    - DoD has a good roadmap on what is most important to take effective action

3. **Cyber Risks and Accountability**
    - There appears to be an overall reluctance to hold accountable those individuals/organizations that increase cyber risk and vulnerabilities by their mistakes or actions (no solid consequences)
    - Fixing cyber incidents and problems needs to be put directly into the Chain of Command, and holding commanders accountable for implementing cyber standards and discipline throughout their organizations as they would any other mission area (this is a culture change)

INDUSTRIAL CONTROL SYSTEMS (ICS) CYBER SECURITY

Dr. Joe Weiss, Managing Partner, Applied Control Solutions, LLC

Dr. Joe Weiss shared his perspectives on Industrial Control Systems (ICS) and ICS Cyber Security. Highlights of his presentation include:

ICS Performance and Safety – Within the ICS world, performance and safety must win over security. We can come close to maintaining a balance, but there will always be residual risk because you cannot design ICS systems exclusively for security.

ICS Components and Functions – ICSs are critical to operating industrial assets that includes including power, refineries, pipelines, chemicals, manufacturing, water, military systems, and medical systems, and monitor and control processes in real time. They include Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and Intelligent Electronic Devices (IED).

ICS Cyber Security, Threats, and Risks – While cyber threats to ICSs are increasing, the ICS community has been more concerned about mission assurance over information assurance, and that systems work over the confidentiality of the data. These systems were designed before networks, and it is important that the ICS community focus its efforts on making sure these systems work first over placing too much focus (and resources) on data controls and security. These systems were never designed to be secure...they were designed to be reliable and efficient. The risks to the electronic grid is not from information technology, such as was the case in the 2003 North East Power Outage (the power restored in a couple of days). On the other hand, if there are cyber attacks on ICS components of the electrical grid or refineries that are connected to the Internet, e.g., such as the Programmable Logic Controllers (PLC), we are talking about outages that are several months in length. Today, there are smart phones and tablets that not only monitor the process, they control the process. However, a denial of service is not the real issue or problem; instead it is the loss of control, and the loss of view. We do need to start over and design ICS systems with a focus on reliability, safety and security.

ICS Cyber Security - why there is so little understanding – The first reason why there is so little understanding is that ICS systems are not mainstream. There are culture issues between Operations, Information Technology and Forensics, and a lack of understanding by IT and Forensics on intentional and unintentional actions (attacks) on ICS systems. It can be unintentional and still kill people. In a 2008 Florida outage caused by a control system cyber incident, the only thing between it being deliberate of unintentional was the motivation of the engineer in the substation that took the initial action. There is also inadequate consideration of cyber, and the ICS community does not really know when an event can be classified as cyber,

although there are tools such as Probabilistic Risk Assessment (PRA) and islanding to increase our understanding.

ICS Cyber Security concerns – For ICS, it is about mission assurance and not information assurance, and an initial concern is that there is a general tendency to look at the system components (boxes) instead of the connections between these boxes. While policies and technologies have been developed for IT, they have lagged behind for ICS. This is one of the drivers for ISA 99, Industrial Automation and Control Systems Security, and the ISA 99 standards development committee that brings together industrial cyber security experts from across the globe to develop ISA standards on industrial automation and control systems security. Another concern are the physical impacts, as you are not destroying data, you are destroying things and affecting physical processes that can last several months. These are also cascading effects, in which one industry can affect another, and it can quickly become international.

Unique ICS Cyber Threats and Incidents – Cyber threats to ICS have both a cyber and physical component to them, and caused in most part by persistent design vulnerabilities and not an advanced persistent threat. Some noted threats include gaps in the protection of the process, as witnessed in the 2007 Aurora incident where the generator room at the Idaho National Laboratory was remotely accessed by a hacker and a diesel-electric generator destroyed. They were also attributed to design features of the controller, as shown with Stuxnet that attacked PLCs and that reportedly destroyed several Iranian nuclear centrifuges. Finally, they were attributed to the compromising of field device measurement, as seen in the HART vulnerability.

Recent Cyber Threats and Incidents – Some recent cyber threats and incidents included:

- ICS Hacking Video Game (Watchdog) that was developed with the help of a cyber security expert and focused on attacking critical infrastructures
- ICS Honeypots (Southern Utility Mock-Up) that within seventeen (17) hours had an actual small utility hacked from Russia and Middle East
- Tilted Oil Rig (Coast of Africa) cyber attack that altered the stilts, thus impacting the tilting and damaging of the rig
- Faulty Security Patch that was installed in a $100 million dollar turbine, and after installation, unintentionally shut the turbine down.
- Iranian Stuxnet paper and translation of Project Shine, where an engineer working on Siemens controllers procured test versions of anti-virus products used in an article he submitted to the editor of Control Magazine
- Project Shine that was developed to extract information about the existence of SCADA and ICS devices accessible from the Internet, using an existing online search engine called SHODAN to scan the Internet looking for attached devices (there are an estimated 1 million ICS/ICS related devices connected to the Internet)
- There have been an estimated 350 actual cyber incidents to date, ranging from significant discharges, significant equipment damage, and deaths.
- ICS specific cyber security technologies, training, and policies are very few in number

Aurora Incident – As discussed earlier, the Aurora incident was caused by a gap in the protection of the process, which involved the turning off, then on, of equipment that was out of phase with the grid. The Aurora incident was enabled by the electric power grid to intentionally or accidentally damage or destroy

motors, generators, and transformers. Protection was used as the attack mechanism, with the attack oriented on using protective relays and high speed breakers designed to protect grid components. Destruction of components was caused by the unsynchronized reclosing of them of them on the synchronized electric power grid. This could create situations of critical U.S. assets, such as turbines on a nuclear power aircraft carrier that are routinely connected to the grid when in port.

Next Steps – Some of the things that need to be done includes:

- Getting senior management acknowledgement and willingness to address the problem
- Getting ICS, IT, Security, and Forensics to work more closely together
- Improving the security posture of legacy ICS, and engineering security into new ICS systems (initial design and specifications)
- Developing and implementing ICS policy and other changes to include ICS resilience and recovery, ICS cyber security training, and appropriate information sharing
- Increasing use of demonstrations (Test Beds), such as the Utility Test Bed that evaluate ICS cyber security technologies for impacts on ICS performance and overall system reliability, as well as the DoD ICS Cyber Security Test Bed, a collection of systems and devices typically used in Naval facilities that evaluates attempts to break into these systems as currently installed and after migration measures implemented by commercial vendors, universities, and laboratories

Concluding Remarks – Dr. Weiss concluded his presentation by reaffirming how vulnerable ICSs are to cyber attacks or incidents (intended or unintended), how ICS cyber security is a major risk to DoD missions, how a "smoking gun" called Stuxnet made ICSs a legitimate target for cyber attacks, and finally, how securing ICSs require tailored, ICS specific approaches.

DEVELOPMENT OF CYBER IN THE AUSTRALIAN DEFENCE FORCE

GPCAPT Paul Wade, Deputy Defense Cyber Coordination Office, Australia

GPCAPT Paul Wade provided the following unclassified abstract that expanded upon his classified presentation. Sanitized, unclassified highlights of his presentation, and additional information of importance to the Defence Cyber Coordination Office, include:

Australia Defence White Paper (2009) – this white paper assigned high priority to cyber warfare and undertook to invest in a major enhancement to Defence's cyber warfare capability.

Defence Cyber Coordination Office (DCCO) – in January 2012, the Australian Defence Force (ADF) established the DCCO in the Joint Capability Coordination Division under the Vice Chief of Defence Force to facilitate the development of ADF Cyber. Key DCCO roles and responsibilities, and activities, include:

- Sponsoring Cyber doctrine development, to include Joint Doctrine Note 2–12 that was published in October 2013, and current development of a full Australian Defence Doctrine Publication (ADDP) that will be released by December 2015.

- Providing input to the development of Cyber policy by the Strategic Policy Division. White there is an extant Defence Cyber Policy dated 2010, new Cyber Policy and Strategy documents are currently in development.
- Developing a six-tiered ADF Training and Education model (completed the strawman) .
- Developing the ADF Cyber workforce development, to including determining Joint and single-Service workforce requirements and specification of roles and responsibilities
- Integrating, normalising, and operationalising Cyber, to include the consideration of Cyber in operations and planning, capability development, and 'business as usual.'
- Conducting planning and coordination of Defence's participation in the Exercise CYBER FLAG (CF), USCYBERCOM's annual Tier 1 five-eyes exercise. CF is providing considerable value to the ADF in the development and validation of an ADF cyber-specific C2 construct, and exposure to operating in a contested and degraded cyber environment.

Cyber Challenges – there are significant challenges that are impeding the rate of cyber development progress, to include:

- The cyber threat to military operations has not been adequately understood by the ADF's senior leadership until 2014. Until recently, the cyber focus has predominantly centred on protecting internet-facing government networks from cyber espionage, not on the cyber threat to 'closed' military networks and systems.
- The ADF is seeking to better understand the magnitude of the cyber threat to its Network Centric Warfare (NCW) architecture, given that the NCW model was developed back before the cyber threat was a major concern.
- The ADF needs to understand the impact of adversary's use of offensive cyber capabilities against us. Of concern, effective cyber attacks on combat systems may not be obvious, such as subtly degrading a key combat or C2 system
- The ADF also needs to better understand the vulnerability to cyber attack of the supply chain and infrastructure that supports military operations.
- Non-state actors will increasingly seek to develop offensive cyber capability. Barriers to entry are relatively low and the sophistication of the attack methods is increasing. While non-internet facing ADF systems should remain reasonably secure against non-state actors, the challenge to protect Government networks and national infrastructure will increase. We can expect non-state actors to launch offensive cyber action against Government networks in response to Government policies.
- CND responsibilities in Defence are not clearly defined. Responsibility for the CND of stand-alone systems (those not directly connected to Defence's Information Environment) is an area of ambiguity. Defence's Head ICT Officer argues that he is the CND capability manager for all Defence and hence responsible for all stand-alone systems and networks, including those owned and operated by the ADF. However, the opinions of his staff are divided on whether 'stand-alone' systems include the mission, weapon, sensor and engineering systems in combat platforms.
- The identification of resources necessary to develop a dedicated ADF cyber workforce has not yet been achieved, although workforce design is currently in progress.
- Retention of our emerging cyber workforce is also a challenge. Australian Public Service (APS) employees and ADF personnel who acquire skills and experience in cyber are in high demand in the

private sector. Retaining cyber-skilled ADF personnel is a challenge because many want to continue in the cyber field but the Services want them to return to core specialisation or trade – private industry provides them with the opportunity to resign and continue in the cyber field with a generous pay raise. The ADF is too small to introduce a dedicated cyber core or mustering at this stage, so an innovative solution is required.

- The classification of cyber incidents in the ADF prevents their use as educational vignettes for military personnel. The media largely focuses on cyber crime and the threat to internet-facing Government and Industry networks, so the majority of ADF personnel are largely unaware of the cyber threat to ADF combat systems and operational networks because the threat is not readily apparent. The ADF has had a number of cyber incidents, yet the specifics remain highly classified, thereby limiting their use to educate the wider ADF workforce on vulnerabilities and threats.

Concluding Remarks – while there are a number of key challenges to cyber development, none are insurmountable and the ADF is making slow but steady progress. Our five-eyes partners are all on similar journeys and there is an excellent level of cooperation and information sharing that is expediting our progress on some challenges.

PANEL 1 – ALLIED AND PARTNER NATION CYBER POLICIES AND RULES OF ENGAGEMENT

Dr. Steve Chan, MTI/IBM NSRC/Sensemaking PACOM Fellowship (Moderator)
Mr. Bob Griffin, CEO, IBM i2, IBM NSRC (Panel Member)
Mr. Ed Bryan, United Kingdom, IBM i2 (Panel Member)
Mr. Jan-Kees Buenen, Amsterdam, SynerScope (Panel Member)
Mr. Jim Hackett, Canada, Mehta Tech (Panel Member)

Dr. Steve Chan introduced his panel members, and opened up with a video message from Ms. Mary Aiken, Ireland, Royal College of Surgeons in Ireland, who shared her insights on CSI Cyber, a television show inspired by her involvement in Cyber Psychology to educate the general population on cyber security, and the impact of emerging technology on human behavior, the fundamental underpinning of Cyber Psychology. Ms. Aiken also discussed her experiences and involvement in Cyber Psychology and Forensic Cyber Psychology, and the various undergraduate, graduate, and post graduate programs at the Royal College of Surgeons. Dr. Chan then requested each panel member to provide opening remarks, and then directed a series of specific questions to each panel members. Highlights of the first panel included:

Mr. Bob Griffin, CEO, IBM i2, IBM NSRC (Panel Member)

Mr. Bob Griffin provided some of his insights on Ireland's impact and contributions in Cyber, and other topics such as the proliferations and open sharing of information. Highlights of his panel remarks included:

- One of the primary Cyber focus areas within Ireland includes the Cyber Center discussed by Ms. Mary Aiken, and Ireland's conscious decision to provide incentives to define itself in Cyber, one of which includes investing in people and using their intellectual property as an asset.
- Many companies in Ireland are investing in people, and creating fabulous minds in Cyber, Cyber Psychology, and Cyber Forensics – and these minds are getting drawn to other areas of the world.
- Ireland is building economic infrastructures for development of Cyber resources, and moving off shore.
- Some advantages achieved by this approach include Ireland is now seen as pushing the envelope in Cyber, Cyber Psychology, and Cyber Forensics.

Mr. Griffin then provided some of his insights on proliferations and open sharing of information, and also techniques and attack vectors on critical infrastructure that now looks like on massive Maginot Line.

- One of the lessons learned from Iraq, in looking at the criminality across the world, from a cyber perspective, was that we are seeing more activity originating from Eastern Bloc countries, more cash flow to Russia, and more sophisticated methods.
- A substantively increased percentage of these nations organizations are involved in organized crime, terrorism, and fraud in cyber space.
- Insider threats are increasing, as illustrated in NYC where insiders obtained control of assets through system privileges. The perpetrators raised ATM limits, used their hacking skills to observe PIN numbers, and applied sophisticated Supply Acquisition techniques to manufacture ATMs. Within 48 hours, and across 16 different countries, they were able to withdraw 48 million dollars without triggering behavioral changes and subsequent alarms. They clearly demonstrated IT skills, hacking skills, supply chain skills, trusted networks, C2 structure, and coordination.
- Within Law Enforcement involving cyber crimes and incidents, Interpol and other agencies have broken down the barriers of international boundaries, frequently exchanging information with other internal organizations and countries.
- Within the UK, there is a single point of contact within the National Cyber Crimes Unit for people to report a cyber crime or attack.
- Within the UK, and not unlike the US, law enforcement is conducted by county, and cross coordination across countries is tougher than it should be. So in an isolated cyber event, local establishments take details of that event, but their knowledge of what is actually happening is isolated, requiring coordination across the UK to allow more intelligence and information together (breaking down the barriers.
- From a network science perspective, the electric grid is a network. I worry about the actual compromising of the grid, and that utilities' themselves can compromise the grid. The challenge is that technology plays a critical role in protecting the grid, and human behaviors identified to act. The promise of technology is that it moves as the fast as the speed it is directed, but the real challenge is how fast can humans assimilate this technology and information it generates?
- It is also not only technology involved in the protection of critical infrastructure, it is also the ability to take the "human sensor signal" and apply that to dynamic analysis. The human sensor piece needs to be able to build indicators that someone should act on, e.g., anomalies.
- We also live in a world where people are dynamic in their intent, and very adaptive. Bad guys typically are early adopters of technology, and adapt when we change ours.

- Things are not going to slow down, and they are going to become more complex and challenging, which highlights the value of "big data." The reality of big data is that without sophisticated analytical tools to make sense, such as visual analytics, there is no value added from this "big data."

Mr. Ed Bryan, United Kingdom, IBM i2 (Panel Member)

Mr. Ed Bryan discussed how the United Kingdom has transitioned from a traditional sea-faring nation and traditional naval warfare into a nation focused on cyber and cyber warfare. His insights on the United Kingdom's cyber transition and impact include:

- The UK redistributed its resources from traditional naval warfare into cyber
- Cyber threats have become Tier 1 threats to the UK, on equal footing with threats from nuclear to biohazard threats.
- In 2011, the UK government published a Cyber Security Strategy White Paper, which formally established the Office of Cyber Security and Information Assurance as a Cabinet level reporting office. This was a UK defining moment to declare Cyber threats as a Tier 1 threat, right with International Terrorism, and the importance of Cyber Security.
- The Office of Cyber Security and Information Assurance coordinates Cyber Security policy across the UK, and includes responsibilities for working with law enforcement agencies, intelligence agencies, and the public sector about Cyber, Cyber Attacks, and Cyber Security.
- The Office also provides education, not just how you take an offensive or defensive position, but also on educating the population and the need to make them aware of what is going on, as well as raise general awareness and to educate the public sector as well.
- The Office is also responsible for coordinating with all the internal actors and communicating/sharing information on cyber threats that are increasingly global (they don't just target the UK).
- UK government investment to date in its Cyber Security Strategy white paper has been an estimated 650 million pounds (over a four year period), and in 2015, and additional 200 million pounds will be added by the Chancellor. While some nations have been thinking budget cuts, the UK has been actively funding since Cyber threats are in Tier 1.

Mr. Bryan then addressed the moderator's comments regarding as we move to the smarter grid, smart devices are increasingly dependent on access to the internet, but disinformation or misinformation come into play, so social media monitoring may come into play too. Comments included:

- There have indeed been events in the UK where disruption started with social media, and was coordinated through social media, so leveraging that source of publically available data is important.
- Social media is used extensively in investigations (not much an issue), but it is the thought process of social media being used in a more subversive way that is troubling. Sometimes people will use social media to post what their motivations are as they maneuver and manipulate through social media.

Mr. Jan-Kees Buenen, Amsterdam, SynerScope (Panel Member)

Mr. Jan-Kees Buenen discussed how Amsterdam has moved much of its services to the Internet over the past two decades, and how visual analytics can enable increased situational awareness and discovery. Highlights and insights include:

- Many services, such as financial institutions and banks, have moved to the internet and "essentially done away with cash," and now rely on banking on the internet. By 2013, all four major banks had also outsourced their services.

- Amsterdam has experienced a mass movement to mobile platforms, the newest targeted attack vector.
- The government is increasing its emphasis on cyber security and threats, and the impact of cyber security.
- Amsterdam is a major hub to cyber traffic, and financial traffic over the internet. It is connected worldwide, and has stepped up to the plate.
- Amsterdam has a cyber security research agenda, and it is interesting on how much they are handing out dollars on research conducted at the cutting edge.
- Amsterdam is increasing visual analytics, as it is difficult to maintain and make sense of all the heterogeneous data being generated by all these devices. With visual analytics, we are able to take structured, semi-structured, and unstructured data and try to transform (through normal visualization techniques our brains can comprehend) them to images about networks, time lines, and natural language into one view.
- Visualization addresses "messy data," and you don't have to have perfect data. It is transforming disparate information into a picture. Social media networks are increasingly used in this process.

Mr. Jim Hackett, Canada, Mehta Tech (Panel Member)

Mr. Jim Hackett discussed the need for interoperability and synchronization, and a brief overview of their role in maintaining and securing the smart grid and utilities. Highlights and insights include:

- In the Northeast Blackout in 2003, I contacted a couple of utilities in Canada to assess the impact of this blackout on utilities. One utility after another needed assistance and restoring utilities was a system effort between them that crossed borders with the U.S.
- Within the utilities, operators wanted to find out what happened, so they went to the equipment in the sub-stations and brought back data (references) which was not time sensitive.
- In 2004-2005, Canada introduced new regulations in anticipation of future utility outages, and wanted to make sure utilities/systems were connected to each other, which produced more and better data that was time synchronized, thus helping the infrastructure handle things better.
- The key message is that there is a need for time synchronized data and time synchronized measurements on the grid. The utilities and independent system operators must have access to the right data to advance the security and illumination of the grid.
- In looking at a real time environment and data, data has to be recorded by people. Some utilities are using data mining tools, not just to look at data in real time, but over a period of time to see if they can identity patterns. Some tools when they recognize something happening (or anomalous) relay the situation to the utilities. More predictive tools are needed to identity trends, and how significant event affects one or more types of situations.
- If the utilities can recognize precursors, they might be able to preposition operators to automatic control before any outages or blackouts occur.
- Within Canada, some utilities are walking (looking at data), some are running (using automated systems) and actively collaborating with the Canadian and U.S. government, industry (not just utilities), and academia.
- These utilities don't like to be told what to do by regulators, even less by their government. Additionally, utility engineers do not always listen to senior executives in their own organizations. You can't expect utilities to act in a homogenous manner and dragged along; it is not going to happen.
- Within the U.S., the U.S. is dictating minimal levels of performance for utilities, as a price for membership.

- With respect to cyber security, and how these utilities perform overall, utilities have their own cyber practices related to their own organizations and operations.
- There is tension between engineers and IT, because engineers know they have to operate their systems, and don't want to be constrained, while IT is doing the right things from the corporate perspective.
- Disgruntled employees (insider threats) are a greater risk than outsiders trying to get in from a cyber threat perspective

PACIFIC COMMAND SCENARIO

Dr. Richard Berry, Director of Strategic Partnerships, U.S. Pacific Command

Dr. Richard Berry provided an overview of U.S. Pacific Command, Public Private Partnerships, and Resiliency. Dr. Berry is responsible for broadening the USPACOM engagement strategy through Public Private Partnerships and Senior Leader Engagement. Highlights of his presentation include:

U.S. Pacific Command Snapshot – U.S. Pacific Command is one of six Combatant Commands. It is the largest COCOM covering 52% of the world's surface. It has seven of the largest militaries in the world. By 2020, 7 out of 10 people will be living in the Asia-Pacific region. An estimated 50% of all cyber attacks originate in the Pacific, with 40% originating from China. What weighs on the USPACOM commander is that PACOM responds, on an average of once every six weeks, to some national disaster in the Asia-Pacific region.

State of Hawaii Senate Bill 2742 (Passed) – The purpose of this Senate Bill 2742 is to initiate a revolutionary and innovative public and private partnership to be known as the Pacific-Asia Institute for Resilience and Sustainability. This institute will develop the next generation of leaders to address the world's most difficult problems, including climate change, environmental degradation, public health, sustainable use of natural resources, critical infrastructure protection, and cyber resilience.

Public Private Partnerships: The Fourth Sector of Society – Public Private Partnerships (P3I) are considered messy in terms of authorities and regulations, but USPACOM has identified ways to make this work, the first approach of which is "Resiliency by Design."

Resiliency by Design – Everything is being connected, and globalization is happening at hyper speed. We are politically and economically connected, and co-located. When something happens locally, it can send a ripple effect throughout the world, as we saw in the March 2011 Japan earthquake and tsunami, an epic disaster the demonstrated the resolve and resilience of Japan in its aftermath. It just was not just a local disaster, and we saw in the debris fields that traversed the Pacific Ocean, and in the supply chain across the world in which billions of dollars were lost. There are other problems, such as the oceans rising and how that impacts our business, our communities, and other problems it starts to present. These are the problems "above the water line," that we either knew about and/or dealt with before. It's the things below the water line, the deep problems that we do not see or are aware of that concerns me – the unknown unknowns.

USPACOM Commander Takes Action – The previous PACOM Commander, after a series of incidents to include the 2006 earthquake in Honolulu that brought power down and the spillage of millions of sewage in Waikiki Beach, stated emphatically that it is time to do something different. What does this different look like? This question made us look at things differently from multiple places, same time, and a very conceptual approach (layered) to getting from point a to point b. With the level of complexity, this is much more than a 3D model that creates the choices we have, and even with the massive amounts of data that we have access to, where do we need to go? It's a big maze, and even though we have created more data in the last two years than in the history of the world, how do we bring this to bear in solving these wicked, below the waterline problems?

AIRS and the Banyen Tree – The world we create is a product of our thinking and cannot be changed without changing the way we think about it. We need to ask ourselves, are we doing anything different than what we have not done before? USPACOM has embraced this new challenge and vision under its AIRS Model, which is based on the concept of the Banyen Tree which is the largest tree in the world and has physically and symbolically become the center of the community.

Banyen Tree

The Banyen Tree's root system is the public-private sectors that try to come together to solve problems, each from a different perspective. This is the core of the society. The trunks and branches represent how we go about solving these problems, and under the AIRS Model this is all about education and applied research. We want to change the paradigm so not the same, with a focus on:

- Education with a purpose
- Workforce development
- Getting a skilled workforce to do the things we need to do and pull those things together

The canopy are the leaders, those individuals who build capacity. Finally, it all comes together when they return to their organizations with a renewed vigor and purpose.

The Banyen Tree is unique in that the branches start growing back towards the ground, where they root themselves to the ground and start to create an ecosystem for the community.

AIRS attempts to develop an ecosystem that not only provides a place for the private sector to solve problems, or only a place where academic research is conducted, but also produces the skilled workforce needed. In this way the Governor of Hawaii can do what he originally intended to on coming into office, and that is to provide for the public caucus. One of the problems has been the focus on leader development and not

leadership development. Need to now talk about leadership development and what we want to be the result, and not the individual leaders.

- Leader development is an individual approach, and is about the individual in the organization, ego based, and with individual lanes in the road
- Leadership development is a collaborative approach, with a win-win goal (there is no win-lose), and if the public-private-civil sectors are to win, they all need to be involved and fully engaged

To change something, we need to build a new model that makes the old model obsolete, and this is the AIRS model which is focused on such things as critical infrastructure, cyber, power, sustainable systems, and utilities.

The AIRS model is built on human capital development and building organization capacity through education and applied research, merged together in AIRS model and all worked at the same time.

- From a human capital perspective, this is bringing the right people to do the right things at the right time
- From an organizational capacity perspective, we want these people to be able to innovate and really break out of the silo and think about the problems differently (learn and think differently that solving your typical point a to point b problem)

Through that experience, these are the people we want to send back to the community, so like the Banyen Tree, they send roots back into the ground, and they take responsibility and solve problems we need to face. This is where technology also comes into play, but we cannot apply this technology if we don't have the workforce to go along with it...it has to be done at the same time.

This model brings some of the best minds from the public, private, and civil sectors to bear on these problems is such a way that these problems start to be addressed and start coming up with the real solutions we need.

In designing this model, which the State of Hawaii is trying to move forward to solve USPACOM and Hawaii's problems, need to design it actually on how it works and how it functions.

- Civil, Private, and Public Sectors all work a part of AIRS, but there is no one of the three in charge
- Civil Sector brings the academic dimension needed to educate the workforce
- Private Sector brings the problems, from a perspective of where we need to send them to get experience, and where there is some possible funding
- Public Sector helps by creating and convening to make this happen and help shape policy that is a collaborative policy, not just coming from Washington DC.

The messy part of this starts with the problem, and agreeing to where the real problems are. Fellowships and research is the draw and what brings everyone back together. Effective collaboration brings an end to the new types of leaders we need, and the solutions, and innovative products.

What gets the ball officially rolling is State of Hawaii Senate Bill 2742 (Update: this bill was passed)

During a brief question and answer period, Dr. Richard Berry all brought up the concept and need for reciprocity. If someone is not going to come to the table with a concept of reciprocity, it is a partnership that won't work too well. Ego-centric perspectives, such as what is in it for me, will not work. Instead, what does work is coming to the table focused on what each of us can do, and what each of us brings to fight.

Mr. Sean Kanuck, National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence

Mr. Sean Kanuck provided an overview of the roles and responsibilities of the ODNI, and shared his perspectives on Cyber Defense and Cyber Arms Control, the strategic dynamos of cyber space and international security and what this means at the global level, precision timing and insider threats, and some larger strategic themes. Highlights of his presentation follows:

National Intelligence Committee (NIC) and the Threat – The DNI is responsible for the development of the Annual Threat Assessment, and document forwarded to Congress at the classified and unclassified level. It was no coincidence that cyber is considered the greatest national security threat from the Intelligence Community viewpoint, and that cyber is an integral part of every other threat.

Key Themes – if one thinks about counter proliferation and counter terrorism activities, there are cyber elements involved in all of these in addition to the outright cyber threats in cyberspace.

- **ODNI/NIC doesn't subscribe to the Pearl Harbor scenario**. It does not mean we sleep well at night. It is that we are trying to make a distinction between the various sophisticated global leaders in offensive cyber capabilities (think Russia and China), while noting they are both permanent members of the Security Committee of the UN Charter. Our current position does not see Russia or China commencing a full scale, lights out event in the U.S. absent of other military activities (but at the same time, recognizing that if the grid goes out, there will be problems with missiles and ships).
- ODNI has slightly different concern on countries with lesser capabilities but with possible less interest in the UN paradigm system, and possibly a higher intent for doing things in a peacetime scenario. This includes Iran and North Korea who may not feel their policies are vested in the international community and could be possible sources of complication in peacetime.
- When we talk about when the lights going out, that is already past where we can contribute to the problem. Of more concern is when the "lights flicker," that you cannot explain why as they may be a proof of concept test by an adversary who has forward deployed something.
- Risk mitigation and remediation incredibly important, and as we build our National Intelligence Estimates, we are trying to see things down the road and who is (or may) be fostering these possibilities.
- Nation versus Non-State Actors – we discuss in NIE cyber criminals, terrorists, and hactivists, but have not yet seen a pure incident of cyber terrorism where death and destruction were perpetuated simply by zero's and one's. We do know that cyber is used in support of terrorism, and to support their command and control in real time of attack.
- Corporate Entities – interesting role they are playing in this environment. There are very legitimate processes, penetration testing, etc. to perfect their tools and techniques. It is the propagation, proliferation, and more offensive actions based on this expertise that is of concern. Not saying that

what is happening in industry is illegal or inappropriate, it is something we need to be aware from a proliferation context.

- **Raising the Bar** – all the money going into the information security industry, and the many skill levels and experience that is increasing around the world, is actually raising the bar for people to perpetuate malevolent cyber activity and go undetected for prolonged periods of time. Reports (from McAfee and others) are exposing these events of non-state actors which have been increasing.
- The financial, electric, energy, health care and other sectors are not necessarily well protected, and some incredibly vulnerable. Trying to work with DHS and government partners to address.
- **Global Trends Paper (2030) and Critical Thinking** – there will be significant environmental changes, and incredibly technical centric. There will be increased disruptive technologies, and disruptive applications of technology. Consider the Internet of Things, with everything and everyone connected to the Internet. Governments are having an increasingly harder time keeping pace with technology changes and adaptation of potentially disruptive applications. We are at a critical juncture in national security thinking, as our society changes with new platforms that are recreating.
- **Cyber Security Trends and Impact** – the trends are not looking good. There is a lot more malicious activity; there is a broader range of actors, state and non-state, some internally motivated while others ideologically motivated (murky swamp); and there is more disruptive and destructive activity. This neighborhood getting more dangerous. The rising, malevolent tide of activity, that is aggregating over time, will take a drain on our society, economic competitiveness and viability, and our ability to defend ourselves if and when needed (from a military and homeland security perspective).
- **Strategic Thinking and Complications** – The U.S. is very immature in its strategic thinking in cyber security matters discussed above. We have outstanding tools and capability, but we have not formed our own strategies they want we want to, formulating a strategic dance with our adversary. We seem to know not what we are doing, and everyone is holding their cards close, and everyone is trying to get individual advantage. It is understandable that technology eventually gets militarized or used in conflict someway, and there are efforts to use the law to stop it that includes:
    - International Humanitarian Law
    - Law of Armed Conflict
    - Hague Convention

Economic and Security Interplay – there is significant interplay between security and economic efficiency, and Internet governance debates are going on today. This is an unstable, unsecure environment based on how players going to be interacting. The three perspectives from which to look at this are ecosystem, tools, and how tools are used.

- **Eco-System (Duality)** – the same sector or channel in which you would want to use coercion against an adversary or competitor is the same channel used to monitor, signal, and verify.
- **Eco-System (Non-Separability)** – the non-separability of non-security strategic deterrence creates domestic problems, regime instabilities, and complex politics of using them in an international capacity. Strong probability that cyberspace will be the same vector for dissidents may be the same vectors external adversaries may seek to disarm, exploit, or attack.

- **Eco-System (Multi-Polarity)** – The stakeholders include companies, skilled hackers, ideological hactivist groups, all of which creates a muddy environment. There is an increased use of proxies, making it difficult in knowing who were fighting and "playing chess."
- **Tools (Perishable)** – tools are perishable, and patches/upgrades that are now available to the adversary might obviate the utility of your own tool. Tools have a "one time use," so once revealed, the tool may not work again based on an adversary reverse engineering of this tool. The adversary can also repurpose sections of the tool, such as seen with Stuxnet. Since you are not likely to use the tool into when really needed, this creates an "all or nothing game" which in game theory is not good.
- **Tools (Specificity)** – if tools are going to go after a target of interest instead of opportunity, cyber tools have to have the equivalent of having their name on it to be sure it is going to work. Resource allocation and target identification needs to be done in advance, which creates foreign policy issues as this occurs against an international threat.
- **Tools (Immediacy of Effect)** – what are the immediacy of the effects the tool expects to have? USCYBERCOM has a mission for dominating cyber domain to assure freedom of mobility and to deny that to the enemy...at the speed of light, internet speed, cyber speed. To deal a lethal blow (cut off the neck of the snake), these tools have to be pre-deployed well before an adversary can do the same to us, in multiple locations.
- **Tool Usage (Clandestine)** –tools will be used clandestinely, without overt attribution, and staged below the line of conflict and active aggression. We know how we are supposed to behave in the global community; the problem is that when you universalize the clandestine use of cyber tools in this created an incredibly unstable ecosystem. In the context of transparency (Maj Gen Davis comments), it might be strategically advantageous for the U.S. to put its name (stamp) on its tools.
- **Tool Usage (Discrimination)** –the Law of Armed Conflict has a principle on not going after civilian targets, but this point is more than that. If the case is made to go after civilian targets than over decapitating/immobilizing a country's command and control, this could cause immediate retaliation.
- **Tool Usage (Unpredictability)** – there is real potential for collateral damage that you will not know in advance. Doubt actors fully know the full scope and ramifications if they released certain cyber weapons. This could bump against foreign red lines and perceptions, it could increase the potential for cascading effects that are unintended, or it could result in a de-escalatory shot across the bow that takes out a hospital.

Concluding Remarks – Mr. Sean Kanuck closed his presentation by stating that instability and volatility are the two words that best describe cyberspace. It is important that strategic thinkers in the military, industry, academia and elsewhere come together and find the right strategic model, and see if we can find the right dynamic that increases everyone's security.

DOE CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS R&D

Dr. Carol Hawk, CEDS Program Manager, Department of Energy

Dr. Carol Hawk provided an overview of the Department of Energy (DOE) roadmap to achieve energy systems cybersecurity, and the multiple DOE activities that are aligned with this roadmap. Highlights of her presentation include:

Overview – the development of the roadmap was a DOE collaborative effort that brought in the utilities and those associated with Industrial Control Systems (ICS). The roadmap is the energy sectors synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones. It also provides a strategic framework to align activities to sector needs, coordinate public and private programs, and stimulate investments in energy delivery systems security. The overall vision of the DOE is by 2020, energy delivery systems (EDS) are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

- This will be an interdisciplinary approach, an intersection of power systems engineering and cybersecurity (computer side).
- Cybersecurity must be initially designed into the system, but must follow the rule of "do no harm"
- Cybersecurity capabilities must not impede the performance and functioning of the system it was designed to protect
- There are legacy EDS devices out there that there is no economic case for replacing, as they function as intended (designing cybersecurity in these instances is not a concern)
- There is a need to protect legacy EDS devices as well as the next generation devices that are coming into the power grid. EDS components widely dispersed geographically, and located in publically accessible areas where they are subject to tampering.

DOE Goals and Fundamental Directions – there are several DOE activities that align with five fundamental directions (goals), to include:

- Building a Culture of Security – through activities focused on training, education, and improved communication within industry
- Assess and Monitoring Risk – through activities such as an Electricity Subsector Cybersecurity Capability Maturity Model, situational awareness tools, common vulnerability analysis, threat assessments, and consequence assessments
- Develop and Implement New Protective Measures to Reduce Risk – through activities such as support to cybersecurity standards development, near term (0-3 years) industry led R&D projects, mid-term (4-7 years) laboratory R&D projects, and long term (8-10 years) laboratory and academia R&D projects.
- Manage Incidents – to include the National SCADA Test Bed (NSTB), outreach, and cyber exercises
- Sustain Security Improvements – to include product upgrades to address evolving threats and collaboration among all stakeholders to identity needs and implement solutions.

CEDS Alignment with the Roadmap – CEDS has an overarching goal to accelerate cybersecurity investment and adoption of resilient energy delivery systems, and provides federal funding to national laboratories, academia, and solution providers. The CEDS program balances higher risk (longer term, minimum cost

share), medium risk (mid-term, lower cost share), and lower risk (shorter term, higher cost share) projects. The CEDS program emphasizes collaboration among the government, industry, universities, national laboratories to advance R&D in cybersecurity that is tailored to the unique performance requirements, design, and operational environment of EDS. Figure 3 highlights key components of the EDS architecture.

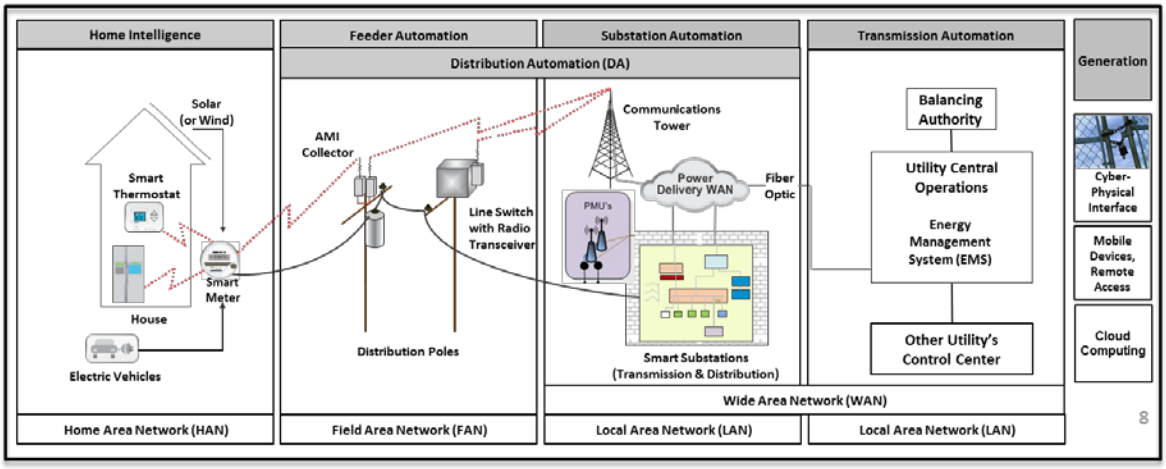

Figure 3 – EDS Architecture

CEDS Projects – CEDS projects engage national laboratories, vendors, asset owners, and academia throughout the project lifecycle to deliver relevant projects with clear commercialization paths. CEDS projects include applied research, prototype development, and field demonstrations. The following highlights the myriad projects that have been undertaken under the CEDS Program, with details not included in this final report but discussed in depth in her presentation that has been made available to participants. These projects, all of which have been aligned to the roadmap, include:

- Cybersecurity Procurement Language for Energy Delivery Systems – language tailored to the specific needs of the energy sector
- Supply Chain Integration for Integrity (SCI-FI) – research to understand energy component supply chain integrity
- Energy Sector Security Appliances in a System for Intelligent, Learning Network Configurations Management and Monitoring (ESSENCE) – stronger, easier to manage operational and back office network security for electric cooperatives
- Alliance Projects – unified central control of cyber and physical access to energy sector building and cyber assets
- RBAC Driven Least Privilege Architecture for Control Systems – modular toolset for systems-wide role-based access control (RBAC) and enforcement
- Secure Policy-Based Configuration Framework (PBCONF) – reduce risk of cyber attacks that exploit incorrect or inconsistent energy delivery device security
- Secure Information Exchange Gateway (SIEGate) – flexible, real-time, reliable and secure information exchange for electric grid operations
- SDN Project Defined Network – more secure, reliable operational network traffic shaping, with automatic, predefined rerouting around network disruption
- Collaborative Defense of Transmission and Distributed Protection and Control Device Against Cyber Attacks – does not allow cyber activity that could jeopardize grid operations

- Exe-Guard – whitelist malware protection for control systems at the device level
- Secure SW Defined Radio – more secure "communications to the remote sites
- Applied Resiliency for More Trustworthy Grid Operations (ARMORE) – more secure, faster ways to use substation data from both legacy and modern devices
- Padlock Security Gateway – greater situational awareness and incident response capabilities for field devices
- Cyber-Intrusion Auto-Response Policy and Management System (CAPMS) – detect, evaluate, and respond to a cyber intrusion without disrupting the power grid
- Cyber Intrusion Detection and Monitoring for Field Area Networks – smart meter and distribution wireless communications security
- Cyber Physical Modeling and Simulation for Situational Awareness (CYMSA) – predict in real time how a cyber attack might disrupt energy delivery, and dynamically protect
- Patch and Update Management Program for Energy Delivery Systems – reduce the risk that a known vulnerability could be exploited on an emergency delivery control system

CEDS 2013 Energy Sector Projects

- Trustworthy Cyber Infrastructure for the Power Grid – trustworthy technologies for wide area monitoring and controlling, and a project that impacts all aspects of the 2011 roadmap
- AMIlyzer Tool – specifications-based intrusion detection system for advanced meter infrastructure

CEDS Coordination and C2M2 Program

- CEDS coordinates with other Federal Cybersecurity R&D programs, and supports networking and information technology making in the White House Office of Science and Technology Policy (OSTP)
- CEDS has developed an overarching Cybersecurity Capability Maturity Model (C2M2), as well as for the Electricity Subsector and Oil and Natural Gas Subsector. Since 20012, hundreds of organizations have used the C2M2. With C2M2, DOE has facilitated self-evaluations for utilities servicing an estimated 39 million US customers. Business Executive for National Security (BENS) plans to endorse C2M2 for their 400+ members.
- C2M2 goals include strengthening cybersecurity capabilities, enabling consistent evaluation and benchmarking of cybersecurity capabilities, sharing knowledge and best practices, and enabling prioritized actions and cybersecurity investments.
- The C2M2 model includes ten domains, or logical groupings of cybersecurity practices, and include:
    - Risk Management
    - Situational Awareness
    - Workforce Management
    - Asset, Change, and Configuration Management
    - Information Sharing and Communications
    - Cybersecurity Program Management
    - Identity and Access Management
    - Event and Incident Response, Continuity of Operations
    - Threat and Vulnerability Management
    - Supply Chain and External Dependencies Management

PANEL 2 – U.S. ROLES, RESPONSIBILITIES, AND CAPABILITIES (GOVERNMENT AND DEPARTMENT OF DEFENSE)

Mr. Robert Spousta, Sensemaking/U.S. Pacific Command Doctoral Fellow (Moderator)
Mr. Randall Cieslak, SES, Chief Information Officer, U.S. Pacific Command (Panel Member)
Col William Hutchinson, U.S. Cyber Command (Panel Member)
Mr. Ross Roley, Energy Office Lead, U.S. Pacific Command (Panel Member)
Mr. Jeff Johnson, Command Information Officer (N6), Naval District Washington (Panel Member)

Mr. Robert Spousta introduced his panel members, than provided some introductory remarks on threats and vulnerabilities, and how these relate to critical infrastructure and the energy sector, as well as set the stage for panel members to discuss what they are doing in the field to address these threats and vulnerabilities in general, and specifically with the electrical grid and critical infrastructure.

Mr. Randall Cieslak, SES, Chief Information Officer, U.S. Pacific Command (Panel Member)

Mr. Randall Cieslak provided an overview of a Cyber Discussion Framework that USPACOM developed in an effort to discuss cyber capabilities vice systems amongst colleagues within and outside USPACOM and the Pacific. Highlights of his presentation included:

Introductory Remarks – For the past five years, most of the discussion on cyber surrounded roles and responsibilities, command relationships, and offensive versus defense cyber operations. Within USPACOM, we found it useful to create a framework to discuss colleagues both within and outside USPACOM and the Pacific. As a result, we came up with this thing called the Cyber Discussion Framework, and as we talk about the organization for defensive cyber, we noted it significantly different than for offensive cyber. This model was also shaped by the direction and words provided by the former USPACOM Commander, Admiral Archie Clemens, who did not want to be told about systems, but instead about capabilities.

Cyber Discussion Framework (Capabilities) – There are two types of capabilities – information capabilities and exploitation capabilities.

- Information Capabilities – includes information warfare and getting information needed to make decisions. This includes provisioning, the building of cyberspace which is a man-made environment, where nothing is free. The provisioning dimension of this is the physical space. Information capabilities also include operations and defense (of what you provisioned)
- Exploitation Capabilities – includes active defense (hit actors before they hit us), and exploitation has been done for years.
- Dimensions of Cyberspace – includes the physical, logical (virtual), and cognitive (mental).

Cyberspace Operations at USPACOM – There are three primary organizations supporting cyberspace operations at USPACOM, to include Communications (J6), Operations (J3), and Intelligence (J2). The Joint Cyber Center at USPACOM fuses these three operations.

- Communications (J6) – is responsible for enabling capacity, empowering users, protecting information, maintaining security, and responding to threats and vulnerabilities.
- Operations (J3) – is responsible for decision making, executing command and control, and assessing impacts to the force.
- Intelligence (J2) – is responsible for assessing adversary information gains, assessing threats and vectors, and assessing adversary vulnerabilities. The J2 is focused on both friendly and adversary loops, and relays information to the J3/J6 as to what could be exploiting us to defend against, and if the adversary has information they should not have obtained.
- Joint Cyber Center / Plans (J5) – plans cyber operations and makes sure we have the resources and forces ready to go for future operations connected to operational and contingency plans.

Activities (J6 CIO) to Provide and Improve Information Capability – There are many activities the USPACOM J6 CIO is responsible for in providing and improving information capability, to include:

- Enabling the Workforce – includes user training and educations; and information worker professional development
- Delivering Services (System Management / System Design Life Cycle) – includes operations, administration, and maintenance; project management and implementation; architecture and planning; and removal and disposition
- Providing Technologies
- Managing Capabilities, Requirements, and Resources – includes strategic vision, oversight and leadership; information resource policy management; and research, development, and technology insertion
- Assuring the Missions – includes information capability mission assurance and cyberspace security management
- Empowering Users and Partners – includes collaboration, knowledge and information content management; and process improvement

Joint Information Environment (JIE) – The impetus and driver for the Joint Information Environment (JIE) came from the Joint Chiefs of Staff / Secretary of Defense who stated the need to improve our information systems to deliver better, improved effectiveness, improved security, and improved efficiencies. Key objectives are:

- Improved mission effectiveness and operational flexibility
- Increased cyber security
- IT efficiencies and joint information services

The JIE Increment 2 converges NIPRNET, SIPRNET, and CENTRIXS into a single information infrastructure for the warfighter. The vision is to take all these networks and put into a single network, and secure domains of a single workstation separated by different windows. Within the Navy, JIE has been integrated into the Next Generation Enterprise System (NGEN) and Consolidated Afloat Networks and Enterprise Services (CANES) programs of record. In theory, JIE takes the people, and community of interest, and gets them into the same information environments. To enable security, the Virtual Service Enclave (VSE) is used for trusted networks and IPSec Virtual Private Network (VPN) in an untrusted network.

Mr. Jeff Johnson provided an overview of the Naval District Washington and NAVFAC Washington Smart Grid (Smart Shore) program. Highlights of his presentation included:

- Naval District Washington (NDW) has a large footprint in Washington DC, Maryland, and Virginia, with the National Capital Region heavily focused on R&D activities
- In Fiscal Year 2012, NDW became the Smart Grid / Smart Shore site with an active infrastructure and marching orders to transition existing micro grids and smart grid. This effort is a combination of smart grid operations and cyber security for industrial control systems (ICS) across control systems, radio systems, and utility systems.

NDW Smart Grid / Smart Shore Approach and Architecture

- The heart and center of NDW Smart Grid / Smart Shore approach and architecture is the Secure Accredited Platform (SAP), with Industrial Control Systems (ICS) put into a protective enclave
- Command and Control systems include command centers and operational technologies to ensure enhanced public safety
- Advanced Metering Infrastructure (AMI) expands the enclave to include metering systems so we can leverage the infrastructure for the Anti-Terrorism Force Protection (ATFP)
- One of the objectives is to commission electric / energy cost savings in command buildings, reducing energy use and reduced energy cost
- Smart Shore is an integrated C2 system, with integrated networks and operational technologies that is now funded using savings from mission support and repair activities.

Navy Public Safety Network (Shore Operations Backbone)

While the Navy developed NMCI for its business system, it developed a separate network for its operational technologies and systems, and C2 system. The original reason was to provide support for regional dispatch centers and C2. DISA did not have this capability, so it was decided to establish both an NMCI and Public Safety Network (PSN). PSN serves as the Shore Operations Backbone and consists of the following components:

- Shore Sensor Systems Platform (SSP) Local Area Network (LAN) that connects each enclave at each host site, to include access control systems, camera systems, video analytics systems, etc.
- Outside of this enclave are other closed system enclaves that are connected to it that does not require LAN connectivity, such as Enterprise Local Mobile Radio (ELMR) and Navy Emergency Management Response System (NERMS).
- In addition to SSSP, the PSN includes the PSNet "Closed" Architecture for dispatch, and a PSNet "Open" Architecture for Emergency Management (this is open to the close side solution to allow access to business systems)

Naval District Washington Smart Grid Architecture – Figure 4, below, provides a systems architectural view of the NDW Smart Grid Architecture. The Navy has taken a hardware based approach to segregate the middleware panel, where the cyber risk is blocked. All communications occur in IPSEC tunnels such as the Virtual Secure Enclave (VSE). Network traffic is encrypted, and there is both wired and wireless intrusion

protection. Command and Control occurs at the regional level, and locally deployed using private clouds and servers. Regional Operations Centers (ROCs) are connected to Shore Operations Center (ShOC).

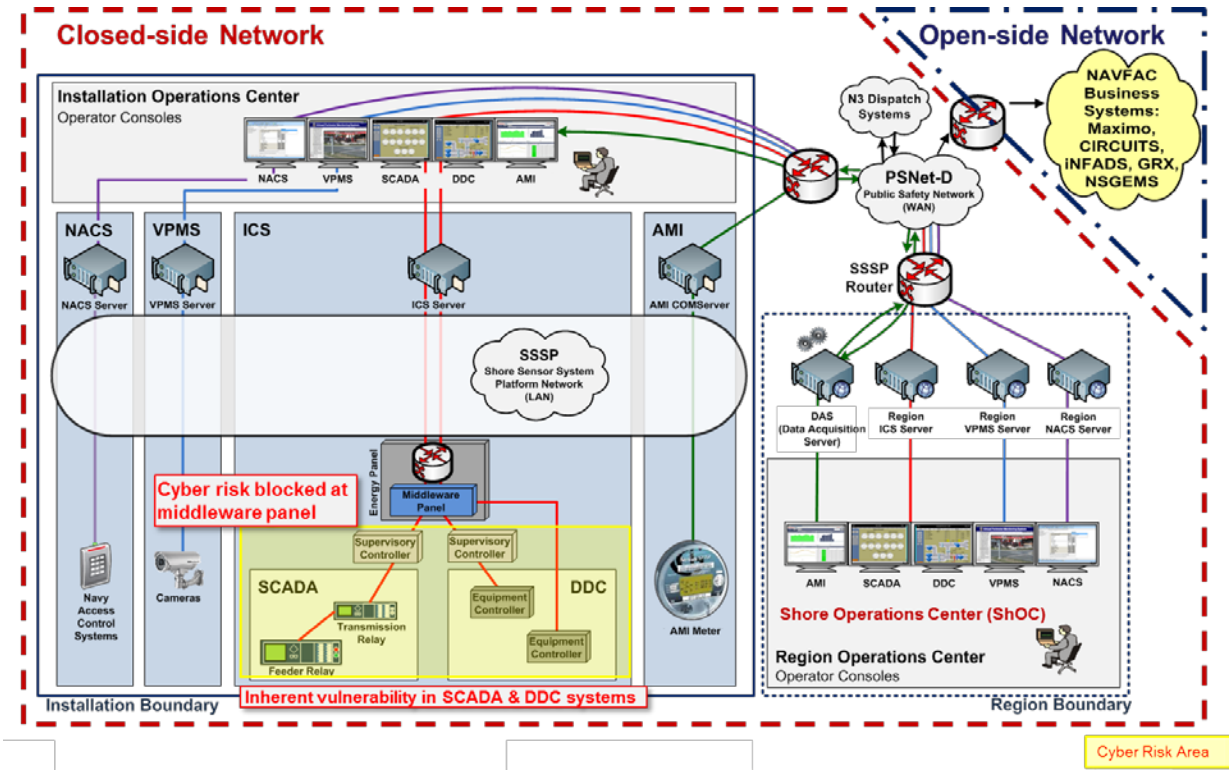

Figure 4 – NDW Smart Grid Architecture

NDW Smart Grid – ICS Cyber/IA Security Risks – The Navy, and NDW, identified the risks and developed mitigations (in place) for Physical Security, Network Security, and ICS Operations.

- Physical Security – most ICS are located in mechanical and electrical rooms that are not typically accessed control. While they are typically locked, the rooms typically possess no ability to monitor personnel access. Given the operational nature of ICS and the networks that connect to them, unauthorized physical access provides an entry point for malicious attacks and is deemed high risk.
- Network Security – ineffectively implemented networks environments may result in an ICS environment that does not meet DoD-mandated Information Assurance standards. NSA, with support from other government agencies and ICS subject matter expert, conducted an assessment and reported on ICS devices we connected to the Internet.
- ICS Operations – a reasonable balance of ICS operational and Information Assurance risks must be achieved to ensure the most effective operational capability. ICS operational technologies exist in their native environment, and many cannot be hardened (this is where a modern C2 piece and middleware panel, which is connected to the Internet, can block cyber risks). One of the operational changes that has taken place is ICS maintenance and programming occurring from command centers with day access to mechanical rooms, and all programming being conducted under government oversight).

Additional information on risks and mitigations are included in Mr. Johnson's briefing slides, as well as other information about the NDW Smart Grid program, which has been made available to conference participants.

Mr. Ross Roley provided an overview of the Joint Innovation Experimentation Division, and its focus on micro grid, operational energy, and wind energy experimentation, one program of which is the Smart Power Infrastructure Demonstrations for Energy Reliability and Security (SPIDERS). Highlights of his presentation include:

- USPACOM serves as the Operational Manager for Phase I and III of SPIDER.
- One of the primary objectives of SPIDER includes replacing and automating back-up generation of critical infrastructure, in this case developing the smart grid (micro grid), and to make them more secure (cyber security).
- One of the first demonstrations of this capability occurred at Fort Carson, where a smart micro grid, and electrical vehicles requiring two-way charging in emergencies for continued operations, was successfully demonstrated. This was an initial validation of the micro grid, and how it needs to be synchronized with utilities to have stability, under the SPIDERS program.
- In 2008, the first installation-wide micro grid in the DoD occurred on Hickam Air Force Base, based in large part of Defense Science Board finding that the majority of power to DoD comes from off-base utilities, and that these utilities are potential single points of failure. One of the recommendations was to take immediate steps to "island the installation," and as a result, Hickam AFB became the first instantiation of "an island in DoD." The installation of the micro grid on Hickam AFB also enabled the DoD to obtain a return on its investment, as it could now work with the Hawaiian Electric Company (HECO) representatives on their ability to reduce and share electricity generated on Hickam AFB, and receive payment from providing this electricity. The micro grid also enabled mission assurance back-up generation, an estimated 25x increase in reliability, and provides weeks of back-up operations capability (as opposed to 72 hours).
- As each phase progresses, there will be cyber security best practices and red team assessments for enhanced micro grid cyber security. The micro grid is a "transformation concept" that is going to positively affect the electrical industry, so we wanted to build cyber security in the front.
- Another of the primary objectives of SPIDER is Cyber Experimentation with the overall scheme of how cyber security is built into the micro grid (this is a complicated thing).
- Sandia National Laboratory (SNL) developed the reference architecture and framework for Micro Grid Cyber Security.
- USPACOM will conduct red team experimentation, and Pacific Northwest National Laboratory (PNNL) will conduct independent tests, at each phase of the operational demonstrations.
- Naval Facilities Command (NAVFAC) Port Hueneme has been given the responsibility to transition this system and capability to the rest of the Services, in order that they can build similar micro grids on their installations.
- One of the primary governing documents for this effort is the Uniform Facilities Criteria (UFC), which is currently underway at Port Hueneme. NDW is an example of its implementation at other military establishments, under the NDW Smart Grid initiative.

- Of substantive interest and excitement is PNNL effort to do similar things on the civilian side to make sure the lessons learned can be translated across the country with other utilities, making the entire ecosystem of micro grids more capable and resilient.
- Our way ahead and approach includes ten events, seven of which have been completed. USPACOM has responsibility for five (completed), and PNNL for three, of the ten events.
- The Virtual Secure Enclave (VSE) concept, developed by USPACOM J8, has been applied to Industrial Control Systems and demonstrated at the Idaho National Laboratory Test Bed following the Aurora threat, which proved that VSE could work in an ICS environment.
- The SPIDERS team also took a SNL designed experiment that look at "enclaving access and compliance" and observe the interactions of three variables (confidentiality, integrity, and availability" at each data exchange, and that included development of a scoring methodology. This information was aggregated into a single vector to show notionally what a given cyber security posture looked like under attack.
- The USPACOM J8 Vulnerability Branch (San Antonio), Army Research Laboratory, and SNL Red Teams also cooperated on the first actual red team attack on an operational micro grid (under strict rules of engagement) at Hickam AFB in order to convince NAVFAC that the Services should proceed on a similar path forward. These ROE included the concept of do no harm, the electrical control elements are to be off limits, the networks are to be off limits, and no Denial of Service attacks.
- A more recent cyber experiment occurred in Boulder, CO at the Intelligent Power and Energy Research Center Cyber Laboratory that involved a smart micro grid controller (actual hardware in the loop). The experiment involved running generators and real micro grid controllers to add to the operational relevance of the experiment, and this experiment also used the previously developed CIA scoring methodology.
- The SPIDERS team most recent experiments involved taking the live micro grid at Fort Carson, and then conducting live micro grid experiments at Boulder and Fort Carson.
- However, there are some impediments to fully implementing the SPIDERS vision when it comes to Cyber Secure Industrial Control Systems at DoD Bases.
    - Ownership – right now, nobody wants to take ownership of the ICS Handbook, and much of this has to do with the conflict between Information and Operational Technology.
    - Lack of Awareness – there is currently no way to tell if ICSs are under attack. In an actual test conducted at NAVFAC, there were significant attacks on the micro grids, but ICS operators were not aware of attacks (as they were not monitoring the ICS nor had the tools to do so).
    - Priority of Funding – DOE, DoD, and DHS have pumped over $9 million dollars to date, and follow on efforts will soon have to show a return on investment. The value of energy security is hard to quantify.
    - Resources – as stated by USMC General Smith, vision without resources is a hallucination.
    - Classification – of the three departments, the DOE, DHS, and DoD, the DoD has a propensity to classify everything. If it is in the gray area, lean towards unclassified (as MG Davis emphasized in his presentation). This information, if unclassified, can now be more readily available to the utilities.

Col William Hutchinson, U.S. Cyber Command (Panel Member)

Col William Hutchinson provided an overview U.S. Cyber Command responsibilities and initiatives involving ICS Cyber Security within the Department of Defense. Highlights of his presentation included:

- USCYBERCOM has a responsibility to develop Cyber Security systems, processes, and tactics, techniques, and procedures (TTP) for DoD ICS.
- Within DoD, there is a list of 2000 crown jewels (critical infrastructure and key resources) that we need to keep up and running for global operations.
- USCYBERCOM developed a concept of operations for our Cyber Mission Forces (CMF), but it was rather thin. Need to get a better understanding on how to organize, what weapons we have and need, and then how to use those weapons. Once we figure that out, then we are better positioned to figure out what type of cyber training we can defend.
- How big a force do we actually need to do cyber defense and associated training? Is it based on the number of machines, or how connected they are? Something we need to solve.
- We also need to know within CYBERCOM how to do Cyber Defend. The 2000 crown jewels better clarifies on where each is on the Cyber Security curve, and what level of preparedness they are at. This led to the development of an assessment process and model called JBASICS, which is focused on the ICS environment side. This provides a comprehensive view, not just technical, resources, personnel, what tools do they use and how they execute those tools – it is about taking a people, process, and technology approach. This assessment will better equip Cyber Protection Teams (CPT) more than past attempts to throw dollars at cyber – this gets to performance based, cost focused metrics and measurements.
- At our MIT/Lincoln Laboratory event, we created a hybrid military and environment similar to Cyber Flag and Guard, with pockets of the DoD community, and the reserve community with substantive experience in the government and industry. An outstanding event, achieved in large part by the use of state of the art network environments and actual simulators (such as those obtained from SNL). Similar events occurred at APL/John Hopkins, where the lead team got the network up quickly.
- However, if there was a critical asset in Washington DC that faced an imminent risk of attack, if we did dispatch a CPT, what would they do? There is no full CPT in existence, only a smaller CPT prototype blended into a squadron (similar to a Delta Team/SEAL Team construct). How quickly could they convert a relatively insecure network into one that is hardened, under stress from an adversary?
- Our next phase was to simulate an attack from a medium level threat, and while the advanced persistent threat did not replicate a nation state, we did work a medium, advanced level threat. In this event, we did not have access to "the crime report," but only the information needed to create a baseline from which to build upon. We created a checklist to know if we could go into battle; this check list had an operational framework borrowed by the Cyber Security Framework. Tried to capture SME from participants and then put it into a piece of paper so we did not have to relearn. Standardization of performance was created.
- This past September we conducted four events in Boston. The first modeled the Lincoln Lab environment at MIT, where we worked with network staff, operators, and monitors and then built avatars. Conducted an assessment, modeling the environment. We tried to assess whether or not we had sufficient resources, or redundant routers and other devices. We also wanted to assess if common tools out there provide only moderate increments to security over what you can get from open source.

- Finally, at another MIT event, and with a full reserve contingent, we tried to highlight the daunting nature of the 1000's of IT systems that our teams may encounter. Moving away from the IT to the warrior approach, our team prioritized and sought to better understand the key terrain and the crown jewels. From a mission assurance perspective, there were three Tiers developed to guide team activities:
    - Tier 1 – 100% running all the time, immediate impact on missions
    - Tier 2 – entities over time have severe impact on mission privacy information and intellectual property
    - Tier 3 – operations ignored, other 90%, over time creates an unhealthy environment
- If you are assigning forces, you need to know the key terrain.

PANEL 3 – CYBER INTELLIGENCE

LTC Michael Smith, Commander, National Capital Region IO Center (Moderator)
Dr. Ernest Hampson, Technical Director, Cyber Intelligence/Counter Intelligence, Battelle Memorial Institute (Panel Member)
COL Drew Ryan, Cyber Integration Lead, Military Intelligence Readiness Command (Panel Member)
Mr. Elijah Owen, Senior Analyst for Security and Threat Assessments, California Governor's Office of Emergency Services (State Threat Assessment Center) (Panel Member)
Mr. Douglas Raymond, Vice President, Endgame Inc (Panel Member)

Dr. Ernest Hampson, Technical Director, Cyber Intelligence/Counter Intelligence, Battelle Memorial Institute (Panel Member)

Dr. Ernest Hampson developed a scenario that included a logical sequence of steps a potential cyber terrorist group might take in conducting a cyber attack against a critical infrastructure in the U.S., a dam. Dr. Hampson Highlights of his presentation included:

- What was the possibility of a terrorist attack? We talk about cyber terrorism, a debate on whether there could be a true terrorist attack through cyberspace.
- Thinking has changed, so I sought to instruct leadership through a plausible scenario of a cyberterrorist attack by looking at a mass casualty incident caused solely through cyberspace.
- The process began by looking for a mass casualty incident solely through cyberspace. Based on actual events, the event that occurred ruled out cyber as the root cause; however, there were cyber factors that led to the disaster. Additionally, in 2002, Al Qaeda was noted looking at dams in the U.S. that possibly could be used in a cyber attack. This provided the baseline scenario... what could we do to a dam with the criteria that this had to be a mass casualty event (creating an attack that would create mas casualty). Opening the flood gates that we could control through cyber events would not create this mass casualty event as they could be closed; instead, taking down the dam itself (uncontrolled release) would create this mass casualty event, and an earthen/rock fill dam (pump storage reservoir) was considered the most vulnerable.
- Despite claims to the contrary by the dam's CIO, the dam's control systems were indeed accessible through the internet. The intent was taking control of the pump in a pump stage reservoir and enable those pumps to keep pumping and overflow the dam.

- Activities taken to get the requisite information to conduct this cyber attack and associated mass casualty included:
    - obtaining detailed maps from the National Inventory of Dams (its help menu provided back door to search engine on web site)
    - researching the internet for information on the actual pump-storage dam, noting it had a long history of leaks, and finding out that information about the operational control network for the facility, dispatch center and the fact that it had limited monitors for operations, and details on its operational control site (where all operations and maintenance was conducted) and how very little monitoring and operations capability were actually there
    - researching the internet to identify job sites who were hiring, and then determining what SCADA software and Programmable Logic Controllers (PLC) were being used
    - identifying that their operational control sites were connected to their corporate WAN, obtaining critical information and actual blue prints of the pump storage reservoir
    - identifying that the pump storage facility was unmanned at night, no cameras were on site, and that there was no hardware backups at the dam
- With information in hand, the attack scenario was developed, which included disengaging monitors on the pumps that noted actual reservoir levels which enabled them to keep filling the reservoir even as it overflowed (undetected), destroying the dam, and spilling one billion gallons of water that destroyed (conceptually) the national park at its base.
- While this event was fictional, the actual dam involved was the Taum Sauk Dam located in Southern Missouri, whose hydroelectric power station failed on December 14, 2005 (off season) and that destroyed the national park at its base. The ability to conduct a cyber attack of this nature is well within the scope of a dedicated, skilled cyber terrorist, as was shown as the scenario developed.

COL Drew Ryan, Cyber Integration Lead, Military Intelligence Readiness Command (Panel Member)

COL Drew provided an overview of Military Intelligence Readiness Command (MIRC), and their role (as well as the U.S. Army Reserve and Army National Guard) in providing intelligence support to cyberspace operations. Highlights of his remarks include:

- As the Cyber Integration Lead, I am responsible for serving as the integration lead for the MIRC, a six-thousand man command, in support of their mission to provide intelligence support to cyberspace military operations.
- The MIRC provides tactical intelligence to support national agencies, providing uniquely qualified soldiers that are "employed at their civilian day jobs" to these same agencies.
- MIRC soldiers' support of U.S. Army Cyber Command/U.S. Cyber Command enables these commands to obtain "deep analytic work" and intelligence support, and serve as a ready cyber intelligence force in warfighting, homeland defense, and other national efforts that are supported by these commands. There are just not enough active forces to do this job, even in this collaborative and teamwork environment.
- The U.S. Army Reserve and Army National Guard bring capacity and capability to the fight (even if they don't have their active duty partner credentialing), and the MIRC has a small piece (important) in this process.

- The MIRC provides intelligence support to Army Cyberspace Operations, with soldiers who possess an impressive depth and breadth of civilian acquired skills.
- The MIRC is definitely having an impact, an example of which included building a human intelligence network in Iraq in a manner in which U.S. law enforcement would establish a "snitch network." This was an instantiation of how one's civilian job (in this case law enforcement) melds well with the military obtained skill sets of the reserves and the national guard.
- The MIRC provides three types of intelligence support to cyberspace operations:
    - All-Source Intelligence Support to Cyberspace Operations – with intelligence analysis being the primary component
    - Exercise and Training Support – plan and coordinate cyber exercises, especially when their active duty counterparts are in the real fight, and serve in supporting cells, such as the white cell (with Army, Navy, and Air Force reserve and national guard counterparts)
    - Long-Term, Non-Sensitive Target Development – focusing on Tier 3/4 nations such as Sub-Sahara Africa and other nations not covered and/or of current interests by their active duty counterparts, and then providing a baseline of analytic support and development of target packages (which would be readily available if something happened in these countries)

Mr. Douglas Raymond, Vice President, Endgame Inc (Panel Member)

Mr. Douglas Raymond provided an overview of how a small technical company such as Endgame can be part of the solution and problem set in cyberspace. Highlights of his remarks included:

- **Situational Awareness** – Endgames is a unique, small technology company, that like other companies wants to increase their situational awareness of what is going on in cyberspace, figure out who the key actors are (good and bad), and then take some action as required to operate and defend their networks, systems, and databases.
- We are actually part of the problem of the proliferation of devices (tools) out there that are connected to the internet. Google is leading the development of capabilities (new operating system) that allows all your devices, to include your home, to be connected to the internet, and the cloud. This is great from a consumer standpoint, but for the U.S. and our allies, this presents another complication and attack vector surface our adversary can use. We look at this from the perspective of how we can defend against this challenge and advanced persistent cyber threat.
- Small companies can provide the engineers and build technology that provides situational awareness of the devices an adversary could use (or is already using) against us, as a lot of computer science is based on who is connected to what computer device or network.
- **Discovery** – this includes turning data into intelligence and big data. However, with big data, if you cannot make sense of it, it does not lead to actionable intelligence. Our approach (innovation) is taking disparate information and piecing our information with other information sources to produce intelligence. It includes a transition from a focus on signatures to one based on anomaly detection, looking over a longer period of time to detect irregular behavior, which in turns leads to a broader span of innovation (e.g., not attacking a network or making purchases related to technology considered to be important). What systems (e.g., SCADA, iPhones, computer systems, etc.) and

supply chain pieces operating in cyberspace needs to be brought into a common operating picture, and this is both a big data challenge and innovation challenge small companies can address.

- **Taking Action –** the best way small technology companies can contribute to the cyber security problem is just to make better, more secure products, as well as easier to use (intuitive). It is so hard to train people, to find the time, and to resource. We are looking at more junior people to take on more responsibility to defending critical infrastructure, and it is becoming harder to get their confidence in using these tools. We need to make them easier to use (like the ease of use of an IPad) and definitely more secure in their initial design and development.

Mr. Elijah Owen, Senior Analyst for Security and Threat Assessments, California Governor's Office of Emergency Services (State Threat Assessment Center) (Panel Member)

Mr. Elijah Owen provided an overview of State Threat Assessment Center and the need for increased collaboration. Highlights of his remarks include:

- At the 2014 RSA Conference, a key theme was collaboration across the threat intelligence landscape, and identifying the best way to implement collaborative solutions to protect privacy, free speech, individual rights, business concerns, government legislative responsibilities, and how do public-private partnerships work together to create a resilient infrastructure for information sharing and support a variety of data formats. This serves as a backdrop to the State Threat Assessment Center (STAC) mission, vision, and activities.
- The role of the STAC is to advise the CA Governor on all threats to the State of California – all threats, all hazards.
- The STAC notifies all stakeholders across CA (public-private entities) who are also affected by cyber incidents
- One of the cyber intelligence challenges involves identity ways to push information quickly on a cyber incident to organizations for timely action. This is where the state level fusion centers come into play, and there are currently six located throughout the State of California.
- The STAC gets involved in informing organizations when there has been a cyber incident in their organization. STAC has partnered with the California Chief Information Systems Officer (CISO), National Guard, ISAC for Internet Security, and fusion centers across the state to quickly put together the intelligence picture, make notifications, tailor messages, and provide remediation assistance.
- Fusion Centers also network across the country (there are seventy-two centers), and comprise a "cyber working group" that is leveraged by the STAC for strategic tend analysis and establishing a baseline of cyber threats.

Questions / Open Forum Discussion

1. Cyber Security Framework

- Proposed as a solution to Executive Order 13636 – Improving Critical Infrastructure Cyber Security, which includes ICS, SCADA, and Electric Grid
- This framework provides prioritized, repeatable, performance-based and cost-based approach.
- Machine readable indicators can assist with detection and incident response, intelligence threat and information exchanges, and also supports DHS

- ICS community has not come to an agreement on adopting Security Technical Information Guides (STIGs)

2. Information Sharing Standards and Challenges

- If we reduce the friction from information sharing, we can react faster
- One of industry's challenge is getting some indication of a threat (signature trigger), but not enough information (intelligence) to generate an action requiring outside assistance. If there was better information sharing, they could translate that threat signature into some type of risk involved, and then take action
- Information sharing is a key factor (goal) in increasing the cost of an attack (by an adversary) and decreasing the cost to defend against this threat
- We need to remove the stigma associated with organizations reporting a cyber incident, and personal relationships are important to facilitate the sharing of cyber incidents by industry to government organizations
- Intelligence and information sharing needs to be both predictive and proactive

DISTINGUISHED GUEST SPEAKER – CYBER ANALOGIES

Dr. John Arquilla, Director, Professor and Chair, Department of Defense Analysis, Naval Postgraduate School

Dr. John Arquilla provided highlights of the work he, and his colleagues, did under an NSA sponsored Cyber Analogies project.

Analogies – Analogies help us think through complex things to find our way forward, and what endures and what changes, and no analogy is perfect. They do help us, however, to think better about the problems that face us. In standing on the edge of the largest wilderness in the world, the Pacific Ocean, it was not hard to perceive that our world was 70% covered by water, but even with all the technology we have today, there is little understanding on what lies beneath the surface.

Cyberspace Wilderness – Cyberspace is a vast, artificial, ever-expanding wilderness...beautiful yet dangerous. The rangers in that wilderness are those that try to bring order and security to it...and protection of individuals, organizations, and national and internal security. Within this wilderness are terrorist networks, despite our efforts. One of the challenges in this wilderness is sharing information to bring greater order to this vast wilderness. We need to be willing to consider all different sorts of analogies that may apply in the cyber realm, to include the most advanced technologies and newest sorts of social interactions.

Cyber Analogies – General Alexander approached the Naval Postgraduate School (Dr. Rothstein) on exploring the notion of an analogy project which became the Cyber Analogies Project, and to try to think through the issues of cyber security and cyber warfare through that lens...how we are using analogies and how we might be able to improve our understanding and powers of thought. Two years ago, General Alexander stated something that should chill us all...that using a scale of 1-10, he rated U.S. Cyber Security a 3 and that every day, there is a level of death in America intellectual capital that is unparalleled in history. The General asked

NPS if they could do something to help us think more deeply about this and use cyber analogies to think through some of these problems. This project provided an exceptional opportunity to mine those people and expertise (we don't need to make everyone cyber experts as there is a great deal of expertise out among the 300 million people in the U.S. already). Consider the model of the militia in the early republic, a small active force and large militia protected us then...imagine a Cyber Militia protecting us now in the Cyberspace wilderness.

Cyber Analogies Theme 1 (Strategic Warfare) – there is tacit recognition that cyber warfare is another form of strategic warfare with no standing army, but instead with cyber forces (or fugitives) fighting with 1's and 0's. There is the notion of strategic attack and its use by us, but the threat posed by this kind of attack by others is the focus of this project, and is discussed in great depth in the book, "Strategic Warfare in Cyberspace." My concern with this air power analogy is that in the discourse, we have neglected close support interdiction capabilities of airpower...they don't get as much attention. When you use this analogy of strategic attack and parallel that with airpower, and when looking at the 100 or so strategic bombing campaigns over the past century, you can count on one hand the number of successes. When looking on how aircraft at the tactical level changed warfare "profoundly," with close air support and Germany's blitzkrieg as examples, we need to look at this tactical view when it comes to cyber warfare. Cyber warfare at the tactical and field operations level was clearly demonstrated by Russia in 2008 in its war with Georgia, as they skillfully blended field operations with simultaneous cyber attacks that had an absolutely crippling effect. In discussions with the Georgia Minister of Defense, the minister shared details of this cyber attack and stated that a lot of their systems were provided by the United States, which made this particularly troubling. This requires us to conduct a very careful study on this attack at the very strategic level of cyber, as well as the close air support level (the Georgia effects were crippling). In using a nuclear power analogy, it did not take long for cyber to become a "weapon of mass disruption," with huge costs (9/11 cost the insurance companies an estimated $40B, while commercial companies currently pay $40B a year on cyber initiatives). An adversary, who puts in a concerted campaign, with a nasty disruptive virus let loose every week for six months, would be economically devastating and definitely a "mass disruption." Additionally, while nuclear weapons create mass destruction in a small area, cyber weapons can create mass disruption effects across an entire society, across the U.S., and the world with effects that are not very well predictable. There is much debate on the longer term effects of that, not much different than the nuclear debate. In continuing the nuclear analogy, it takes an ICBM to deliver its effect on the U.S., and as this puts significant pressure on our command and control, pre-delegated authority has been given to our strategic nuclear forces (e.g., nuclear submarine force). With cyber warfare, launched at the speed of light, we need consider the level of national command authority that is pre-delegated to our forces.

Cyber Analogies Theme 2 (Cyber Pearl Harbor) – using this analogy, we are talking about a surprise attack, which is a big concern and what cyber is all about. In this analogy, you don't see armies massing, or a huge number of electrons, or indicators and warnings of attacks. In the "Cyber Analogies" book, there are three chapters specifically referencing this analogy. Whoever launched Stuxnet launched a surprise attack, and surprise will always be a central element of cyber warfare with very little indications and warning. An author in one of these chapters suggested to look at the very high, strategic level under high tension of strategic parties, take this down to look at what our vulnerabilities would be with the attack profiles and capabilities of this "cyber order of battle."

Cyber Analogies Theme 3 (Economic Warfare) – in this analogy, the principal concept is if we disrupt the trade of our enemies, we bring them to their knees. In the Guns of August, Britain tried the same concept against Germany, only to quickly find out that not only did this not work, it created a self-inflicted wound, and Britain was forced to call this off in a month. The same can be seen in strategic cyber warfare in the context of economic warfare, where we go beyond "controllability of its effects" and where collateral damage is done against ourselves and our allies. We are playing "Armageddon" if we try to bring down an enemy's economic systems. If one wants to disrupt the entire cyber system, you do not have to be the "top sea power of the world" or "leading economic power." You can be a small terrorist group or nation state.

Cyber Analogies Theme 4 (Silicon Valley) – in this analogy, how did Silicon Valley become the mecca for advanced technology, human capital, and new cultural organizations? In Silicon Valley, even though we have a competitive society, there was a lot of sharing of ideas and best practices, and where the local cafes became hot spots for discussing and bringing ideas to venture capitalists. Does our institutional culture foster something like this with cyberspace, and in creating a "strategic thought culture" and concept of "culture of innovation?" I contend this serves as a blueprints, and this is where the incorporation of the active, reserve, and national guard components provides an openness to fresh perspectives (many here are from the Silicon Valley).

Questions / Open Forum Discussion

1. What are Reservist opportunities to take NPS Cyber Courses?

- Need agility and flexibility, as most programs at NPS are eighteen months long.
- NPS seminars have been provided to the State Department and other government organizations
- Suggest shorter, 2-3 month courses as potential ways to get NPS education
- There are six departments that can provide these seminars and courses

2. Do we need to suffer an "empirical experience" to get where we are needed?

- Hope our experiences do not have to be too terrible, and hope that it is someone else's experience that we can observe and learn from.
- The Russia-Georgia experience is a good experience to study hard – if that happened to us, that would be catastrophically disruptive

3. Do we need to look at analogies from a "Non-Western" viewpoint?

- Terrific idea, and we have looked at Chinese views (Chinese military affairs)
- Mao's "peoples war" philosophy is relevant to what we already see in cyberspace
- We have also seen, however, current Chinese thinking being a derivative of Western thought
- We also need to determine the intent of the adversary to use cyber, but this is becoming harder as everyone seems to be entering the game

PANEL 4 – U.S. ROLES, RESPONSIBILITIES, AND CAPABILITIES (RESERVE COMPONENT AND NATIONAL GUARD)

LTC Michael Smith, Commander, National Capital Region IO Center (Moderator)
MG Darryll Wong, Hawaii Adjutant General (Panel Member)
BG Gabriel Troiano, Commanding General, Military Intelligence Readiness Command (Panel Member)
Col William Hutchinson, U.S. Air Force Reserves (Panel Member)
Col Mark DiTrolio, Commander, Army Reserve Cyber Operations Group (Panel Member)
LTC Kelly Greenhaw, Chief Cyber Planner, Joint Force Headquarters of California (Member)

Col Mark DiTrolio, Commander, Army Reserve Cyber Operations Group (Panel Member)

Col Mark DiTrolio provided an overview of U.S. Army Reserve Cyber Operations organizations and Cyber Protection Team (CPT) transitions. Highlights of his panel remarks include:

- There are a number of elements in the U.S. Army Reserve that have cyber capabilities, or play in Cyber.
- The FY14 U.S. Army Cyber Mission Forces consists of five battalions that today are set up in a Mission Support Team structure within the ARCOG, but that is in the process of transitioning to a Cyber Protection Team (CPT) structure. The Cyber X-Games is directly tied to that transition.
- There will be a total of ten CPTs (2 CPTs per battalion), each CPT of which will have an estimated 78 reservists (39 manned), and will be leveraging the CYBERCOM/ARCYBER structure.
- Each CPT will consist of a Command Element, as well as a Cyber Readiness Team (White Team), Support Team (Green Team), Mission Protection Team (Blue Team), Counter-Infiltration Team (Hunt Team), and Threat Emulation Team (Red Team). Warrant Officers comprise the bulk of the manpower.
- ARCOG's proposed mission is to support ARCYBER and 2nd Army by planning, coordinating, integrating, synchronizing, directing, and conducting network operations; conducting cyberspace operations in support of unified land operations to ensure U.S. and Allied freedom of action in cyberspace; and denying the same to our adversaries.
- ARCOG locations are spread out geographically within the U.S., with its headquarters in Washington DC, with 18 locations comprising the National Capital Region, Northeast, North Central, Southwest, and Western IO Centers. These locations are spread to attract cyber talent where it is understood, and to limit the travel of reservists to their assigned locations.
- When you look at the cyber talent in government and industry sectors, that is what you will find in the ARCOG with its cyber talent, to include numerous professional certifications (many NSA certifications), various government (NSA, Joint, DC3 DCITA) courses, and other professional certifications (such as CCNA, CCNP, and PMP). Collectively, ARCOG has a deep bench of soldiers with IT knowledge and professional experiences, as well as strong academic, inter-agency, and corporate relationships.
- The ARCOG's training concept includes individual training (baseline skill sets); small team (sub-team) training, CPT training (collective training and exercises, where senior leadership brings it all together), and military unit training (where emphasis is placed on technical expertise over rank).

- ARCOG had a busy cyber exercise schedule in FY14, to include Cyber Flag (USCYBERCOM), USCC ICS SCADA (Project C), ARCOG Cyber Avenger, Army CIO G6 Insider Threat Project, Terminal Fury (PACOM), Cyber Guard (CYBERCOM), Austere Challenge (EUCOM), Global Thunder (STRATCOM), NSA Cyber Defense Exercise, and Cyber Endeavour 2014.
- ARCOG also supported Cyber Security Community Outreach/STEM programs such as Cyber Patriot, maintains a number of public-private partnerships with leading academic organizations, mobilized and deployed a 22 soldier team continuously (every nine months) to SWCC/RCERT-SWA Kuwait, and supported multiple DoD/Joint/Army organizations on a continuous basis.

LTC Kelly Greenhaw, Chief Cyber Planner, Joint Force Headquarters of California (Member)

LTC Kelly Greenhaw provided an overview of California Military Department Cyber initiatives, capabilities, and activities. Highlights of his panel remarks include:

- Cyber is complicated with multiple titles and authorities to include Title 10 (Military Operations), Title 18 (Law Enforcement), Title 32 (National Guard), and Title 50 (Intelligence)
- The California National Guard, under its Title 32 authorities, is the federal nexus within California and is deployable to the Governor and The Adjutant General (TAG) during state emergencies and deployment within the state.
- The California National Guard conducts Defensive Cyber Operations only.
- The Adjutant Generals vision includes serving as the leader in cybersecurity within the State of California and as the DoD's forward presence in the region, implementing the Defense Strategy for Operating in Cyberspace, promoting and facilitating cybersecurity information sharing and analysis, and supporting the development of tactics, techniques, and procedures for use in full-spectrum cyber operations through training cybersecurity forces from other states and territories.
- The California Army National Guard includes the 40th Infantry Division Computer Network Defense Section and Computer Network Defense Teams (CND-T). This is a Blue Team function, responsible for providing comprehensive risk mitigation with a focus on fortifying postures and processes from the "inside-out."
- The California Air National Guard is the 261st Network Warfare Squadron, a USCYBERCOM asset that provides full spectrum cyber operations support, to include Mission Protection (Blue Team), Discovery and Infiltration (Black Team), Cyber Threat Emulation (Red Team), Cyber Readiness (White Team), and Cyber Support (Green Team).
- The California National Guard provides a full range of cyber support activities, and works in concert with other government organizations such as the DHS National Cyber Security Assessment Team (e.g., DHS red teaming and joint penetration testing), and the typical initial service (cyber engagement) is the initial health assessment.
- In the initial health assessment, the California National Guard conducts a vulnerability scan of systems on networks or isolated switches, sweeps several network segments, generates confidential agency reports and briefings, and provides recommendations regarding analyzed network observations.
- The California National Guard also supports incident response under multiple Titles, to include:

    - Federal Support Missions, in which California Military Department Cyber (CMD Cyber) forces support USCYBERCOM/ARCYBER (Title 10) and NSA/ Intelligence Community (Title 50) through the National Bureau.
    - State Support Missions (Title 32) through the Adjutant General (TAG), much of which is grass-roots initiatives and conducted in support of CALOES and State Technical Office.
    - Private Critical Infrastructure Support Missions through various government organizations and national laboratories, to DHS, FBI, and Sandia National Laboratory. Typically, DHS would lead and CNG support these efforts with industry.
- We are sensitive to the environment and our capabilities. If something becomes a significant cyber event, and if we cannot solve and has exercised emergency assistance contact with the State, there is then the option having CNG support USNORTHCOM (Title 10) missions in concert with the Army Reserves, a proven process and success in cyber. This would be the case in a SECDEF named event (e.g., Katrina Hurricane), in which the CNG could support operations to save lives and protect critical infrastructure.
- As Cyber is not an isolated state event, the CNG can work with its TAG and Governor to establish contact and provide (or receive) emergency assistance and support from the other states.

Col William Hutchinson, U.S. Air Force Reserves (Panel Member)

Col William Hutchinson provided insights of his time in USCYBERCOM as a reservist, and an overview on the preparation and sharing or resources in support of CYBERCOM Cyber Flag and Cyber Guard exercises, and other cyber events. Highlights of his remarks include:

- During my tenure at USCYBERCOM, I was responsible for planning a cyber exercise in 4 -5 months (traditionally an 18-24 month evolution). There were no networks to operate on, we were trying to get offensive forces into the mix, and we initially had only four red team members (ended up with 65 members). But despite the short time to plan this exercise, there was a ground swell that ended up creating the 1st Cyber Flag Exercise in support of the Combatant Commands' "defend the nation against a strategic cyber attack against U.S. critical infrastructure and support in their defense."
- In looking at Cyber Flag, how does the Reserve Force support Combatant Commands and their missions? We have simulated air strike packages, and ship transits, but how does cyber support kinetic operations, and how does kinetic support cyber operations? We can take out a primary node, and we know secondary/tertiary paths where we could use pre-planned network sniffers (as an example).
- Over the four month period from November 2011 – February 2012, there was actual indications and warning of a potential cyber attack on the U.S. from a Middle Eastern country, in which USCYBERCOM and USCENTCOM were called upon to prepare a response. Tactical reserve forces (located at Fort Meade) were currently working side by side with NSA to support this mission from within the U.S. However, nobody was talking about what the National Guard would do, or how the Reserves could support?
- This event generated some strategic thinking on conducting an exercise called "Cyber Guard" that would use some of the same forces from Cyber Flag. The proposal was presented to and approved by General Alexander, thus creating an enduring relationship between Fort Meade (USCYBERCOM/NSA)

and our states. Fort Meade would help out states, and the states in turn would provide insights on what is happening in the networks in the states, resulting in the appropriate national response.

- Cyber Guard Exercise planning commenced in April 2012, and executed in July 2012 (4 months). DoD, DHS and FBI were involved in the planning (not without tension over authorities), and the National Guard in the National Capital Region provided teams. A total of 20 teams were available to participate in this event, and during the planning, much of the discussion surrounded the role(s) of the reserve component. Reserves have combined military and government/civilian sector skills that would be needed; they live in the communities that if networks were attacked, they have established relationships with the network owners; and it is easier for them to lend a hand that having a federal official knock on the door. This became a legal policy and not a technical problem, with legal elements considered to ensure this was done properly while preserving civil liberties.
- Another cyber event is "Cyber Wargame" that projects what the cyber environment looks like in the outyears, and fights it, and then identifies gaps and requirements so to make purchases of new tools, and identity the new capabilities and teams needed. This is another perfect opportunity for the reserves, which bridge the military and private sectors (and have a foot into each realm). They have insights into military requirements; they have networks and relationships with the private sector; and they can help expedite the acquisition process in cyber, by assisting in translating classical military requirements into private sector solutions and getting them back into the military side to solve problems faster.
- Another cyber event was "Project C," which involved all-stars from the Washington National Guard and participants from Cyber Guard (which included ARCOG members. To mitigate the exuding confidence, the Red Team (Pittsburg Unit) turned up the heat on the network built by CMU/SEI whose developers had comfortable relationships with the ARCOG. Of the 200-250 folks who participated in the event, the ARCOG's Chief Ortiz achieved recognition as the Cyber Defense Top Defender, an example of the outstanding skills and knowledge the reserves bring to the fight.
- The Cyber Reserve Force provides the military with fresh ideas and innovative ways of solving things, and the private sector obtains critical insights into the military from these reserves resulting in more secure and more relevant technical solutions.

BG Gabriel Troiano, Commanding General, Military Intelligence Readiness Command (Panel Member)

BG Gabriel Troiano (the senior intelligence officer in the U.S. Army Reserves) provided an overview of the roles MIRC performs in terms of Cyber Operations. Highlights of his remarks include:

- MIRC has an estimated 80% of the Army Reserve Intelligence assets.
- Within the MIRC, there are 6,2000 soldiers located between Hawaii and England, and an estimated 800 soldiers worldwide supporting the Geographic Combatant Command in a combat operations or intelligence support capacity.
- MIRC serves as a "Federal Force" to support Combat Support Agencies such as DIA, NSA, CIA and the State Department. They also provide full spectrum intelligence operations, such as SIGINT, IMINT, GEOINT, Counter-Intelligence Battalions...and we also have tactical level battalions who serve as strategic level analysts in "particular fields" fully embedded into national agencies.

- Our Intelligence role in Cyber is important. At the tactical level, it is about killing the enemy. From an intelligence perspective, it is not what we are fighting that moment in time that is important, it is telling him what is coming next. So for the tactical commander, our role is to look at everything going across the spectrum, bring that data in, process it, and get the message back to the decision maker so he can interdict and destroy what possibly could come outside a direct fight.
- With a cyber attack, you are not going to know about it until it actually happens.
- MIRC's function in the cyber realm (intelligence) is a supporting role, and this includes both Offensive and Defensive Cyber Operations. We won't press the buttons, but when there are intelligence requirements coming out – based on gaps – our intelligence assets will be pushed forward to collect that information (intelligence) to fill these requirements.
- Within intelligence, this is a predictive analysis process…you collect information to determine what are the intentions of the bad guys. When looking at the role of intelligence in context of cyber, this is challenging as there are policy issues, as well as the tactical and technical.
- Within the Army, we take the lead from the U.S. and Army Cyber Commands, who have to help me define accurately how I can help them what I need to do to help, and define Army reserves to better support their efforts.
- Unlike the soldier, we are not the "tip of the spear," but instead the "tip of the spoon." We look at long term, threat based requirements areas of concern, and the next hot spot. Thirty years ago it was looking eastward, now it is looking everywhere. The Army Reserves are still developing their roles, and so is the MIRC in terms of policies and authorities. The MIRC is taking on a much larger Army Reserve role, and established an Intelligence Support to Cyber Operations Cell, consisting of eighty four (84) soldiers, that are responsible for conducting planning and all source intelligence support for cyber operations, and for targeting. We build our packages and development of information so that we can pass it to the "tip of the spear."
- The MIRC intelligence force has tremendous civilian skills, and our forces are positioned at the Joint Force Headquarters for Army Cyber Command, within National Support Teams (NST), Cyber Support Teams (CPT), and Intelligence Support Team.
- We build the cyber environment, i.e., Intelligence Preparation of the Battlefield," and conduct assessments supporting offensive and defensive cyber operations. While we cannot go directly to industry for much of the information we need to conduct our intelligence missions in support of cyber, our reservists, many of who work in the Silicon Valley, bring that knowledge to us.

MG Darryll Wong, Hawaii Adjutant General (Panel Member)

Major General Darryll Wong provided an overview of his role as the Adjutant General for the State of Hawaii, a cabinet level position, and how he oversees the training and readiness of the 5,500 soldiers and airmen of the Hawaii National Guard. Major General Wong is also the Director of Emergency Management, provides direct support to the Office of Veterans Services, and is the Homeland Security Advisor to the Governor. The General also shared his insights of some of the unique challenges he faces in supporting an "island ecosystem," and how it all comes together. Highlights of his panel remarks included:

- We talk about national security and defending the industrial grid, but it is important that we bring it "more to the home" as within Hawaii we have the people in both the Federal and State Governments, and one important point...all disasters are local!
- So if we bring it down to a state level, national security is one thing, but how do you manage the day to day to keep everything normal in order to keep government and lives of the people from being disrupted by cyber? How do we continue to let the economy of not only the U.S., but also the economies of each state and companies within that state to continue without this type of cybersecurity?
- As the Homeland Security Advisor, I meet with my Homeland Security counterparts of the 50 states and territories on emergency management matters. I am one of twelve (12) military TAGs serving in this capacity.
- On the military side, the Reserves, National Guard, and Active Duty in Hawaii are struggling on how to integrate force infrastructure and identifying authorities and jurisdictions. In Cyber, there is no way one can stay in their own lane. I recognize I cannot tell the State Government what to do, but at some point, because USPACOM is in the State of Hawaii, there are definite roles that USPACOM needs to talk to State Government.
- Private industry is important too, but does not want to tell the Department of Defense, and is afraid to tell them, about their vulnerabilities or cyber incidents.
- On the Homeland Security side, DoD and DHS are trying to figure out their individual and share roles in cyber, which is not a problem in Hawaii but something we have to further discuss.
- Hawaii is an enclosed system, an ecosystem that requires management and security by everyone. The economy of the state needs it as well, as well as the national security mission the state requires.
- The interdependence of critical infrastructure in Hawaii is more critical due to the many non-redundant systems within the state.
- On the National Guard side, the NG plays at the strategic level. As the Adjutant General, I work with local, state, Federal, and private parties to increase relationships and understanding of one's roles, authorities, and jurisdictions that is not very well understood by the DoD.
- The National Guard can bring this group together to discuss missions or a problem sets that really this room (Cyber Challenge participants) needs to resolve with us, and not just DoD or DHS or the private sector as everyone has a role in it.
- In Hawaii's Fusion Center, there is a strong interaction and play between DHS and local law enforcement (driven by state police).
- While USPACOM controls tons of assets and war wherever it occurs in the Pacific, everything outside their wires and kingdom is the realm of the private and public sector.
- So how can the USPACOM Commander get the information he needs on what is outside his kingdom? It is important for those outside the fence (for example, electric and power companies, utilities, financial institutions, and even mom-and-pop stores) to bring all this information in and analyze/convert it into intelligence...taking care of the problem and analyzing where the problems are originating. Once completed, then tell the USPACOM Commander, as we need to ensure that what is outside the wire does not take down what is inside of the wire, such as cutting off his power or eliminating water supplies.
- Interdependence requires the USPACOM Commander and the Governor to be in lock step, and both in the know, so sharing information in the aggregate is important.

- Hawaii's National Guard is not as well organized and structured as the reserves, or other National Guards such as in California.
- We got some smart folks in our Army and Air National Guard together to build an ad hoc structure, which they patterned after Washington State's National Guard structure. We have also leveraged California for training, and have recently established a Cyber Range at the University of Hawaii to provide a place for Hawaii's National Guard to work, train, and exercise.
- As a Cabinet Member, I got with the Senators and Governor on the need to create a Cyber Czar position, and the mayor, police chief, and others were brought in to testify to the Senate. The legislative branch wanted a Task Force, but this introduced its own problems. In the end, we were able to create legislation to bring onboard a Cyber Czar.
- Within the State of Hawaii, the Governor can either work with the private sector or call up the National Guard and the Reserves (through the DCO).
- As the Adjutant General, it is my job to leverage every organization potentially available, and across the U.S., to collective address and solve the problems facing our state that also houses the U.S. Pacific Command.

PANEL 5 – TRAINING AND EDUCATING THE FORCE

COL Michael Hildreth, Deputy Assistant Commandant, Army National Guard (Moderator/Panel Member)
Dr. Cynthia Irvine, Chair, Cyber Academic Group and Director for the Center for Information Systems Security Studies and Research, Naval Postgraduate School (Panel Member)
SFC Thomas Blackard, Army Reserve Cyber Operations Group (Panel Member)
COL Heather Meeds, National Guard Bureau (Panel Member)

COL Michael Hildreth introduced his panel members, provided a brief overview of his role as the Deputy Assistant Commandant of the Army National Guard, than provided some introductory remarks on the need to train and educate the cyber force.

SFC Thomas Blackard, Army Reserve Cyber Operations Group (Panel Member)

SFC Thomas Blackard, who in his civilian life is employed at iSIGHT Partners Inc, discussed how education and training within industry and the Army Reserves has its similarities, but focused his attentions of his role in supporting Army Reserve Cyber Training and Exercises. Highlights of his panel remarks included:

- Within the Army Reserves, many soldiers based on their civilian jobs and skill sets, would participate on White Teams in support of U.S. Cyber Challenge / National Cyber Olympics, exercises based on Cyber content.
- This led many into the dynamic defense outfit with extensive experience in cyber, with not necessarily the formal accreditations of their active duty counterparts, and then into Cyber Training Teams.

- This expanded the unit brain and eliminated the institutional amnesia the services have...they forgot they were members of a team, a cohesive unit, of which they are part.
- It was important to drive home to leadership that this was a systemic issue within the unit, and that in other fields there were capstone and group exercises, so why not have the same for Cyber? Our folks go to leadership school and will learn "active directory," but why not have them to a signal or cyber based school, or better leverage their government and/or industry enterprise training than just military? Why not place them side by side the vendors who make the systems and tools used in cyberspace?
- Cyber exercises need to be a primary focus of the Army Reserve Cyber Force, as exercises help to make sure things are done correctly, such as planning, threat and incident handling, and leadership.
- As leadership goes to developing their courses of actions and mission analysis, it is all about requirements and effects, and how effects are to be employed.
- In Cyber, repeatability makes portability which makes usability. The more time the person gets to play with it, the better the person gets. Within the Army / Army Reserves, we take our pistols apart until we get it perfect and then go the range. Computer skills are the same; we have a tendency to teach them how to build it, once. Written test do not reinforce these skills, and standards tests does not equate at all to their ability to one day build and defend the network.
- Additionally, there is nobody (really) around to validate these skill sets, and then these "trained soldiers" go to their units. Now is that unit combat effective in cyber mission areas? No, they are not.
- The Master Cyber Training Team (MCTT) goal is to identify items that we can "add into the play." We developed and are using a "Scorebot" to help us achieve our goal. Ninety percent of what we need is already in house. We "repurpose this equipment" for a training event. We have people take apart the system many times, then put it all back together. Why bother getting brand new equipment – not needed at this juncture. It is like a new soldier on a road march, who carries a rubber duck instead of a rifle, which undoubtedly will be lost or dropped or broken. With cyber systems, there are a lot of components that do not need to work up front.
- Many of our folks are not getting the "official certifications," but they are learning the softs skills in certification, or being able to effectively put together a system. Sure, members in their civilian careers participate in cyber mentoring programs, or go to AFCEA events, or take cyber classes – but are they learning troubleshooting? It seems the more you educate, the more problems there are. It is not about taking a class and getting a certificate, it's the ability to take a box of parts and build a computer system, or being able to spot and correct a problem that the "educated person" might not be able to see or do anything about.
- Within the ARCOG, we now have Cyber X-Games, an ICS/SCADA based exercise that involves training over years, which equates to compartmentalizing components to talk together. You don't' need to own the network, need to operate to standards though...so training needs to meet the standards. The bottom line objective is getting the network off the ground, and conducting system administration and troubleshooting. The skills needed are mostly achieved from the reserves' "other job" in government or industry.

Dr. Cynthia Irvine provided a candid assessment on some of the potential reasons that women – which comprise 50% of the workforce – are not involved in cyber programs, and what might help, and an overview of available NPS cyber education and research programs. Highlights of her panel remarks include:

Women are Missing in the Cyber Workforce

- We are missing 50% of the workforce in the cyber workplace. Only 12% of the students in the Scholarship for Service (SFS) program sponsored by the National Science Foundation (NSF) are women, and only 18% of these women were in Computer Science Departments. Additionally, within the U.S., there were three states where not a single woman took the Advanced Placement Computer Science examination. The trends seem to be computer science and cyber specifically, and sends a message when there is an even number of male and female students in Advanced Placement Calculus, one of the foundation areas.
- There are most likely psychological factors for this phenomena to include the "imposter syndrome," that women might think they should not be here and have other self-defeating thoughts; that women and men have different brain wiring not accommodated in class, with men focused on coordinated actions and women focused on communication between the analytical and intuitive; and finally, women's desire to be socially meaningful.

Women in Cyber Competitions

- Cyber is interdisciplinary sport, with competitions heavily participated by men and much less than by women
- During the ACM Intercollegiate Programming Contest, only four women participated, in large part due to the contest being overly aggressive rather than socially constructive, the frequent use of militant terminology, and the abuse women take in elite cyber competitions.
- During a DEFCON cyber competition, the organizers developed and provide cards to women participants to present to the male counterparts, with green cards associated with respectful and mindful behavior, yellow creeper cards for mild infractions, and red creeper cards for major infractions. There were substantively more red and yellow cards handed out than green.

What my help the situation

- One way to help the situation might be to establish separate classes for women, as was the case with Harvey Mudd College who tried this and had success.
- Another way may be for males to have socially meaningful one-on-one mentoring sessions, especially during K-12, and find out what makes them tick or what is their passion.
- Another is to explain the social nature of jobs, and the balance between work and life.

Cyber across the Naval Postgraduate School

- The Computer Science and Electrical & Computing Engineering, and the Cyber Academic Group, are the primary Cyber organizations at NPS, although several other departments are fully involved in Cyber that include Mathematics, Defense Analysis, National Security Affairs, Information Sciences, Graduate School of Business and Public Policy, and Operations Research. These are intended for the Military, in particular the Navy, with openings for Army, Air Force, DoD civilians, and NSF scholarships.

    - The Cyber Academic Group is focused on practical applications and principles, and offers MS Degrees on Cyber Systems and Operations and Applied Cyber Operations
    - The Computer Science Department is focused on foundation principles with an emphasis on software and networked systems, and offers MS Computer Science Degrees with tracks in CND/IA, Cyber, and Cyber Operations
    - The Electrical & Computer Engineering Department is focused on foundation principles with an emphasis on hardware systems, and offers MS Electrical Engineering Degrees with tracks in Security and Cyber, as well as MS Computer Engineering Degrees with a Cyber track
- NPS Cyber Education Programs include over forty cybersecurity and cyber operations courses leading to a Certificate or Graduate Degree, as well as short courses, lectures, and cyber exercises supporting continuing educations, as this is a "lifelong learning process." Sample NPS Courses include:
    - Cyber Wargame: Blue Force Operations / Red Force Operations (2)
    - Cyber Operations in a Contested Environment
    - Information Operations Systems (a classified course)
    - Cyber Mission Planning
    - Cyber Policy and Strategy (a political science course)
    - Network Traffic Analysis
    - Advanced Cyber Vulnerability Assessment (focused on reverse engineering)
    - Advanced Cyber Munitions (a classified course)
- Within the Cyber Academic Group there is a Cyber Battle Lab (CYBL). The laboratory supports both education (teaching) and research, includes configurable and separable virtual networks, and will become a node on the Joint IO Range in the winter of 2015. The laboratory supports NPS cyber classes every quarter and semi-annual Cyber War Games; an annual Cyber Defense Exercise involving the Service Academies, NPS graduate level students, and NSA Red Team; and short term and longitudinal projects.
- NPS is also playing a key role in setting the stage the DARPA Cyber Grand Challenge, which aims to create the first-ever tournament for fully automatic networked defense systems, to include preliminary qualifying events and a series of competitions that eventually have one team emerge and receive a cash prize from DARPA of $2 million.
- NPS faculty possesses substantive subject matter expertise in cyber, and many have authored Cyber books and articles.
- NPS has also received recognition for its Cyber Programs, to include:
    - NSA designated Center of Academic Excellence in Cyber Operations
    - NSA designated Center of Academic Excellence in Information Assurance Education
    - NSA re-designated Center of Academic Excellence in Information Assurance Research
    - CNO designation as Chief of Naval Operations Cyber Center of Excellence

COL Michael Hildreth, Deputy Assistant Commandant, Army National Guard (Moderator/Panel Member)

Col Michael Hildreth provided an overview of the Army National Guard and their role in defending our nation, and an overview of how the Army National Guard will build the enablers to meet Combatant Commanders' needs. Highlights of his panel remarks include:

Building Combatant Commander Enablers

- The Army National Guard focuses on building the enablers to meet Combatant Commander needs, when and where needed, and their ability to have freedom to operate, protect and secure risk and mitigation, and to develop a common operating picture within the cyber operational domain.
- It also includes integrating cyber planning and execution, delivering cyber effects to Commanders objectives, and synchronizing lethal and non-lethal force.
- Cyberspace is where our networks are operational platform, a single secure network. Within the information environment, how does everyone and everything integrate into it to meet the needs of the Combatant Commander?

Cyber Center of Excellence and the Road to 2025

- Training and maintaining forces, education, and leadership development is key to us providing the enablers, so one of the key initiatives the Army National Guard did was to stand up a "Cyber Center of Excellence."
- A major aspect of the CCOE is to train, educate, maintain, and develop world class signal, cyber, and electronic warfare professionals supporting operations at the strategic, operational, and tactical level.
- In today's rapidly changing global operating environment, the DoD and our nation must operate in a more congested, competitive cyber environment space and electromagnetic spectrum. Ultimately the CCOE must enable to Combatant Commanders to seize and maintain the land and cyber domains while also being able to simultaneously denying the adversary from doing the same thing.
- The Army National Guard works with many agencies as we shape the way ahead, to include NSA, DIA, State Department, and ARCYBER for example, and deliver joint capabilities for the warfighter.
- To get to 2025, it is about people and partnerships. We must continue reach out and establish partnerships with industry, services, interagency, academia, and coalition partners. We must build a cyber ready force to ensure training is done to joint accreditations and equivalency standards.
- We also need to build joint, defensible networks; joint (vice stove-piped) information environment; secure situational awareness and C2 of the network; and operational controls of the network.
- Need to take a close look at policy and make some changes to bring us working closer.
- Our focus should be "speed, agility and action" to meet Combatant Commander requirements, something we are instilling in CCOE and Army National Guard as a whole.
- The Army National Guard supports the Adjutant General and Governor of each state and territory, which when put in context to our establishing relationships with the Army Reserve and Army, we need to fully understand how to use the authorities when needed to effective execute our missions.
- How do we build the bench? How do the Army Reserves build the bench? How does the Army build the bench? Then how do we bring this all together to provide capacity to the Army and Combatant Commanders?
- The Army National Guard cannot do it alone, it does not have the capacity, and why people and partnerships are key to our current and future success.

Col Heather Meeds provided an overview of the National Guard and her views on what the states are doing within the cyber world as they lead forward in the education and training of cyber warriors and leaders. Highlights of her panel remarks included:

- There is no one set way to train a cyber warrior, and no one institution that can train the cyber warrior. This requires collaboration amongst multiple organizations
- Within the Guard, we are integrating and coordinating and building relationships to include U.S. Cyber Command, Army Cyber Command and the Cyber Center of Excellence, and are in step with what they are doing.
- We are also in step with TRADOC and their training standards and requirements, and help to fill the gaps and increase throughput. We do that in many ways, to include supporting the Cyber Center or Excellence and getting NSA ADEC Qualifications for the Cyber Planning Teams.
- The Guard is on the tail end of training and equipping, so we have explored ways on how we can educate and train soldiers and still meet Army standards.
- We have a 49 man team with quantified baseline skills; our goal is to keep them engaged until they get some of the key cyber classes, and to retain them to accomplish the Guard's missions in support of the State Governor.
- Within California and Hawaii, it definitely appears the states are good at determining this themselves, however many of the other states are also leaning forward and integrating with DHS, FBI, and NSA, and are out there making these relationships from the ground level.
- They are leaning forward not only to meet the standards of the active component, but also to keep them engaged and honing their skills.
- We have worked with USCYBERCOM< ARCYBER, and Cyber COE, and have already taught TRADOC approved courses for 85% of the CND Teams, and the Active Duty CPTs that have taken classes at the National Guard.
- The "school house," such as the one in Little Rock, Arkansas, does not have the throughput to do this, be we are coming onboard to help the throughput situation and provide this type of training to get this baseline type training.
- Due to this all being new, we work together closely on determining how best to produce CPTs and Cyber Warriors at the Brigade level.
- We are working with CECOM to develop some courses that match the "ADA and ADEC courses at NSA," and many of the interagency organizations in order to develop an accreditation.
- The Guard looks out for many ways to train its soldiers, and then emails others to come in and get some of the same type of training in order to better help the Guard, Service Components, and DoD.
- We are more than just the Professional Education Center (PEC). We have different staffs that have joined with multiple universities in order to develop skills for the cyber warrior, to include a base course, cyber ethics courses, and others. We also send soldiers there for their semester to get graduate credit, as well as developing courses to do the things required for performing the work our soldiers do in the Guard. We have a lot of instructors in academia that we work closely with on how to best train (educate)and mover forward our cyber warriors.

- On relationships, we are strengthening relationships with DHS and FBI, both organizations of which have members in the Guard.
- As the Army is helping the community, the community is now helping the Guard with respect to industry standards. We need to recognize these skills and give credit. It helps with costs, and we retain our members better, as they now are increasing their education and skill sets.
- Regional Training Centers (RTC) bring all these things to the schoolhouse, which is important.
- As for ICS/SCADA training, the Guard has water treatment, water, finance and other critical infrastructure facilities being built in Atterbury, Indiana, with grants...and in concert with the Army Research Laboratory.

GEORGIA/UKRAINE DISCUSSION – ANALYZING BEAR BEHAVIOR IN THE WILD

Mr. John Bumgarner, CTO, U.S. Cyber Consequences Unit

Mr. John Bumgarner then opened the final day of the conference with an "analysis of Russian (Bear) behavior in the wild." In early 2014, Russia invaded the former Soviet Republic of Ukraine, which was the second time in recent history that Russian military forces strayed across an international border. The first time was in August 2008, when Russian forces entered the Republic of South Ossetia and clashed with the Georgian military. In both incidents, Russia used a mixture of traditional military operations and information operations. Highlights of his panel remarks included:

Bear Behavior in Georgia (2nd Attack) (and looking back to Estonia, the 1st Attack)

- When Russia clashed with Georgia, the conflict evolved with the distribution to civilian actors instructions on conducting cyber attacks against certain targets. The principal actors (controllers) went to thousands of forums to recruit people preceding and during military engagements, and they provided them with the instructions they needed to conduct cyber attacks against pre-identified targets of interest (these attacks never waned from the targets).
- When military engagements occurred, the use of botnets and other tools against targets or interest did not stop until Russia and Georgia reached a peace agreement. The attacks included ping attacks and distributed denial of service.
- In looking back to when Russia clashed with Estonia in 2007, when a country knows they are going to be attacked, they put their defenses in. The attacker (Russia) knows about the defenses put into place, switches tactics, and causes the defender (Estonia) to be unprepared for this morphed attack and to subsequently be taken out.
- During the Estonia clash, an estimated half-dozen web sites were set up with IP addresses of controllers in Estonia, but nobody within Estonia was prepared to collect on. The Estonia CERT did not have in place sufficient tools and capability to collect.
- When Estonia asked two years later if they could provide records of the attacks, we were informed they did not have records.

- Georgia controllers were located in Moscow and/or Istanbul. The "internet pipes" in Georgia run through Moscow and Istanbul (Turkey) data centers, and are well known enclaves of Russia cyber criminals who controlled the entire pipe. What controls Georgia put in, their defenses were taken out by those pipe providers.
- Russian controllers were skilled and creatively used cyberspace and social media to their advantage. On the first day of the conflict, an image of then Georgian President Mikhail Saakashvili was uploaded onto several websites, with expressions and poses paralleling that of Adolph Hitler. After substantive analysis, this image was developed in 2006, two years prior to the conflict and with a date stamp tied to another Russian attempt to oust the Georgian President.
- There were many factors that precipitated this event, but from a historical perspective Georgia and Russia have always had issues that date back to the Persian Empire. When Georgia became an independent state, it had 6% of the proven natural gas reserves in the world. U.S. and Britain (British Petroleum) developed the pipeline that runs through the Caspian Sea and Turkey. In 2006, when the pipeline became operational in Georgia, Russia pipelines (and market) could not compete and in essence now had to address what they perceived "the U.S. and Georgia undercutting their market."
- During that conflict, Russia would never bomb the pipeline for environmental damage; however, an insurgent (terrorist) group that never operated in Turkey decided to place satchel charges inside Turkey to know out the pipeline. Georgia then took natural gas across the country by rail, and at a strategic chokepoint (rail bridge), someone then blows that up.

Bear Behavior in Ukraine (3rd Attack)

- Following the collapse of the Soviet Union, NATO soon went to work on bringing Ukraine in as a member, and action that did not stand well with Russia still smarting over the role the U.S. played in this matter, and who then 'flaunted with arrogance at times."
- When Russia came across the border (this was not claimed to be an invasion), special operations forces were involved but with no insignia and the expected denial by Russia that their troops were involved. I came across a French TV station noted guys in civilian clothes running through the streets with very unique arm bands and even more interesting weapons, sophisticated weapons later discovered used by Russian Spetsnaz (Special Forces). As for Russian vehicles, they were the legacy tanks and trucks that would supposedly not be associated to Russia (directly). So while this was "an invasion," it could not be 100% be associated with a "Russian invasion."
- In trying to get an accurate picture of what was going on within the cyber realm, I used harvesting tools to get information about the actors and activities that were running in parallel. In a short period, and by using these harvesting tools, I got six million hits on what was going on. There were web sites focused on a United Ukraine – State Department to Help Ukraine, and there were Free Palestine and Free Syria sites defaced, as well as government sites in Ukraine. Anon Ghost (Syrian Electronic Army) sources were identified, as were Digital Voice 2012 (Russian and Anti-Russian messages), news articles posted on "operations for independence," police organizations (Pro-Russian) complaining about attacks in the Ukraine, and millions of Facebook/Twitter accounts of the event.
- Over 103 key websites (media) received strikes instantly, with pre-staged automated tools fixed on set target sites. Much of it was focused on how Ukraine betrayed Russia, and how their President signed away the government, and how Russia were now saviors. There was also video that showed this

dynamic of Russia (e.g., Russian Saviors of Ukraine) that was professionally done, and with sources that identified original source to Russian controllers.

- While Georgia encountered massive ping attacks during their conflict with Russia, Ukraine encountered more sophisticated attack/tools, to include use of network time protocol and 63GB (vice 814MB during Georgia) of traffic that could not be defensed against.
- This conflict highlights the many standing issues facing the U.S. and NATO as they seek to bring Ukraine (as with Georgia) into the NATO fold. While the U.S. and Ukraine plan a military exercise in Ukraine as a response, will this be one of several activities that reignites a new cold war with Russia.
- Russia is not going to leave the Ukraine, Georgia is at the edge of collapse, and the Crimea has been lost...this is a time to think outside the box, think inside the box, and think as if there is not box.
- The carefully orchestrated military and cyber activities undertaken by Russia against Estonia, Georgia, and Ukraine may be precursors to future "bear behavior and activities"taken by Russia against its former republics.

DHS ROLES, RESPONSIBILITIES, AND CAPABILITIES

Mr. Antonio "T" Scurlock, ESSA Portfolio Lead, U.S. Department of Homeland Security (S&P/NPPD)

Mr. Antonio "T" Scurlock opened up his panel remarks by restating the need for us to work more closely together, and that during a cyber conflict, there will be no single entity that will have all the information, authorities, and/or capabilities to enable comprehensive national action. Mr. Scurlock then provided an overview of the Enhance Shared Situational Awareness (ESSA) and Information Sharing Architecture (ISA) initiatives. Highlights of his presentation included:

Enhance Shared Situational Awareness (ESSA) / Information Sharing Architecture (ISA) Framework

- We cannot order anybody to do anything. It is a coalition of the willing and uncomfortable working together, and about sharing critical information that is predetermined to share based on information requirements gathered from partners (we continued to sit down with partners so we can provide it in a timely [machine speed] way).
- ESSA is a Federal interagency effort to create, share, and enhance cyber shared situational awareness to enable integrated operational actions. This was formerly the Comprehensive National Security Initiative Five (CNCI-5).
- ESSA will be realized through the ISA, a future framework and set of requirements for cybersecurity information sharing.
- In looking at the Bubble Chart (Figure 1, Page 6), DHS has clearly defined roles and responsibilities. Shared situational awareness that enables integrated operational actions is part of the foundation agreed to by the DHS, DOJ/FBI, and DoD. We had already been working on architecture initiatives, so stepped up to the plate to support this effort in concert with our DoD and DOJ/FBI counterparts.
- The ESSA Strategy includes the following four goals:
    - Plumbing – implementing an extensible technical and information sharing infrastructure based on mission-driven information and technical requirements

- Productivity – maximizing the operational and analytic value of shared situational awareness (SSA) to enable integrated operational action
- Policy – coordinating cyber SSA information sharing policy (this is where ethics come into play, as well as roles and authorities)
- Partners – expanding the full range of information sharing participants (the coalition of the willing and uncomfortable)

- The ISA framework includes definitions of cyber functions to be exchanged (validated through use cases and exercises), participant-led capability self-assessments, and demonstration exercise.
- The three Federal ESSA Centers – the DoD (U.S. Cyber Command), DOJ/FBI (National Cyber Investigative Joint Task Force, or NCIJTF), and DHS (National Cybersecurity& Communications Integration Center, or NCCIC) – have their own lexicons and perspectives on their missions.
- The ESSA Centers sat down and talked about common ISA functions, which included network operations, computer network defense, domain and sector awareness, threat assessment, threat operations, integrated operational action planning, and integrated operational action coordination. Each of these functions was further broken down into several sub-functions.
- For each sub-function, the Centers also agreed on a common description of the information exchanges that are required to execute the function, recognizing that each had different information needs.
- The next steps in the process included the Centers agreeing on the ISA "Enduring" Functional Exchanges (EFE), which were associated to each of the seven primary functions. These were then mapped into an "Integrated Function and EFE Exchange Diagram."

Requirements, Mission Use Cases, and Implementation

- ISA foundational requirements are mission, information, and technical based, and includes an agreed upon phased implementation.
- Mission use cases were developed and will be used to validate the Common ISA Functions and Enduring Functional Exchanges, and include Peer Shared Situational Awareness (SSA), Planning, National Level Situational Awareness and Risk Assessment, Integrated Operational Action Planning, and Integrated Operational Action Coordination.
- Relationships between use cases and an "operational state" from normal to critical, as well as between mission and operational levels (strategic, operational, and tactical), will highlight the various interactions and interdependencies of Common ISA Functions and Enduring Functional Exchanges.
- The National Security Council (NSC) Staff and Cyber Interagency Policy (IPC) has endorsed the ISA, and the task for implementing ISA is in the hands of the Cyber IPC sponsored "Information Sharing Architecture (ISA) Implementation Executive Committee that includes DHS/NPPD, DHS/CS&C, OSD Policy, DoD Joint Staff, NSA, ODNI NIM Cyber, DOJ, and FBI. This committee is supported by the ESSA Portfolio Management Team (PMT) and Inter-organizational Coordination Group.
- The ICG in turn is supported by an Implementation Working Group (IWG), comprised on technical and engineering subject matter experts, and a Policy Working Group (PWG), comprised of Federal, legal, and policy subject matter experts. DC3, IC-SCC, NCCIC, NCCIC, NTOC, and USCYBERCOM supports the IWG, PWG, and ICG.

- There is a two prong ISA implementation strategy, based on a:
    - Top Down, Bridging Strategy – provides near term value, and is based on operational needs, applications, and a Cybersecurity knowledge model
    - Bottom Up, Shared/Enterprise Strategy – implements ISA at scope and scale, and includes a shared architecture at the Unclassified, Secret, and Top Secret levels.

Partnership Engagement

- ESSA partnerships and participation is expanding beyond the government to non-USG domains.
- The ESSA has engaged and seeks to integrate with State and Local Government, Law Enforcement and Counter-Intelligence, Critical Infrastructure/Key Resources (CIKR), and Private Sector organizations, and our Foreign Partners. The ESSA is using ISA as the framework and basis for these partnerships.
- The partner engagement process includes four primary criteria that needs to be met, to include expressed interest, mission criticality, maturity of sharing relationships, and existing information exchanges.
- Partners can participate in one or more activities, and state of engagement could evolve to other activities. Lessons learned are captures to ease future engagements, and where necessary, the partners can integrate and derive products.

Challenges and Lessons Learned

- As stated earlier, DHS cannot order anybody to do anything.
- ESSA/ISA is a coalition of the willing and also uncomfortable. Not every participant is identical, and it is imperative to build trust early in the process. No one organization does it the same. What we are trying to do with our machine-to-machine sharing is not just about faster human-to-human sharing. We also recognize we are not the only game in town, and may not have the highest priority in the face of the current cyber ops tempo. Finally, it will be a challenge to keep looking forward (instead of choosing the familiar) and focusing on a strategic, robust system (instead of falling back on near-term capabilities).

PANEL 6 – ETHICS AND POLICIES

Dr. Bradley Strawser, Department of Defense Analysis, Naval Postgraduate School (Moderator/Panel Member)
Mr. Javier Santoyo, Senior Director, Symantec (Panel Member)
Dr. Dorothy Denning, Department of Defense Analysis, Naval Postgraduate School (Panel Member)

Dr. Bradley Strawser introduced his panel members, and provided some initial comments on the need to ensure ethics and policies guide our activities in cyberspace, both at the concrete and abstract level, before turning the floor over to his panel members.

Mr. Javier Santoyo, Senior Director, Symantec (Panel Member)

Mr. Javier Santoyo provided an overview of Threat Intelligence and Internal Security capabilities at Symantec, and the role of ethics in guiding what they do. Highlights of his panel remarks include:

- Within Symantec, there are three teams that do threat intelligence, but there are ethical and policy guidelines that prevent us from doing response actions. The three teams are the:
    - Internal Security Team that does traditional Security Operations Center activities to include incident response, malware analysis, and investigating incidents
    - Services Organization Team that supports customers by managing their security services
    - Global Response Team that provides threat response services and develops countermeasures
- With respect to threat intelligence, many private companies are doing this themselves and conducting information sharing with the government. However, the private sector is focused on building better security products for themselves to counter adversaries, the same adversary that the government is focused on, and to looking to the private sector for resetting the atmosphere. We are not talking about the binaries, but the services on the infrastructure that cost time and money to build.
- We don't do exploitation, but can ask for information from the internet services providers to support internal security and tracking of the adversary.
- We can also do honeypots to protect ourselves, so we can obtain some of the binaries, download them, and create countermeasures for them.
- In terms of internal security and threat intelligence, it is about tracking the adversary and intelligence focused, and our goal is partnering with other private companies and government, and resetting the adversary. What really stops us is that we do not do active exploitation, but we do focus on who the adversaries are, we try not to do any attribution or postings, as there is no real way to know who the actor is unless you are in their networks, otherwise you are looking at 2-3 hops down. Most attacks coming into our networks are from U.S. based hosts, but they may not be initiated from those actors.
- We need to do things legally. If malware has an associated password, and there is a host on the internet, we can get those passwords and monitor the account. The goal is to find out what they are doing, and try to map out their entire infrastructure, and then having the adversary find new command control servers and creating new toolkits that cost them time and money.
- A typical threat may only reach 5-6 endpoints, and a targeted attack my only get a half-dozen users in a company. The attacks being done against Symantec are similar to those done elsewhere in the private sector, and not just against security companies but also Fortune 500/100 companies. Information sharing is critical, and done through public-private partnerships, and individuals that come from the intelligence community, reserves, or government sector are typically those that are leveraged for information sharing instead of policy.
- Symantec has a huge world footprint, and may be the first to identity the indicators of an adversary, and their infrastructure.

Dr. Dorothy Denning, Department of Defense Analysis, Naval Postgraduate School (Panel Member)

Dr. Dorothy Denning focused her panel remarks on "vulnerabilities" as a policy issue, and whether the government, if they find a vulnerability in a product, should disclose it. Highlights of her panel remarks included:

- There is a huge market in security vulnerabilities. There are thousands of vulnerabilities that are found and being reported, tens of thousands that reside in NIST databases, and an unknown of vulnerabilities not being reported.

- There are several types of players in the market, to include:
    - Security Researchers – who in the past would find them for free based on the challenge, but began to sell them to certain interested parties when they found out big money involved
    - Vendors – responsible for those vulnerabilities and for fixing them, which takes place within their organizations. Many of these vendors have bounty programs and are paying people to find vulnerabilities in their products. Google and Microsoft have bounty programs. These programs do pay off, preventing these companies from hiring additional staff at greater cost.
    - Brokers – who buy vulnerabilities from researchers and sell them to other parties which could be other vendors or government. There is much criminal activity in that market.
    - Governments – buy vulnerabilities from brokers and security researchers, and find their own vulnerabilities.
- On this last point – the Government finding their own vulnerabilities – what is their obligation to report these vulnerabilities? When vulnerabilities are disclosed to the vendors, so they can fix them, does this make things more secure?
- My colleagues believe we need to make sure the government uses "responsible disclosure" of a vulnerability to vendors so products can be fixed. While many disclosures lead to enhanced security, many vendors are slow to develop the patches, so their particular systems could be vulnerable for months or years. However, what some of these colleagues may not want to disclose is the fact that when vulnerabilities are disclosed, especially those with an exploitation to go with it, the number of attacks that exploit that vulnerability sky rockets. In one example, there was increase of an estimated 100,000 attacks (five orders of magnitude) after the vulnerability disclosure, and after the vendor had released a patch to fix, the organizations were slow to adopt the patches.
- We also found the variance of the malware to exploit these vulnerabilities also went up by orders of magnitude.
- We have one side saying things are more secure because we are fixing a vulnerability that is there, but that the threat has also gone way up. So in looking at risk, which has to take in account vulnerability and threat, it is not so clear if we are really better off or not.
- Another factor is that security and defense does not equal fixing vulnerabilities in products, as human error contributed to estimated 95% of the thousands of incidents that have been looked at such as opening attachments, poor configuration management, and poor passwords. So even though you are fixing vulnerabilities in these products, it does not mean attacks are going to stop.
- So in coming back to the question, should the government disclose vulnerabilities that they find?
    - The argument for disclosure, that disclosure makes cyberspace more secure by having the vendors fix these problems, is consistent with U.S. government rhetoric that cyber threats are serious and we need better cybersecurity, and is consistent with government efforts to promote better security.
    - The argument for keeping this secret is so the government, such as the FBI/NSA, can exploit these vulnerabilities in cases involving national security.
    - The counter-argument for keeping them secret is that vulnerabilities are out there and anyone can exploit them, and so by not disclosing them, the Chinese and Russians might be inclined to exploit them. Because the U.S. sponsors technology more than other countries, the negative effects to the U.S. are greater than to the other countries.

- Another counter-argument for keeping them secret is that the government will lose credibility if abdicates from securing these vulnerabilities and instead are focused on exploiting vice fixing them. We also lose moral authority when we criticize other countries for launching cyber attacks, and then we either conduct them ourselves or better position ourselves in the future by hanging onto these vulnerabilities in secret.
- China accused us of that when we accused China of cyber espionage, and they came back and cited what NSA is doing. We argued that it is not the same thing because we don't focus on corporate espionage, or do it to give our companies and unfair competitive advantage. On the other hand, if we uncover unfair trade negotiations that are harming U.S. corporations, and then exposing what we have to our corporations, this could well benefit U.S. companies involved in the trade negotiations.
- Another issue is trade-offs. Is it worthwhile keeping all vulnerabilities secret? A recent study looked at NSA surveillance and found that in 7.5% of the 225 terrorist cases, data collection was involved in a small fraction of these cases. With NSA, this was about full surveillance which does not rely of exploiting vulnerabilities or asking data providers for data. It wasn't clear what the benefit was for keeping vulnerabilities secret.

- As for current policy, if there is a clear national security or law enforcement use, vulnerabilities can be kept secret and exploited, otherwise the bias is for now towards responsibly disclosed vulnerabilities.
- Michael Daniel, the Special Assistant to the President and the Cybersecurity Coordinator, stated that "this administration takes seriously our commitment to an open, interoperable, secure and reliable internet, in the majority of cases the responsible disclosure of newly identified vulnerabilities is clearly in our national interests…and has continued to be the case." He also gave a list of the types of questions they look at to make a decisions about disclosures:
  - How much is the vulnerable system used in the core internet infrastructure and other critical infrastructure systems in the U.S. economy and in national security systems?
  - Does the vulnerability without a patch pose a national security risk?
  - How much harm could a nation or criminal group do with the knowledge of this vulnerability?
  - How likely is that we would know someone is exploiting this vulnerability?
  - How badly do we need the intelligence from using this vulnerability?
  - Could we use this vulnerability for a short time before disclosing?
  - What is the likelihood someone knows about this vulnerability?
  - Can this vulnerability be patched or mitigated?
- Another issue of not exclusively disclosing vulnerabilities surrounds interjecting vulnerabilities into systems by advocating for weakened security products, or explicitly putting back doors in things. This raises all the same issues of vulnerability disclosure, and the tradeoffs between security and risk and exploitation for national intelligence purposes. It also raises another issue of the long term effects of U.S. companies losing business due to the loss of trust of those products, with the concern in which NSA has placed back doors. Forrester has estimated that this is going to be a $180 billion loss...are we shooting ourselves in the foot.

Dr. Bradley Strawser provided an abstract view of Ethics and Policies by looking at Cyber War through the lens of "Just War" Theory and can we do that. Highlights of his presentation included:

Just War Theory

- How do we ethically understand the notion of cyber wars in the context of the Just War Construct?
- There is a classic problem philosophers had when they think about harm, and liability to harm, justifiable defense, and things like proportionality...and whether you can take small harms and aggregate them up to a level for a justifiable response to the harm that is still considered proportionate. As an example, if someone is flicking your ear, even if they were wrong, could you justify killing them as a proportional response. No. If they were to flick a million ears over the years, at what point could these small harms add up such that you could kill them in response?
- Cyber warfare makes some of these philosophers questions real, as most harms done in cyber war are minimal, and much less than that because they are being widely distributed.
- So how do we measure harm, and what level of harm must we add up to in order to respond with a justifiable response? There are different types of harm, and some of the lesser types could never justify other types of harm. So what is a justifiable cause for war?

Cyber Warfare and Just War Construct

- When discussing cyber warfare, we are not talking about non-state actors, cyber crimes, and hactivists – instead we are talking about full state-on-state armed conflict in cyberspace.
- What threshold needs to be brokers to justify war? In cyber war, this question becomes complicated because you are not killing people, and even if doing harm it is distributed harm with usually small scale damage (we are not killing people or blowing up buildings).
- In cyber war, there will be sub-level action but these do not justify lethal kinetic actions in response.
- From an ontological approach, all harms are on a spectrum, and just a difference in matter of degree.
- From a utilitarian approach, if you add up the harms together, you can then justify a proportional response. In this context, if there are enough small cyber harms, then this could result in a proportional response.
- In looking at the International Community of Red Cross, how do you shape International Humanitarian Law for cyber warfare – and how can we apply it? In traditional war, it is easier, with red lines on what is armed conflict and there are certain protections, especially with harm to the civilian populous. In this context, law and ethics pertains to how you behave in war in dealing with protections from harm, and protecting civilians is always an aim. From an International Humanitarian Law perspective, some civilians are expected to be harmed unintentionally as collateral damage (secondary effects), but even that has to be weighed proportionately.
- The vast majority of cyber warfare activities will often impinge upon civilians, often in a direct way, or at least annoy or interfere with civilians in a "small war." If you take one view, it is irrelevant, as you cannot add up enough of these harms to justify kinetic responses. If you have enough of these, taking the other view, then Just War Theory applies.
- As an example, there is a new challenge in Just War Theory as it applies to Cyber War. Do we want to think of harm in a purely physical view, or do we view harms as wrongs anytime we touch critical

infrastructures. This has a double effect, as long as harm done to civilians is a secondary effect, and not an intentional effect, it can be justifiable, as long as it is proportionate in context, in looking at cyber war in context to the International Humanitarian Law. You still are going to have to weigh out proportionality. So unless we decide on how to count these little harms, we cannot develop that calculus upon which to decide to aggregate them up or not. If not, then there is a potential for massive widespread harm to civilians, which brings into play International law, policies, and ethics in coming to a decision.

- There is a concept called "dual use" that could factor into decision making. If a building or object is used for dual purposes by military and civilians, then you can target it as long as at the time it is used for the purpose of the military. In the cyber world, there are massive infrastructures used by the military. The vast majority of them use the internet which touches upon this dual use concept as this now involves some interactions with civilians.
- Another possibility could be that all attacks in cyber space should be other that the internet, and directed to thumb drives or peripherals as examples.
- There appears to be no solution to this, if you stay within the guidelines of International Humanitarian Law and Just War Theory.
- Cyber definitely pushes the boundaries of Just War Theory as proportionality becomes difficult to weigh if you cannot come to a clean decision on how to counter harms and measure what it means to harm someone. In traditional war, it is generally neat. In cyber, it is not that easy to measure harm or how to counter harm.
- Does an aggregate of harms in cyber justify a kinetic response? In theory, no, but if there is no correlation, International Humanitarian Law becomes a non-voice in cyber war, as you cannot add up harm and you cannot justify killing. Cyber war appears to be outside the bounds of civilian protection from harm.

Questions / Open Forum Discussion

1. **As Cyber Warfare moves to "destructive malware," such as with Stuxnet, how do you measure when a cyber activity becomes a kinetic activity or an act of destruction of a physical device?** When we talk about destruction of property, it is easier. However, what we are destroying may not be a physical device, and instead software or "economic loss."
2. **Relevance of International Humanitarian Law –** today, it may not be so relevant, but when you look at technologies such as automated cars, implants and medical devices, cyber attacks can potentially have much greater harm than just shutting down a computer.
3. **Responsible Disclosure –** even if a vulnerability is not disclosed, there is a window of opportunity of 6-9 months before the vulnerability is fixed, in which the threat takes advantage of exploiting this vulnerability.
4. **If a vulnerability is going to be released by a competitor state, such as China, that could bring significant economic harm is the vulnerability was exposed and exploited, could that justify a kinetic response?** There could be potential billions of damage by having a state exploit a vulnerability that has been exposed.

5. **Can Russia's cyber activities in Estonia, Georgia, and Ukraine be classified as a war crime, as so many innocents were affected?** While there was devastation to their infrastructures, understanding the role of the government (in this case, Russia) is important. How do we weed out the nation state actor, the criminal, the hactivist in all of this? This ranges from the difficult to the impossible.
6. **Proportionality and Adversary Perspectives** – With any given cyber action, proportionality is going to perceived differently from us. In theory, with kinetic actions, it is generally predictable. In Cyber, it is not predictable. There may be unpredicted results of cyber attacks, and you do not know the "cyber blast radius" of cyber attack weapons. Erring on the side of caution is recommended, as this effect how the enemy interprets internal community viewed.

PANEL 7 – PUBLIC PRIVATE PARTNERSHIPS

Ms. Alison Kuzmickas, Sensemaking/U.S. Pacific Command (Moderator)
Dr. Richard Berry, Director of Strategic Partnerships, U.S. Pacific Command (Panel Member)
Dr. Steve Chan, MTI/IBM NSRC/Sensemaking PACOM Fellowship (Panel Member)
COL Margaret Roosma, Chief, Cyber Initiatives, Office of the Chief Army Reserve (Panel Member)
Mr. Bob Griffin, CEO, IBM i2 Group/IBM NSRC (Panel Member)
Dr. Kathleen Kiernan, KGH/Infragard/Naval Postgraduate School (Panel Member)

Ms. Alison Kuzmickas introduced her panel members, emphasized the importance of public private partnerships and the process of collaboration, and made a few remarks on the work being done by the USPACOM Sensemaking Fellows in applying Big Analytics atop the Big Data to generate Big Insights, and some of the research being done that includes cyber supply chains, astro-turfing, bad data's impact on decision making, and visual data.

Dr. Kathleen Kiernan, KGH/Infragard/Naval Postgraduate School (Panel Member)

Dr. Kathleen Kiernan introduced herself as a "pracademic" instead of an academic, based on her career in law enforcement and the experience you can only get by walking the ground, and then adding academic rigor to that along the way. Highlights of her panel remarks included:

- My first career was with ATF, and what I learned early on was that if you could not the competitive piece at the crime scene, you would end up being competitive against one another in the interagency environment instead of against the adversary.
- My career evolved and I did the same thing in the international arena, and saw the same kinds of scenarios play out. It was the blind spot of not who is in charge, but who had the most to offer in that environment, what was the best in this environment, and to obtain the best result which included developing some organic kinds of collaboration capabilities.
- Over time I began to support the Office of the Secretary of Defense in the Rapid Reaction Technology Office, where we looked at developing exploitation technology and second, third, and fourth effects impact of that technology in the first responder community. Prior to that effort we did a lot with

irregular warfare exercises, and learned in table top exercises that you do not want peers to fail, and oftentimes end states of those games are not anything earthshaking or innovative, breakthrough ideas.

- The Deputy asked if I could bring more of my friends in here, the cops, the robbers, the malcontents and outliers – those that think differently than those encumbered with intelligence or defense badges. So we started to put this in progress, and that meant bringing in people external to the Washington and "bureaucratic" AOR, folks from academe, hackers, and other areas. What we found over time is the results of those games became much different. Part of it was exploiting and illuminating those blind spots. Translated from Latin, these became the "Crappy Bastards," which has a parallel construct called the "Cyber Bastards."
- I also teach at the Naval Postgraduate School's Center for Homeland Defense and Security, where we get the best and the brightest from the first responder and defender community, bringing them in at the average experience of 20-25 years, and infuse them with a sense of curiosity and academic rigor.
- When looking at change, and the inherent difficulty in trying to change behavior of adults, there are there three pieces of literature that provide some insights into this phenomena.
    - In one piece, the author talked about conflicts and threats coming together and getting different kinds of reaction, and highlighted the interagency being "dirty." He was not implicating necessarily, from a law enforcement perspective, that dirty meant corruption or bribes, but instead that there is no way to engage in an interagency environment without getting dirty and coming out differently than when you went in. You have to have that openness to understand that it is going to get you to change the way you think and react and do your business.
    - In a second piece, the author discussed the dynamics and implications of putting business lessons into policing. The first part of the book focused on finding a common platform and the second is that you have to decide what currency matters to whom. On that common platform you have to decide what you are willing to give, and what you need to get back, and it is a pretty messy environment which requires having a common platform of collaboration. This was tested in many ways by the author, who personally set out to professionalize the Port Authority Police (New York City) and Transit Police, who were rogue in the early 90's (improper uniforms, not making arrests, and who did not ride the subway...otherwise known as the electric sewer). He took everyone from Sergeant and above, and made them commute on the electric sewer, so they understood the undergirding of the NYPD and the city and why it necessarily did not function well. He enabled these officers to make felony collar arrests, because 1 of 7 of the fare jumpers had a felony warrant on them. He reintroduced policing in a whole new level of professionalism and compelled them to understand their mission and responsibilities.
    - In a third piece, the author discussed the construct of adjacent spaces, and where good ideas come from. The author talked about the interagency and global environment, about pushing people beyond their comfort level to understand new domains, and uses lots of metaphors. It teaches people to explode through traditional boundaries of thinking. In putting my law enforcement hat while working with the ATF, DEA, FBI, and other organizations, I (we) learned that we either collaborated or perished for some very basic reasons. The DEA and FBI initially decided they needed de-confliction of operational and analytical talent, as there was a deep divide. Operators didn't want to talk to analysts, and analysts didn't want to talk to operators.

But if you put them together, a couple of good things happen. They solve blue-on-blue cases, and they build better and more robust cases in trying to collapse underground networks and economies that support them.

- In looking at my private sector hat, Infragard is a shining example of a public and private partnership, which was started by the FBI in 1988. The construct was that there were so many people in the Cyber World that were committing fraud on the internet, or parking themselves in banks to steal money and identities. It was a very hard sell, as who wants the FBI knocking on their door? When banks see regulators at their door, they much rather lose a small percentage of their competitive advantage and deal with the problems in house and not share information about threats . The Bureau did a great job of convincing the financial industry that a threat to one is a threat to all, so information sharing increased. The Infragard initiative spread across the other 15 critical infrastructures based on trust, and an understanding of the nature of threat. Infragard now has 62,000 members, and I had a privilege of leading this for a while. These are folks that are the "first line of defense" in terms of seeing anomalous behavior and early indications and warning. They may not think in those terms, but they are positioned to see those and have a means of bringing those to national attention. This helped the FBI find the "space between the cases," big cases that did not hit the screen yet being seen first at the local level.
- Within Hawaii, you have the Medici Effect, which is what I call the convergence of academia and private sector, the island effect, and having an adjutant (1 of 12) that has a dual hat. It was interesting to hear General Wong state his uniform should be ½ Blue and ½ Hawaiian Shirt, because he has to navigate Titles 10, 32 and 50, understand Title 18, and then figure out how to respond. With a crisis every six weeks, and help of Dr. Chan and the Sensemaking Fellows, and others in the civilian populous, they put together an initiative to test the boundaries of past practice, community practice, bringing in education from that 3rd grade level where we can teach those kids the code in order to build the next generation of leaders. This is a perfect convergence of great talent. At the end of the day, they have to be self-sufficient.
- As we look into cyberspace, we are looking into terrestrial kinds of thinking, with lessons learned from the cyber side of the "Crappy Bastards" methodological approach. We looked at swarming in Cyberspace, and looked a lot at the "art of diversion." If someone wants to smuggle something, they want your attention somewhere else. The key is to find some of the indicators of behavior of concealment, and then look at social media, cadence, and patterns.
- In order to "illuminate blind shots," we need to move to "big insights." Collaboration must be organic, competition must be against the adversary and not each other, we need to develop our workforce by imbuing them with a sense of discovery, accidental discovery is actually the best kind of learning, and what we are doing with the Sensemaking Fellows in Hawaii may serve as a model we build and bring to the world.

Dr. Steve Chan, MTI/IBM NSRC/Sensemaking PACOM Fellowship (Panel Member)

Dr. Steve Chan is the Chairman of Mehta Tech, Inc, Director of the IBM Network Science Research Center (NSRC), and Director of the PACOM Sensemaking Fellowship Program. Dr. Chan acknowledged Dr. Kiernan's "Crappy Bastards" concept which helped him in opening his eyes to some of the blind spots, as well

as his relationships with Dr. Berry on the Sensemaking Fellowship, with industry such as IBM with the fusion of Watson's foundation technology with Big Analytics, and with COL Roosma and OCAR with P3I. Dr. Chan considers himself to be a "momentary matter expert," based on his contention that change is constant and this requires a perpetual constant learning experience. Highlights of his panel remarks include:

- The Office of the Secretary of Defense (OSD) Rapid Reaction Technology Office (RRTO) hosted a workshop in Hawaii to look at these blind spots and mitigations. One of the problems they looked at was how to track something (like a submarine) with monitoring systems and ISR assets, or by tracking the officers and the crew, or other means and methods. Some of these illuminating points brought Hawaii onto my screen for the first time.
- Some of the granular techniques needed for visualization and visual analytics – seems everyone in the search of a common operating picture – requires some kind of look across the space and open source, and we started to look for capabilities (3rd party open solutions) to enhance the visualization, such as with IBM Network Science Research Center. We were able to foster an effective relationship, a micro-P3I, and in many ways to look at "problem sets" with insurmountable mathematical complexity, and to bring them down to an "np problem set."
- I'd like to put forth a "grand challenge," and that is how to understand the Hawaiian Islands or even Oahu for that matter. From an academic perspective, we have to develop a framework and break it into problems you can solve. The original challenge, which was similar, was what can be done about Civil Affairs complexity? In looking at the Civil Affairs framework, it can be broken down into the political, military, economic, social, infrastructure (energy, water, sewer), and information (talking about big data and data analytics, e.g., IBM Watson). In getting back to the challenge, I developed several Centers of Excellence at MIT, and each center was interdisciplinary, with people from the Systems Engineering Division, Systems Management and Design, and Systems of Systems. I got them involved with Harvard and Cyber leadership at DEFCON conferences, and noted there is no Cyber Security Center at MIT. What would we do with our researchers? We sent them to Carnegie Mellon University or to Fort Devens on the weekend.
- In a disaster situation, such as was with Haiti, team dynamics and partnering come into play immediately. Students at MIT wanted to assist in country, but were initially hampered since no student can go into a country with the State Department's International Travel (Registry) restrictions. They solved the problem by working with the University of Florida and USSOUTHCOM, and found their way to Haiti and successfully navigated the 20,000 NGOs and counterfeit agencies that were in Haiti.
- In looking at the Hawaiian problem set from a reverse engineering perspective, we need to open the aperture a little, and look to the 1946 Tsunami and several 9.2 level earthquakes, and then identify ways to better protect ourselves. We could employ more sensors or buoys, and as we learned during the BP oil spill, or perhaps employ new technology that models not approximations of what may happen, but that has computational abilities to model exactly whether a tsunami will hit or not hit the Hawaiian Islands.
- In describing the network (in the context of network science), in order to understand the network, we have to understand the observation space. From a "system of systems" perspective, we need to identify and illuminate the blind spots. We want to combine human sensors with machine speed defense and machine speed mechanisms, and put this all together. It takes a lot of big data, but we need to get beyond that to accommodate unstructured data as well. We are in that realm where we can

move from big data to even bigger data, which requires big time analytics and insights, and a lot of public-private partnerships and a maximum number of resources.

- In order to understand the network, again, you are going to need a lot of data. When we looked at aggregating big data, we realized that much of this data originated overseas. In context to a JIEDDO problem set, we gathered data sets from China and Pakistan, and as for adjacent spaces, it became necessary to observe and track human factors. Big data is king, but it is a struggle to get data to tackle many of these challenges.

Mr. Bob Griffin, CEO, IBM i2 Group/IBM NSRC (Panel Member)

Mr. Bob Griffin is the CEO of the IBM i2 Group, and has had the privilege of serving the intelligence and law enforcement community in several high profile events and forward deployment actions. He currently sits on Boards of the Intelligence and National Security Alliance (INSA) and Cyber Forensics Training Alliance. Highlights of his panel remarks included:

- We are building an environment in the IBM Network Science Research Center, and it is becoming very clear that we live in a connected world.
- As Dr. Berry stated earlier in the conference, more data has been created in the last two years than in the history of man, and more data will be created in the next two years than the past two.
- This is not a problem that is going to get smaller. The ability for us to take information on demand and start to assimilate that, you start to see hidden signals and patterns, with the whole idea being behind the work of the Network Science Research Center.
- When Dr. Chan explained to us the challenges that Dr. Berry is facing in Hawaii, and his operational vision from the AIRS Project, we believed we could take that set of technologies we had been developing, and start applying it to that environment and really help identify unique and distinct kinds of blind spots.
- One of the most overused expressions is that we have to "connect the dots." The problem is when you have ten million dots, and you only care about four of them, you have to find those four dots very quickly, you need to make sense of those four dots and how they interrelate.
- Some of the big problems we are seeing in our world is, how do we deal with the trillions of dots, and sift and sort through those dots (e.g., IP addresses, continuous streams of data)? So what we believe we can do at the NSRC is to supply that set of capabilities to some of these challenges, in particular, assisting Dr. Berry in actualizing the AIRS vision.
- In talking about public and private partnering, there is no one organization can do it all and it is amazing the requirements that we are going to have to bring to bear in how to solve some of these problems.
- Within IBM, there are 44,000 employees, and they can give statistics on virtually everything. When it comes to issues about cybersecurity and cyberspace, approximately 3% of the world's population has the skill sets to deal with those issues. If we don't ensure that we have that "cooperative movement" among the public/private sectors and academia, we are going to fall short of the ultimate goals and mission.
- We at IBM have developed technologies, to include cognitive technology like Watson that assimilates open source materials and that presents a hypothetical dialogue, with percentages assigned. This addresses an estimated 90% of the problems we could expect to face. It is this type of technology that we are trying to harness to solve problems in environments, such as the AIRS environment, that can

help us start to ask the right kinds of questions that we possibly cannot assume from a cognitive perspective just by pure nature on how fast we can inject and assimilate information.

- Part of the value IBM brings, and more importantly the public-private partnership, is that we can bring technologies like that to bear on lot of these situations to shore up the 3% of the population to become more skilled, or to provide more technology to solve increasingly complex problems, or to provide resources that highlight potential blind spots and eliminate those. When we get down to the science of building capability, we really are building systems that are "resilient by design."
- What I worry about, and what keeps me awake at night, is "brain drain." People in this room are doing wonderful things, and I recognize that many of you are citizen soldiers. However, the 3% of the population is the same group that everyone wants – for example, Bank of America and Hartford Insurance will pay a lot of money for people with these kinds of skills. What I'd like to see is the community addressing the question, "how do we compensate these people that are solving our problems, and that are making us secure, in a way that is market relevant so we don't lose all these great skills out there?" All the corporations are driven by shareholder return, and there are no alternatives in the corporate world. I want that dialogue in these public-private partnerships.
- In the context of what tools and methodology can be used to look at big data, just as nobody can do it all, no one set of data can do it all. My career has been built around fusing multiple, disparate data source. Probably the most critical piece of information is that "human sensor data." While context information is "King," access to and distribution of that information is "King Kong."

Dr. Richard Berry, Director of Strategic Partnerships, U.S. Pacific Command (Panel Member)

Dr. Richard Berry (who developed the original concept of AIRS) spent 20 years with DoD, with some private sector work with Merrill Lynch, and after 9/11 came back into the government in Hawaii, and is now trying to move forward some of the concepts talked about the last couple of days. Highlights of his panel remarks included:

- In 1992, when I was in Hawaii, Hurricane Andrew had just hit Florida, and in Hawaii there was another Hurricane that hit about the same time. It hit one of the outer islands and literally devastated it; it was probably almost 20 years later before you could go over there and see where the infrastructure had been improved.
- Five years ago, stood up the J9 under Admiral Willard, and at that time had a discussion with him that was "provocative." The Admiral posed two questions to me, the first of which was, "are we just wasting our time?" In the context of Cyber Endeavour, we have been here three days, and most have been to a conference that when it ends with our notes and binders, and when you get back home you might be inspired for a little bit, but ultimately you put the notes and binders on a shelf and get back to work. The Admiral really moved me when he asked me that question
- The Admiral asked a second question, "do you want to make a difference, or just go back to doing what you are doing at work?"
- I decided to take him up on the challenge. There is always a crisis going on within the Pacific Command, about one crisis every six weeks. The Admiral said it seemed to him that it never gets better, and do we really ever learn anything, with all the money we have thrown into PACOM and USAID and the State Department. Does anything get better?

- The Admiral then stated he was tired of fighting for inches...let's take a bigger swing at it. Let's take some bold ideas to try to move us forward, and I will support you. This led to the idea of having to do more with the private and civil sectors, as it doesn't seem like they come together when we have to go out there and do something.
- The crisis of our times has nothing to do with financial bankruptcy or economic bankruptcy, but instead that we are running a risk of suffering an "intellectual bankruptcy."
- The following are a few insights on some of the challenges in what I have observed and experienced, without being overly analytical or prescriptive. There are three symptoms of the problem, and what we have tried to do with this AIRS concept as the specific treatment.
    - Symptom 1 – the need for real organizational change. How do we go about addressing those human dynamics that impact our organization? The treatment for this symptom is this idea of reciprocity, which does not mean quid-pro-quo, but instead on what do I bring to the fight, or from a contrarian view, are you bringing me something you haven't solved? So if you are coming to the discussion of P3I with the question, "what can you (Bob) do for me?" I am going to respond with the answer, "I don't know, what can you do for me?" Obviously a wrong discussion for moving P3I forward. There are better solutions. In discussions with Dr. Chan, I stated there are things I could do to help him, as Dr. Chan mentioned that he had great people, and research dollars were not a problem, but what was a problem was he did not have places for his people to work in meaningful, cutting edge research. I can help was my answer.
    - Symptom 2 – leadership development. We (us) are woefully inadequate for what we are trying to do. Not just because we ask the wrong questions, but when looking at the root of why P3I does not move the way they are supposed to, we should start by looking at the mirror and ask the question, why can't I get this thing moving? For me, it has mostly been because I have not asked the right question or have not approached people in the right way. Let's not blame the lawyers, but instead focus on creating the space to have the right discussion. The idea of AIRS is to create the space for ideas to come forth and for those discussions to take place, to include the private sector (what tools they have to solve problems), government (problem sets, and where that technology can be used), and academia (tying it all together). You now have real solutions to the problem. This leadership development is a different model than what we used too. While we talk about education, within DoD it is really about training. When talking about training and giving people additional skill sets, that is a good thing, but if they do not have the theoretical background, they don't have organizational capacity. People can do a lot of things, but education is instrumental, especially entrepreneurial education. It is interdisciplinary in nature – there is a cultural, social, psychological, math, and hard science aspect to this (and it all has to come together, and we have not done it too well). Our educational institutions need to step up and help us move forward.
    - Symptom 3 – integration. How do we integrate all of this? The idea for AIRS is to create the space for that integration to take place. How do you get the private sector a space where they feel comfortable enough to share problems, and talk about where they could use help? Or educational institutions to discuss and share workforce development programs...or the government to actually help convene, shape policy, and outline priorities. You need a common space.

- Education piece has to be holistic, and include K-12, graduate, and post graduate education. AIRS could be a success, but when looking over the shoulder, we still may not have the pipelines, especially in Hawaii.
- The root system of the Banyen Tree is where the public, private, and civil sectors work and it is messy. It takes concerted effort in an ecosystem like the Banyen Tree to bring this together, and it means that we have to change the way we think and approach problems, and not in the deliberate way we have been doing.

- In looking at "big data," we wanted to look at one of the biggest problems we could have in Hawaii, a Category 3 Hurricane hitting Hawaii. This impacts us not for days, but for months in our island ecosystem. We approached Hawaiian Electrics to discuss problem sets they have that we do not have. Dr. Chan put together the Sensemaking Fellows together to look at these problems with academia and the private sector, and approached IBM to gather and analyze the data. We approached the Governor's office, and asked them what else is this tied to and what could be fixed at the same, as an example, when electricity goes so does water and sewer. We also asked them what they were and were not doing with HECO.
- In context of workforce development, we have Sensemaking Fellows in Hawaii, but we need to start addressing what these issues look like. Finally, as we get all the data from the different problem sets, we believe we can pull it all together (with the technology that currently exists) to get it right, and provide real world solutions.

COL Margaret Roosma, Chief, Cyber Initiatives, Office of the Chief Army Reserve (Panel Member)

COL Margaret Roosma is the Chief of Cyber Initiatives for the Office of the Chief Army Reserve, which is a new position created a couple of years ago, and in recognition that the Army Reserve has many cyber professionals in its ranks, but not in its upper leadership that could represent that level of expertise to the Army and other DoD agencies, and out to the civilian community. She is representing the Chief of the Public Private Partnership Initiative, which is now a chartered organization within the OCAR staff. The P3I is one of the General Talley's prime initiatives, and he believes so firmly in the importance of the professionals across the Reserve component, and not just in the cyber world, and what we have given to our community, our organizations, and the Army. Highlights of her panel remarks include:

- There are two prongs to the partnering initiative. <u>The first part is linking in the training and education piece</u>. How many in this audience have a BS in Cyber Security or something related? For those that did not raise your hand, how many of you would like to approach that? Would you like to have that supported by the military, hopefully funded to get that degree in Cyber Security?
- In looking at this partnering initiative, we are working closely with the University of Texas at San Antonio, University of Washington, MIT, Swansea University, University of Massachusetts, University of California at Davis, University of Houston, and the Naval Postgraduate School. The purpose is to expand these opportunities for people in uniform to get these higher level degrees. When we ask the Army and DoD what they are doing to educate their cyber warriors, and they say they have some seats in NSA courses and you (Reserves) don't have any seats until FY17. So we need to look outside the DoD box for training and look at how we can partner with these universities.

- This situation is a win-win. When our military cyber professionals go and join these classes as I saw at the University of Washington's Seattle campus, there is a reservist who is over in Bosnia working at an international center there in Cyber Security, then he was attending his classes (skyping in) every week and joining the discussions, and he had so much to give based on his live, in person experiences. You would do the same thing with those raw, fresh college students.
- From an education and training aspect, partnering is critical, as we found in the Boston Academics Group and our reserves at the Northeast IO Center (NEIOC) and other locations that the sharing between the civilian students, professors, and military students built synergy.
- The other prong to the partnering initiative is implementation. In Hawaii we are working with the National Guard and the utility companies to develop a partnership program where are developing these relationships, which will hopefully turn into a perfect example and model of how to spread this relationship within the United States.
- At a recent Cyber Symposium, Admiral Rogers in his keynote speech talked about how this is all a team efforts, and that when we spend too much time having our cyber professionals just focus on what is on the keyboard, and that is all part of the baseline training, but until you broaden that an link up with the physical effects (such as Cyber City Exercise that looked at what happens when the lights go out at the airfield or an electrical plant is infiltrated), tying in those physical security aspects of what we are seeing in the cyber domain is critical. For our civilian counterparts, they need some of the military skills that we have.
- In our civilian day jobs, we need to think about how to broaden this partnering and somehow bring the military context into what we are doing. If you are working for a local or state agency, that does not already have some type of relationship with the military, this is something we can explore, recognizing there will be hurdles along the way (titles and authorities).
- We recognize the National Guard has the lead in working with state and local agencies, but under certain titles, we can tie in the Army, Air Force, and Navy Reserves into these same support relationships. The more we broaden that, the better we able to be a part of our nation's defense.
- General Alexander frequently talked about the importance of the military defending the nation, but how do we do that in cyberspace if most of our cyber domain is in the civilian quarter?
- This relationship we are building in Hawaii is a great test of how we are able to do that...and take our wonderful planning skills that the military learns from day one, and operations, and then bring to the civilian sectors.
- From a military perspective, the Army is establishing a Cyber Branch, and on September 1st of this year this becomes reality. The Army Chief of Staff stated he is looking forward to shaking the hand of the first Cyber Soldier. The real long term effort is developing a "more professionalize our Cyber Force," and the Cyber Branch is the first step. This group, like others in the services, needs to be managed in a "specialized way," to include additional incentives. There a lot of bureaucratic hurdles to jump through, and what we need to keep in mind in leaning forward is, "how do we incentive and reward our best people?"
- In context of looking at the tools and methodology that can be used to look at "big data," the concept of "humans and sensors" is where a lot of the reserves fit in, and are at the front edge of the problem area. It is important that the information and insights of our junior personnel who are working these problem area bring it to the attention our senior leaders and managers who are working the end of the

problem. We also need to practice how we fight, and work into our planning and activities the various scenarios in which we might be called to support, such as a tsunami or major earthquake.

PANEL 8 – SMART GRID

Dr. Steve Chan, MTI/IBM NSRC/Sensemaking PACOM Fellowship (Moderator)
Mr. Randy Baldemor, Director of Strategic Initiatives, State of Hawaii (Panel Member)
Mr. Michael Champly, State of Hawaii Public Utilities Commission (Panel Member)
Ms. Shari Ishikawa, Hawaiian Electric Companies (HECO) (Panel Member)
Mr. Jeffrey Katz, CTO, IBM Energies and Utilities
Mr. Wesley Rhodes, IBM
Mr. Jim Hackett, EVP, Mehta Tech

Dr. Steve Chan introduced his panel members, provided some comments on how Hawaii is unique in that is a strategic area of the Pacific Basin and leading many smart grid and P3I initiatives, and then directed a series of questions to each of the panel members.

Ms. Shari Ishikawa, Hawaiian Electric Companies (HECO) (Panel Member)

Ms. Shari Ishiwaka provided an overview of the Electrical Grid – Smart Grid from a HECO perspective. Highlights of her panel remarks included:

- Hawaiian Electric Companies are just in their infancy in installing the smart grid, and the smart grid is not just the Advanced Metering Infrastructure (AMI) meters. It is also about overlapping other applications and switches for optimization on the system and voltage efficiency. We are also installing devices, switches, and fault indicators for reliability purposes.
- One issue that we are also trying to address is integrating more renewable energy. The State of Hawaii has an aggressive goal of 40% renewables.
- So with that comes the ability to have two way communications, and what type of managed products (devices and programs) that can utilize this smart grid communications effort to help us further our renewable energy goals.
- We have started initial demonstrations (our commitment to move forward) with the technologies we are using, and we are deploying an estimated 5,200 meters at this time, and we should be completed by the end of July 2014. From there we are going to go to the Public Utilities Commission for their approval for full deployment roll-out, and look to get that approval in the 2015-2016 timeframe and move forward with the full deployment roll out. This will cover the Hawaiian Electric and Maui Electric, which includes the five islands of Oahu, Hawaii (Big Island), Lanai, Kauai, and Maui.
- In shifting to "inverters" and cyber security, within Hawaii 80-90% of the inverters are connected to the cloud, and are collecting data on generation for the customer. It would be easy for a disgruntled employee or someone who knows that to shut all those off at one single instance, and that is almost like putting the utility into a 2nd or 3rd contingency situation. Hawaii's ability to absorb more contingencies

is not as robust as on the mainland, and it will shut us down. If we do shut down, then we have to go into a black start mode.

- We are not interconnected between islands, and each island has its own utility. We have a black start capability, and at night we are pretty much on batteries. We have maybe 1-3 shots of starting up the grid, and if not successful in those three shots, we are done and would need to find an alternative that may take weeks, e.g., a nuclear submarine. This actually happened to us in 2006 and 2008.
- Additionally, with the AMI network, with 500,000 meters, if someone were to hack into the system and shut every meter down, they will cause an "over-generation" situation, and put the utility into a 2nd, 3rd, 4th or 5th contingency situation. That is why we need to put measures in to prevent someone from hacking into our systems, and protections to limit the amount of damage someone can do before we can detect it and shut that port down.
- Previously, our OT systems were separated from our IT, and now we are developing an outage management system. With our smart meters and AMI, it has come to a full head where we now need to find a way to protect the OT side of the house.

Mr. Michael Champly, State of Hawaii Public Utilities Commission (Panel Member)

Mr. Michael Champy provided an overview of the State of Hawaii PUC in their role as the regulator and trying to balance the overall interests of the stakeholders. Highlights of his panel remarks included:

- The State of Hawaii Public Utilities Commission (PUC) serves as the regular and trying to balance the interests of the Department of Defense, the largest customer of Hawaiian Electric Companies.
- The Hawaiian Electric Companies, in addition to the smart grid integration, is undergoing a tremendous transformation. We are going to integrate a substantial amount of renewable energy at the same time we have to modernize the grid. Lastly, more and more customers want to be part of the energy solutions, and want to take matters into their own hands. Hawaii leads the nation in terms of residential customers with roof top solar, somewhere around 10% now, and there is a potential for 20-25% of the homes (homeowner owned) have roof top solar. While that is great for these customers, there are some cyber security implications as by the end of the year an estimated 50,000 customers will be plugged into the grid. On Oahu, if you add it up in the aggregate, 30,000-40,000 customers will have enough renewable energy capacity on a sunny day than the largest generators with HECO.
- All of those customers will have solid state inverters on their homes, and the invertor manufacturers are the solar installers that all internet connections to those inverters.
- There are real challenges for HECO to integrate and create new industries for Hawaii, but really cyber security was not first and foremost in this process.
- So the same time we are integrating a lot of renewables and modernizing the grid, which is good and allows customers to reduce their energy costs and allows Hawaii not to replace this with high cost oil, but there is no free lunch - there is a tradeoff. For the new technology, with the benefits it provides, makes our lives more challenging from a cyber security perspective in the balancing act.
- What is considered data? Some people think it is like oil sensor data in car, and it's a specific thing that is measured, and shows up on a gauge and it goes inside your computer. Let's think a little broader, especially since we are talking about 40% solar penetration – cloud movement, predicted winds, and predicted volt usage – all of these things become sensor data in a larger thought plane. If we look at the

electric grid, and the rules by which the electric grid works, the differentials are sensor data. Additionally, maintenance reports are also sensor data, providing an additional set of data and observations. So what we view as sensing is more than little points of data.

- With all the renewable energy coming into Hawaii, we have some islands that by 2016, and during peak hours, that will have 80-90% of their electricity being produced by solar. The real challenge is, great, I do not have to burn oil, but by 7PM when the electricity peaks and the sun goes down in Hawaii, we now have to get back to more traditional generation. This means I have to replace 80-90% of my generation in a couple of hours. That is great if you have flexible, quick starting generation.
- On Oahu, we have conventional steam fired generation that does not cycle like that. We have a dilemma, something that HECO has recognized, as have the California Independent Systems Operators. So the trend is towards flexible generation, and why is that important to DoD? Flexible generation is like combustion engines that are very quick starting, very flexible, and can be turned on for a few minutes, shut down, and started back up multiple times without a cost penalty. What I see as an opportunity and note HECO is starting in this direction is to either look at putting flexible generation on existing power plants because I have the transmission infrastructure, or begin to look at flexible generation on military bases, but use it for the grid benefit (except in times of emergency). If you configure the grid such that base can be isolated, you have new ways and multiple uses of this flexible generation.
- So in our military bases, especially where there is a lot of renewable energy, there may be an opportunity to find a win-win. We are going to have to eventually replace conventional generation to flexible, but now I can be strategic on how to locate it and now create micro-grids that provide you with the resiliency that you need.
- We may have a problem, but let us look at flexible generation and micro-grid solutions, and get multiple uses out of that.
- In regards to sense making, what happened in the past is that we had a lot of slack or reserves in the system. As we put more renewables into the system, and change the whole operating paradigm, we effectively using up the slack in that system. So we can invest and do the things we really improve our system and sophistication of our operations, or we will have to provide additional dollars in hardware to build redundancy and reserves. I would think we want to go the IT approach, especially with all the renewable penetration. When you are at 5-10% penetration, you can operate at the old paradigm. As the capture rate goes up, you will need to change your paradigm and operate in more "real time" and "more on the fly." Electrons move at the speed of light, so if we do not increase the IT component, we are going to augment with a lot more hardware (capital), and that is not the best and most productive use of customers' limited dollars.

Mr. Randy Baldemor, Director of Strategic Initiatives, State of Hawaii (Panel Member)

Mr. Randy Baldemore provided an overview of some of the State of Hawaii's strategic initiatives being undertaken by the Governor in these areas of critical infrastructures and the smart grid. Highlights of his panel remarks included:

- Governor Neil Abercrombie has a full plate of strategic initiatives, one of which is to oversee a major transformation within the State of Hawaii by overhauling all of our technologies, and updating 30-40 year old systems and processes.
- Hawaii is a closed loop, and has strategic importance beyond Hawaii itself, and also for the nation. As we recognize there are silos, in trying to address some of these challenges, Hawaii has a really good opportunity to address these things right away. In this instance, we are talking about things that are interconnected such as critical infrastructure, in a holistic way, and not just spending money on these matters.
- Governor Abercrombie, when he came to office in his first term, set out to immediately transform government, which is bigger than just government, and on adopting a community approach.
- One of his initiatives is to bring together the 15 critical infrastructures in the state and address that in a holistic matter, and provide coordination across the community to address these issues. One of these areas is the energy grid (smart grid), but it extends to providing broadband to the schools, workforce development, emergency operations, water supply and sewage. These are all critical areas that matter to the state, but also for PACOM and across the nation.
- This is an opportunity with all these things going on to actually put it together in a strategic way that makes sense for everyone. We are working closely with PACOM, and the AIRS team, and my role is to support them as much as I can from the government side.
- In context to sensemaking, there are so many positives but also real consequences in doing all of this, and this is not a conceptual idea that does not impact people. It impacts all 1.4 million residents of Hawaii. Is there any reason for not doing sense making? We should not do it if we are not going to do it right. We are trying to diversify the critical pieces of our critical infrastructure and how we interact with those stakeholders, including HECO which is very important.
- When we talk about resiliency and sustainability, it is not a zero sum game. If you are going resiliency and sustainability as a zero sum game, you not approaching resiliency and sustainability correctly in closed looped island. As we throw out these ideas and solutions, the thing we need to think about is what is the best way to implement this, who do we need to work with, what types of communications do we have to have with these folks, how do we bring everyone onboard, how do we help to bring all the stakeholders together so they can come to the table to help us out? Obviously in this instance, when you are talking about the energy grid, it is heavily dependent upon HECO…and our residents have relied on HECO for 100's of years. We want them to come onboard and help us out because we are all vested in it. That is critical, as this is not a game, this is real life and lot is at stake, and lots of residents are impacted by this.

Mr. Jeffrey Katz, CTO, IBM Energies and Utilities

Mr. Jeff Katz provided an overview of some of the State of Hawaii's smart grid initiatives that are currently underway, and insights on the need for extra sensing and control of the grid in the introduction of renewables. Highlights of his panel remarks included:

- I'd first like to commend Hawaiian Electric for their smart grid initiative, and we supported them and others around the nation. It has been my observation over the years that no two have started the same way. I noted and commend HECO for not limiting this to smart meters, but including the renewable

energy project into the plans and actioon. Most utilities would cringe at the percentage the Governor of Hawaii is pursuing, as they know what its impact will be for the smart grid.

- What we found in smart grid projects is that data integration is so important. Some projects start off by not adding one new sensor to the grid, but actually getting a lot of the utilities engineers together in one place and getting all types of data – technical, system, and minute by minute operational data – then synthesizing it and putting it together and finding nuggets of information in there.
- A key concept is "sense, respond, and learn," and there is a lot of data mining that can be done in systems. All data is not numeric, and much of value can be found in maintenance reports, as this can help the utility learn what patterns of failure happen. In every utility you can find somebody (near retirement for example) that does all this automatically, but the experience and data is hard to pry out of people, and it is hard because it is not something people tend to organize.
- Systems with the smart grid mapped to them not only improve the minute-by-minute operations of the grid, but also learns by noting what operator responses were done, and what were the conditions that brought them to fail. Once these systems fail, you can go back to check the minutia of data that the operators did not see to assess if there were any indicators of that failure. These are some of the concepts of the smarter grid.
- Grids were made for mass generations and for mass distributions. There are two aspects of that. One is when you turn the power plant on, most of the time it runs. The variability brought on by renewables and the idea of power being injected into the grid that is all new to the grid that needs to be handled. Many might ask who needs a smarter grid? If you want more reliability, especially for digital electronics in homes that are more sensitive, compared to the variations of power quality and equipment people used to have in their homes, and if you want to know what to do if there is a big cloud going overhead the island and all these solar panels are no longer generating the same power levels at the moment, you need a grid that is reading all the conditions and responding more rapidly. In most coal fired power plants, you can't press the accelerator and go 200Mwatts to 250Mwatts to make up the gap.
- There is a good side to renewable energy, but a more engineering challenge to keeping all the lights on and all the power available all the time in dealing with this, and this is a major motivator for smarter grids that HECO is working on. The above considerations provided to highlight some of the relationships that are needed for extra sensing and control of the grid in the introduction of renewables.
- In following up on Shari's comments on "black starts," starting up a conventional steam fired generator is a difficult, complex task, and you need power to start up your power plant. It is like a combustible engine in a car, a battery is needed to start the engine. Alternate generating plants are feeding the same grid on the main island. Literally, what this means each of the generator shafts going around have to be in lock step, but mechanically they do not. So you bring on one generating plant, and getting it back up to speed, then you bring the next one on, and that has to be absolutely synchronized. Starting up from scratch is difficult, and all generators have to be synchronized at all times.
- As for cyber security, at IBM we do not look at the stack of firewalls we can have, because the electric grid is so distributed, especially with more intelligent sub-stations and smarter grid. It is about looking at anomalous behavior through the grid, kind of sensing everything and then categorizing events. If it looks like an operational problem, let's send it to the control room. If this looks like a maintenance problem, let's send it to maintenance. If this does not look probable at all, let's send it to security.

Aside from the audit logs, one can look at network flow, and start piecing together all the data, including SCADA and multiple sensor data, to obtain "enhanced shared situational awareness." That is really what we are trying to do with smart grid security, taking all the information from the smart devices and their behavior. What if you have 3 substations fed off the same main feed (higher voltage device), and all three seem to go down in 20 minutes. You might want to find out what was in common between them…if two failed and one going fine, and no data is indicating there was an over voltage or over current, you might want to get someone engaged and investigate as this might be something you don't see in normal operations.

- This is why "sense, respond, and learn" is important, because when you start to bring into play cognitive systems, you can now see patterns of unusual behavior on the grid and potential predecessors to it. You have this pattern of cognitive learning and behavior, and leveraging the real time analytics of massive amounts of data collected. Now we can use everything to learn and experience and not just go into a reactionary mode.
- In predictive maintenance, we can now saw, the last time I saw this rapid a temperature rise in this transformer resulted in a fault the next day. If it happens again, maybe we can now get a crew out there ahead of time and fix it to prevent an outage.

Mr. Wesley Rhodes, IBM

Mr. Wes Rhodes provided some perspectives on sensors, and specifically their importance in sense and respond. Highlights of his panel remarks (in which he attempted to put himself into the shoes of Senator English) included:

- The Senator would say (if he was here) that one of his priorities is to positively impact people, ensuring that food is available, electricity is on, water is available, sewers work, that you have connectivity to the outside to communicate with family.
- In looking at a couple points in history, in 1946 there was a 8.0 magnitude earthquake in the Aleutians that initiated a Pacific wide tsunami. When it came to sensemaking, the first person to see the tsunami was a Captain of a ship outside Hawaii, 4 ½ hours later than when it started, and only minutes before it hit Hawaii. 159 people were killed, and there was massive devastation across each of the islands. 22,700 miles traveled in 4 ½ hours. In sense and respond, and respond, minutes matter.
- In looking at the 2011 Japan Earthquake (magnitude 9) and the savage tsunami it unleashed, there was a "significant impact to people," as were an estimated 4.4 million people without electricity, 1.5 million people without water, and $235 billion of damage.
- What we learned from the 1946 Aleutian earthquake and ensuing tsunami was a sense and respond lesson. After this event, the Pacific Tsunami Warning Center was created to let us know what is coming and a little extra warning. Japan had a 1,000 seismometers that could understand when the earthquake was coming, and with a good amount of fidelity. That actually paid off, as they had only one minute of warning to the general public before the earthquake hit. In that one minute, however, hundreds of lives were saved (as was reported).
- Sense and respond has three perspectives, to include:
    - Sense – gathering more information about our environment (variety of sensors, and for machines its data)

    - Interpreting the data – which gives meaning to the information we collected. Now the more information you got (such as big data), the more insights we have about our environment, and more clarity and better perception of my environment
    - Decided what to do – acting on that data
- In interpreting the data, we got to bring computing to the edge, where the data is generated. Big data is tough to move, and takes time to move around. So we grab onto the data as soon as we possibly can, write analytics to understand and interpret what the data might mean, and then take local action. If I can take action quickly, then I can mitigate with least possible harm, action, and cost.
- Now, with more and more analytics, I get not only insight into what is going on, but I also can pass insights to other computers later on that can fuze with other data to get even more insight.
- What is the end point in all of this? If I can mitigate risk and cost, if I can start planning and even be the harbinger of planning, and take action right then, then I positively impact people.
- I believe that is what Senator English would say, "people is where it is all at!"
- In regards to sense making, there is both the good and the bad for doing sense making.
    - Good thing – it is typically one of my lowest cost options available, as I can invest lots of dollars in assets and not get the benefits associated with sense and respond
    - Bad things – what if I don't at this thing holistically, and buy some sense and respond systems, put the stuff in, and then don't use it…because I don't want to do the rest of the work…like put the processes in, and do the hard engineering work to really glean information from that or to be able to see and visualize that and to take advantage of that. I just wasted my money. Additionally, what if after taking the steps to put in the sensemaking assets I didn't take steps to engineer security into the solutions, I actually increased the amount of risk associated with organization.

Mr. Jim Hackett, EVP, Mehta Tech

Mr. Jim Hackett shared some perspectives on technologies already in place, and how HECO can leverage these and become a "living lab" as they move ahead with their demonstration project. Highlights of his panel remarks included:

- With respect to what HECO is doing to take advantage of technology in place, I am aware of types of technology they got out there with my experience with utilities across North America.
- I think it is really important when HECO started talking about with their demonstration project, and it is important to understand what it is that they are trying to achieve overall. There are specific things obviously of importance to them, but at the same time it is important to give a larger picture of where they are going, and what they might benefit from in looking at the data.
- When talking about sensors, such as smart meters, power quality devices, and phased streaming capability. There are not many utilities connected using broadband, the capability for some monitoring may be there, but may not directly useful at this point. There are systems that take analog and digital information, do some processing at the control station, and then streaming that data off site. There is some low hanging fruit out there that HECO can obtain.
- It comes back to what HECO wants to do with this technology? What is your initial goal, and long term targets? I believe there is a mix of sensor data in this to include smart meters, not just looking down at the distribution system, but trying to see what this has on your sub-transmission systems and high

voltage transmission systems, especially if you have large systems connected to those high voltage transmission systems.

- There are sensors out there already in place to capture data, but data is just one thing. When you look at what we have experienced since 2003, and this is truly a North America initiative, the government encouraged the utilities to put synchophasors to provide a real-time measurement of electrical quantities from across the power system, turning data into information.
- HECO has a real opportunity to take their demonstration project and reap the awards of the work done by other utilities and people in the industry, and use as starting point. As time progresses, we are collectively smarter. What is going to happen is that are things that are unique/special to Hawaii, such as a unique grid and new ways to monitor and detect oscillations. Once HECO puts these sensors (monitors) in place, and especially if they are able to do this in real time, there in a great opportunity to do pattern recognition of the data obtained, and see things they did not expect to see and help them address issues before they become a disaster. It will enable to see things holistically, and how their overall systems on each island react (which likely is differently).
- In providing an example, back in the late 1990's in Ontario, in Niagara Falls, at a substation where the control building was burned down, we took an experimental control station and put it in which had real time monitoring and recording of what was going on. Not just in the transmission lines, but also what was going on in the distribution end, which was primarily industrial. This was the first time we did this in real time, and focused on the distribution system. What we found out was that there were things on the distribution system that people would not believe at first, and who believed the equipment was wrong, and anomalies could not be explained.
- I am going to predict HECO will be a "living lab" and if you are able to share your experiences, you will be invited to share this knowledge with the rest of the community.
- In context to synchophasors and phaser measurement units (PMU), in looking at oscilloscopes on power lines, the theory is that you will see "nice little sine waves." When you have long distance power (distribution) lines, any time things happen on the grid things are not as time synchronized when things start at one location and other things happen further down the line, and you start to see differentials. The difference in these phase angles indicate something, and until recently were not even measured. So PMUs (synonymous with synchophasors) is a device that can measure these time differentials between these AC waveforms in different parts of the grid. It is almost like a tsunami warning system, that when there is a big disparity, that is a trigger for a problem. The synchophasors let you know about the instabilities, which is pertinent to renewable energy because energy generation fluctuates on the grid that can introduce instabilities.
- A major fault in a major transmission station can introduce instability on the grid as well. You actually have oscillations (like hearing resonance in a room for example, an acoustic wave), and get the same effect transmitting electricity over multiple power lines. Without these synchophasers you could not tell that these instabilities are happening and handle faults on the grid, which is an engineering challenge for renewable energy.

CYBER X-GAMES OVERVIEW

Cyber Endeavour 2014 provided an operational environment for exercising offensive and defensive cyber techniques and practices during the Cyber X-Games which consisted of individual and team cyber-attack and cyber-defend competitions. The theme for the 2014 Cyber X-Games was "SCADA System Defense."

As discussed in the Cyber Endeavour 2014 report, a common theme was that Cyberspace Operations was a "team sport," and a mission area enabled by Public Private Partnerships. Cyber X-Games coordinators ensured each participant to Cyber Endeavour 2014, as was the case in Cyber Endeavour 2011 and 2012, had an opportunity to participate in these individual and team cyber-attack and defend competitions.

Cyber X-Games were designed as a training and evaluation tool for the Army Reserve Cyber Operations Group's soldiers, and this exercise is used to help prepare Cyber Soldiers to defend critical infrastructure components; understand the impacts to systems, protocols, and familiarization with the tools associated with critical infrastructure; think in a defense and agile manner while analyzing and applying technical cyber counter measures to prevent threat actors from achieving catastrophic results from attack; and evaluation of Cyber Warrior capabilities.

In support of the Cyber X-Games, the ARCOG established four teams who collectively were responsible for successfully planning and executing this event, to include:

- ARCOG Cyber Protection Team (CPT) "Blue Team" responsible for training, mission planning procedures, team dynamics, and defense methods. The Blue Team was charged with conducting intelligence preparation of the battlefield (IPB), building and employing missing network infrastructure, and securing and defending the network/network components.
- ARCOG Aggressors "Red Team" responsible for motivation, capabilities, implementation of exploits, and methodology
- ARCOG "White Team" responsible for range operations, controlling, and planning
- ARCOG "Green Team" responsible for range support, running the range, and computers/networks

The ARCOG developed the scenario that included a fictitious Shire Electric Company experiencing cyber attacks by possible threat actors, which resulted in the ARCOG Cyber Protection Teams being brought in to defend against further attacks and remove any advanced persistent threat (APT) agents within a substation (Acme Power Company) IT infrastructure and enhance the security posture. In this scenario, CPT leadership worked with the business owner in determining the critical assets, such as the Industrial Control System (ICS), as well as determining pre-approved actions and reserving the right to make informed decisions based on the advice of the CPT Mission Commander (MC) on any activities that may disrupt business operations. Cyber X-Games leadership established and disseminated the following rules of engagement:

- All management networks are off limits to play
- Lariat network and user password is out of play

- Blue Team and White Team wiki and chat are out of play to the Red Team
- Blue Team must maintain CIA with substation
- Blue Team historians must be able to connect to ICS specified equipment provided by business owner
- External access to/from ICS is not controlled
- If it is not chatted, it did not happen
- Observers and OCs are there to help – please provide clarifications when needed
- Red Team may receive some advice from White Team so they don't chase too many "rabbit holes"
- Blue Team will be playing whack-a-mole and chasing rabbits down rabbit holes
- Limited intelligence will be available to the Blue Team
- Blue Team may coordinate with the business owner for additional assets and security
- Have fun

Cyber X-Games participants used several tools to assist them in performing their missions to include Nmap, Tcpdump, Wireshark, Metasploit, SSH & Telnet clients, VNC & RDP clients, Cisco IOS Commands, and Kali.

Cyber X-Games was a four day event that included:

- Day 0 – the Blue Team arrived and briefed, and met with the business owner
- Day 1 – Medium Lever Threat (Organized Chaos) that included the substation being vulnerable; network scanning by the Red Team (detected by the Blue Team); and phishing and other malicious outside activities.
- Day 2 – Medium Level and Quiet Advanced Persistent Threat that included the substation being vulnerable and susceptible to more sophisticated attacks; Red Quiet ATPs, Callbacks, Beaconing, and exfil; and Red phishing and other malicious outside activities.
- Day 3 – Medium Level and Malicious Advanced Persistent Threat that included the substation being vulnerable and subject to more even more sophisticated and malicious attacks; Red Quiet ATPs, Callbacks, Beaconing, and exfil; and the Red Team leaving the network in any state. Note: due to network issues, the ARCOG ran out of time to complete all planned Day 3 activities.

CYBER X-GAMES RESULTS

The ARCOG Commander, individual IOC Commanders, and Cyber X-Games Planners and Coordinators considered Cyber X-Games a **SUCCESS**. Some of the key (positive) takeaways from this event included:

- The Blue Team was full of smart, motivated people
- Once the event started, teams from all Information Operations Centers (IOC) came together for a common purpose
- This was a good training model, and everyone involved got experience from using real world tools during a simulated cyber attack (and really learned something)

Some of the key (negative) takeaways were:

- Learn from initial network difficulties to get more training value out of the limited time.
- This was the first time ARCOG used this network, and there were set-up challenges
- Not enough time on keyboard

CMU/SEI conducted a formal assessment of the ARCOG Blue Team in the following section. The following, however, provides an initial leadership of the "three ups and downs" of this event, as well as Cyber Training Team (CTT) perspectives on the role of Cyber X-Games in the ARCOG's transition from Mission Support Teams (MST) to Cyber Protection Teams (CPT).

Three Ups

- Multiple SMEs came together for a common cause
- Interactive exercise is more than just technical, it was very dynamic
- Difficulty to penetrate with non-Mehta Tech software access to gain access to the substation, while the disgruntled/insider threat was still significant

Three Downs (Singing the Blues)

- Balance between range set-ups and operations, tools setup was difficult with CPT drop in philosophy (limited Green Team/Cell resources)
- Need personnel, process, and tools to understand network and maintain up system status
- Never enough time (did not complete all Day 3 planned activities)

Cyber Training Team (CTT) Comments and Evaluation

- The CTT evaluated how the ARCOG transitioned from MST to CPT
- Within the ARCOG, there are five battalions and ten CPTs
- A challenge for us is how to command and control, and train, very smart, motivated people
- Today we have pick-up teams, not completed teams, who we witnessed at Cyber X-Games "storming and norming"
- The exercise to do the exercise is not the exercise. Getting to build a network and defend the network is to test leadership abilities. It is about building the "middleware," throwing people together and then seeing what leadership lessons we could tease of that.
- The development (and transition) of the CPT from MST will be a time phased, five year process.
- In Year 1, this is where we look at what we have – how many people, how many skills do they have, how much have they been trained, and in building individual skills mapped to gaps. This would also be the phase of small team leadership skill development within the CPT.
- In Years 2 – 4, this is where we build the middleware, and leadership's ability to fully employ its smart people; develop tactics, techniques and procedures (TTP) to handle certain types of issues; handle more technical and challenging tasks such as hardening the network; and most importantly, bring the Blue, White and Green Teams together and galvanize as a cohesive unit under more solid, confident leaders.
- In Year 5, this is where we get to the "culminating exercise," formal certification of the CPT, and deployments; where we can go to our active duty counterparts such as at Fort Gordon and focus on "steering the course" so the active and reserve components work on the same sheet of music; and coordinate with our Air Force, Navy, and Marine Corps reserve components.
- In looking at Cyber X-Games 2014, we threw people into teams, and built leadership structures to lead those teams through these events. Whether or not folks were successful on individual tasks was noted, but what was really important was how we all worked together as a team, and how we could capture best practices and lessons learned and then apply them in our model across all CPTs.
- One of our objectives was to be "reproduceable," bringing in the right people who can make the score, and then shifting them around the other teams.

- Another of our objectives was to create teams comprised of multiple IOCs in order to see how they interacted and for observing cross team dynamics.
- Cyber X-Games is an opportunity for the IOCs to take one step closer to have functional, effective CPTs, and should not squander these outstanding training opportunities.

CYBER X-GAMES TEAM ASSESSMENT

Jennifer Cowley, PhD, Human Factors Psychologist
Roger Beard, CISSP, Information Assurance Analyst,
CERT Division | Software Engineering Institute, Carnegie Mellon University

Background: Dr. Cowley and Mr. Beard scored the cybersecurity blue team at the X-Games event all week.

Problem: A team of experts is not an expert team. Beyond team member cybersecurity competencies, other team member attributes collectively impact whether or not a team will advance. Our research involves the identification and measure of those attributes.

We were tasked at the 2014 Cyber Endeavor X-Games to devise and beta test a team scoring system on teamwork, leadership and soldiering skills. This report discusses the team scoring method and results.

Method:

Materials: Team performance is multi-dimensional. While many team assessments exclusively evaluate the level of team and individual cybersecurity technical competence, we focus on other performance dimensions like leadership, teamwork and soldiering skills. Each performance dimension has defining elements and respective behavioral competencies that we targeted in our team scoring strategy.

Based on prior research findings from aviation and health care surgical teams, we generated this list of elements and respective team behavioral competencies that have been identified in high-performing teams (see Table 1). Not all behavioral competencies generalize to cybersecurity teams; hence, we were also evaluating the validity of these competencies. All behavioral competencies were listed in behavioral observational forms (BOS); an assessment strategy used by outside observers. All behaviors were assigned a BOS point value and when a behavior was identified, the points were awarded. The percentage of points earned out of the total points possible on each BOS became the BOS score. Not all behaviors were of equal importance. Based on the opinions of the senior leadership, behaviors more critical to mission success were weighted more heavily (in the points value) than others. The total score of the team was the average of all scores on BOS forms.

We also collected simulation-generated team performance data to identify the validity of our team scoring strategy for metric refinements.

Table 1 – List of Team Performance Dimension, Respective Elements and Competencies Evaluated

Team Performance Dimension	***Element***	***Example Behavioural Competency***
Leadership	Identifying and utilising team assets	• knowledge of task-specific teammate competencies
	Problem identification	• Has appropriate level of team situation awareness to ID problems with
	Prioritising strategies and respective work tasking	• Appropriate cue-strategy associations
	Task assignment and task sequencing	• Reviews task assignments with team and debugs process
	Providing & enforce team norms and standards	• Sets boundaries for good and poor behaviour and performance a priori
	Workload assessment	• Metacognition required for workload imbalance ID and rebalance.
	Debriefing quality	• Guide debriefings into non-punitive, learning experiences
	Personality and bed side manner	• Dynamically moves between different leadership styles according to team circumstances
Team Work	Coordination	• Strategizes ways to facilitate performance of other teammates job
	Cooperation	• Task interleaving between team members is rehearsed a priori
	Communication patterns	• Acknowledges and repeats messages to ensure understanding by receiver
	Back up Behaviour	• Helps overburdened teammates
	Team Situation Awareness (SA)	• Teammates actively participates in building team SA
	Decision Making	• Teammates use strategies to minimize group think
	Execution	• Mutual performance monitoring and feedback self-correction
	Feedback	• Re-evaluates task execution in relation to achieving mission
	Team Attitudes	• Mutual trust
Soldiering Skills (according to US Army Doctrine)	Quality of Rehearsals	• Team workflow is established
	Quality of After Action Reviews	• New strategies are rehearsed
	Troop Leading Procedures	• Back briefs and confirmation briefs occur
	IPB, Threat Modeling and Predicting Threat Course of Action	• Threat model includes an evaluation of threat's strengths, weakness, vulnerabilities, and threat's high value targets.

Procedure: The mission commander was briefed on all elements being assessed a priori to the start of X-games. Each day, the team received a score for the performance of that day. At the end of the day, the mission commander and the deputy received feedback from the research staff on the team's performance.

Results:

Across the three day X-Game event, the blue team scored at the bottom of the intermediate range for all three dimensions. The team was a bit stronger at teamwork skills than leadership and soldiering skills. We offer explanations below.

Overall, the team was professional and well-mannered which can be important for mission success. Intra-team conflicts were minimal. To an outside, occasional observer, the team appeared to be advanced at

teamwork and leadership skills but the research staff had a slightly different perception. A calm, professional team demeanor has a tendency to mask the lack of a centralized, organized leadership. This lacking would quickly become evident had a catastrophic adversarial attack obliterated team personnel and network capabilities in the first few hours of the X-Games. We recognize that leadership is not exclusive to the mission command but includes all team members. Therefore, we were evaluating the leadership, whether assigned or emergent, to perform these behaviors we expect to see in advanced teams with centralized leadership. These include:

1. An initial inventory of team expertise and assets which is then disseminated to rest of the team
2. The establishment of modifiable workflow and communication patterns before the work begins. This can reduce chaos and response times to adversarial attacks.
3. A discussion of how to achieve the blue-team mission given the threat mission, the likely threat courses of action (COA), the battlefield constraints, etc.
4. A rehearsal of team's response to threat COAs including what tools would surface information related to threat COAs (including the implementation of distractions), work coordination amongst sub-teams and how mission success can be identified. Adversaries often use distracting tactics to lure blue-teams into playing "whack-a-mole" which obfuscates the work tasking necessary for mission accomplishment. Because distractions can be sophisticated, the entire team needs to discuss adversarial distraction tactics and how to identify them in various tools. This helps prioritize work that will lead to mission accomplishment over work that results from adversarial distractions.
5. The generation of a display (e.g., a common operating picture, etc.) facilitating team situation awareness. This should include information like the chain of command, a summary of the key events that have occurred and are occurring, and how close the team is from achieving the mission (e.g., a burn-down chart). It is <u>not</u> a display of raw data like chat logs, log files, etc.; it is the multi-modal display of analytical results that explain: 1) what the team is perceiving now, 2) what that perception means to the entire team and 3) what future events can be predicted that are relevant to mission accomplishment.

However, a balanced view of the team is warranted. Our assessments were based on behaviors that expert teams have that are not always present in novice and intermediate teams. Many of the behaviors we targeted were those that develop through several years of repeated practice; yet cybersecurity military teams are comparatively nascent with limited practice time. Therefore, we would expect them to score in the novice or intermediate range. Even though our X-Games team had no prior work history together as a single unit, about half of our behaviors were of teams that typically have no prior work history together (e.g., commercial aviation and health care teams). Therefore, our scoring system should not penalize teams with little or not work history. Finally, we understand that the simulation was not properly configured with necessary tools required for normal cybersecurity operations; therefore, teams were working on tool install and configuration on the first and second day of the exercise, making it difficult to concentrate on teamwork and leadership.

SECTION THREE – CYBER ENDEAVOUR 2014 / CYBER X-GAMES SPONSORS

PLATINUM SPONSORS

We would like to acknowledge and express our sincerest appreciation to the following three platinum sponsors who played a critical role in making Cyber Endeavour 2014 and Cyber X-Games a success.

- **Mehta Tech**
- **IBM**
- **SynerScope**

Mehta Tech, IBM, and Synerscope were Cyber Endeavour 2014 Platinum Sponsors for the Cyber X-Games and Social Event. They are also members of the Hawaii DoD's Public Private Partnership (P3I) Consortium.

The State of Hawaii's Department of Defense, which includes State Civil Defense and the Office of Homeland Security, is collaborating with **IBM**, **Mehta Tech Inc.**, **Synerscope**, and U.S. Pacific Command to study the potential enhancement of the security, sustainability, and resiliency of critical infrastructure, such as the electrical grid. The collaboration among academia, private industry, and state and federal governments will explore ways of applying *Big Analytics* to better predict potential risks and issues. The industry collaborators (IBM i2/IBM Network Science Research Center, Mehta Tech Inc., and Synerscope) will use advanced network/ relationship science principles and related Smart Grid technologies to provide necessary solutions and services focused upon *Big Data* acquisition and *Big Analytics*. "The collaboration allows us to combine the strengths of the various public, private, and civil organizations that have an interest in the challenges we face to our critical infrastructure and possibly recommend solutions that will make Hawaii a more resilient community," said Major General Darryll Wong, The Adjutant General of Hawaii, Director of State Civil Defense and Homeland Security Advisor. By using an integrated approach that incorporates both operational and transformational information technologies, the collaborators will examine how to improve the overall resiliency for Hawaii, such as grid reliability. As part of this initiative, the collaborators will evaluate **Synerscope**'s Forbes-feted visualization capabilities and **IBM**'s Sensemaking as well as **IBM**'s Watson Foundation technologies of Jeopardy! acclaim, which will apply *Big Analytics* atop the *Big Data* derived from **Mehta Tech Inc.**'s Irwin Phasor Measurement Unit capabilities so as to generate *Big Insights*.

Mehta Tech, IBM, and Synerscope also presented a series of demonstrations at Cyber Endeavour 2014.

We would like to acknowledge and express our sincerest appreciation to the following gold corporate sponsor who also played a critical role in making Cyber Endeavour 2014 a success.

- **Endgame Inc** ENDGAME.

Endgame was a Cyber Endeavour 2014 Gold Sponsor for our Continental Breakfasts and Snacks.

Endgame provides cyber security capabilities that address some of the most complex national security and defense challenges facing the nation. Our core capabilities use data-science and cutting-edge technology to give our customers real-time visibility across their digital domains, and our ecosystem of applications use that insight to solve a wide array of security problems. Endgame allows you to see what others can't, and to take control of your connected world.

Endgame presented the following topics at Cyber Endeavour 2014:

- June 24: Endgame Demo - Take Control: Understanding the Adversary's Network
- June 25: Endgame Demo - Take Control: Defending Your Network
- June 26: Endgame Demo - Take Control: Leveraging Cyber for Kinetic Operations

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