# CYBER ENDEAVOUR 2012

JUNE 26-28, 2012

"Operations in Cloud and Cellular Networks"

# FINAL REPORT

AUGUST 28, 2012

# FOREWORD

The Joint and Special Troops Support Command (JSTSC) Army Reserve Information Operations Command (ARIOC), Naval Postgraduate School Information Operations Center for Research, and IO Centric Solutions are pleased to present this product to all participants of Cyber Endeavour 2012. This report synthesizes materials from our academic and technical co-chairs, panels, special guest presentations, and break-out sessions. 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 2012 was attended by an estimated 150 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 is **"Operations in Cloud and Cellular Networks,"** with the following threads that served as a basis for our extended panels, and general and open-forum (workshop) sessions:

- Cyber Policy and Operations
- Cyber Law and Ethics
- Educating the Work Force: Balancing the Current Force with Generation Y
- Developing, Operationalizing, and Assuring Cloud and Cellular Systems, Networks and Architectures

Cyber Endeavour 2012 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. This year's overall champion was the team from Scientific Research Corporation (SRC). Based on recommendations received from participants, the following areas were chosen as the three break-out sessions that were held on the last day:

- Training and Education
- Identifying and Protecting Intellectual Property
- Cyber and Information Operations Convergence and Relationships

We would like to express their sincerest thanks to our co-chairs, moderators, special guest speakers, panel members, participants, and volunteers who collectively helped make Cyber Endeavour 2012 a huge success. Our particular thanks and appreciation go out to the following corporate sponsors for their generosity and support.

- L-3 (Gold Sponsor)
- Endgame Systems (Gold Sponsor)
- Oceus Networks (Gold Sponsor)
- Sentar / Athena Joint Venture (Silver Sponsor)

We anticipate this report will serve as an important reference document for you and your parent organizations, and to encourage you to continue the dialogue on "Operations in Cloud and Cellular Networks."

Thank you, and hope to see everyone at Cyber Endeavour 2013!

# TABLE OF CONTENTS

**Foreword** 2

**Table of Contents** 3

**Introductory Remarks** 5

CE2012 Academic Co-Chair – NPS IO Center for Research – Dr. Hy Rothstein 5

CE2012 Technical Co-Chair – JSTSC / ARIOC – COL Schroeder/ COL John Diaz (USAR) 6

**Panel I – Cyber Policy and Operations** 8

U.S. Cyber Command – Dynamic Network Defense Operations (J34) – CAPT Robert Goodwin (USN) 8

U.S. Fleet Cyber Command/10th Fleet – DOD Joint Information Environment – CAPT James Imanian (USN) 9

Office of the Chief of Naval Operations – N2/N6 – Mr. Michael MacDonald 10

U.S. Special Operations Command – Information Assurance Division – Ms. Brenda Khoury 11

L-3 – Strategic Ventures – Col Marc Jamison (USAF Ret) 13

**Distinguished Guest Speakers** 15

Naval Postgraduate School –Department of Defense Analysis – Dr. John Arquilla 15

L-3 – Cyber Security and Innovations – COL Joel Bagnal (USA Ret) 16

**Panel II – Cyber Law and Ethics** 19

SAIC – Assistant Vice President / Chief Cybersecurity Technologist/Cyber Law Specialist – Mr. Gib Sorebo 19

Naval Postgraduate School – Department of Defense Analysis – Dr. Dorothy Denning 19

U.S. Department of Energy – Office of the General Counsel – LCDR (sel) Elliot Oxman (USN) 20

University of Nebraska College of Law – Space, Cyber, and Telecommunications Law – Mr. Jack Beard 22

**Distinguished Guest Speakers** 27

Chertoff Group, LLC – Managing Director and Chief Strategy Officer – Mr. Brian White 27

Google – Veterans Outreach – Mr. Harry Wingo 29

**Panel III – Educating the Workforce: Balancing the Current Force with Generation Y** 31

CE2012 Academic Co-Chair – NPS IO Center for Research – Dr. Hy Rothstein 31

Naval Postgraduate School – Department of Electrical and Computer Engineering – Dr. Deborah Goshorn 32

U.S. Cyber Command – Exercise and Training (J7) – Col George Lamont (USAF) 34

Naval Postgraduate School – Information Dominance Center for Excellence – CAPT (sel) Tim Unrein (USN) 36

National Institute of Standards and Technology–National Institute for Cyber Education – Dr. Ernest McDuffie 37

U.S. Army War College – Command, Control and Cyberspace Group – Mr. William (Bill) Waddell 40

**NPS Defense Analysis Department CORE Laboratory Overview and Capabilities** 44

Naval Postgraduate School – Department of Defense Analysis CORE Lab – COL Greg Wilson (USA) / Team 44

**Panel IV – Developing, Operationalizing, and Assuring Cloud and Cellular Systems, Networks, Architectures** 49

HQ Air Force ISR Agency – Air Force DCGS Program – Mr. Roberto Sandoval 49

IBM – Systems Security Division – Mr. John McLaughlin 50

Oceus Networks – Chief Operating Officer – Mr. Randy Fuerst 52
Army Reserve Information Operations Command – WO1 Eddie Contreras (USAR) 54
**Distinguished Guest Speakers** 56
DARPA – Transformation Applications Program – Mr. Michael Lack 56
ServiceNow – Chief Technology Officer – Mr. Arne Josefsberg 58
**CE2012 Workshops (Break-Out Sessions)** 60
Training and Education 60
Identification and Protection of Intellectual Property 61
Cyber and Information Operations Convergence 62
**Cyber Endeavour 2012 Sponsors** 63

## Cyber Endeavour 2012 Academic Chair

*Dr. Hy Rothstein, Director, Department of Defense Information Operations Center for Research, Naval Postgraduate School*

Dr. Hy Rothstein welcomed Cyber Endeavour 2012 participants and acknowledged the four corporate sponsors, then opened Cyber Endeavour 2012 with five points for participants to consider as we focus on "Operations in Cloud and Cellular Networks." Highlights of his comments include:

1. **Cyberspace touches every one of us, and everything we do**. Vulnerabilities have been created by our reliance on cyberspace, and these vulnerabilities affect nations, private organizations, private organizations, and civil liberties. The Internet is the largest part of cyberspace – we rely on it and it is one of our biggest vulnerabilities (e.g., intrusions into critical systems and infrastructures, cyber theft, theft of intellectual property, etc.). These vulnerabilities undermine U.S. confidence in its information systems, and also undermine our national and economic security.

2. **Government has a responsibility to identify and address these vulnerabilities in a way we can all benefit from information technology.** The jury is still out on how well the government is currently organized and capable of dealing with the increased risks and vulnerabilities.

3. **Information and communications that exist today are primarily owned by the commercial sector,** both national and international. As a result, addressing these vulnerabilities requires public-private partnerships at the national and international level.

4. **Cyberspace operations include policy, operations, and education, and encompass a full range of issues very familiar to a "Cold War" warrior.** Some of these issues include threat reduction, vulnerability reduction, deterrence, and international agents. Like the Cold War, experts from a broad section of government, industry and academia have a role in ensuring we have agile, resilient networks and systems.

5. **Cyberspace is important, but not the only thing within the Information Domain, and actually not the most important.** The wars in Afghanistan and Iraq, broadly defined, and the roles cyber warfare has (or has not) played is one of the reasons Cyber Endeavour 2012 is being held. The infrastructure (cyberspace) is important, but not the only thing within the information domain. Substance matters and ideas matter. Ideas have a particular vital role during war, and the U.S. has obligations to friends, partners, and enemies. People need to know why we are fighting, and we also need to make sure that while technology helps, but this is not necessarily a technical challenge. While the U.S. had greater technology and the upper hand, cyberspace has not played a significant role to date. Whatever Cyber contributed has been insignificant to the outcome of these conflicts to date. While Cyber is important, substance is more critical and the narrative, the ideas and narratives we communicate on why we are involved in these conflicts, is much more important.

.

## Cyber Endeavour 2012 Technical Chair

*COL David Schroeder, USAR, Deputy Commander for Readiness, Joint and Special Troops Support Command (JSTSC)*

COL David Schroeder welcomed Cyber Endeavour 2012 participants, provided an overview of the JSTSC/ARIOC and actions they are undertaking to improve coordination and resourcing within the U.S. Army Reserves. Highlights of his comments include:

1. **Cyber is a Joint Affair.** While Cyber is a Joint Affair, Cyber is executed by the Services. There is a need for each particular service to establish enterprise relationships with their counterparts that are non-rigid, non-hierarchical, and non-stovepipe. They need to coordinate to ensure everyone moves in the same direction, combines its resources and capabilities, and reduce waste.

2. **The U.S. Army Cyber Community has three parts**. Active Duty, National Guard, and Army Reserves.

3. **The U.S. Army Reserves is federal, part time force**. The Army Reserves are a part time force that is nimble and ready to provide support to the Active Duty component, and all Department of Defense entities. Their unique combination of civilian and military backgrounds benefits DoD entities. They need Active Duty and DoD to understand that reservists are not full time military and they have civilian careers.

4. **The JSTSC has a host of capabilities – they are not just Cyber Warriors**. The JSTSC has capabilities in Cyber Law (Legal), Information Operations, and a broad spectrum of collaborative capabilities. They find and provide unique resources that leverage their troops' unique skills.

5. **Cyber Technology needs to be fully understood and leveraged to ensure combat effectiveness**. It is important that we work together with combat force protection organizations within DoD to ensure we have the capabilities to defend ourselves and carry out the fight. History has proven time and again that combat effectiveness is directly attributed to understanding and properly leveraging technology - we do not want to end up in a situation like the French in early WWII because of our stovepipes and/or being slow to react. The French, despite having numerous advanced technologies, were overtaken at Verdun by the Germans who fully understood, leveraged, and applied their technology with their Blitzkrieg tactics and overtook the French forces in ten days.

*COL John Diaz, USAR, Commander, Army Reserve Information Operations Command (ARIOC)*

COL John Diaz welcomed Cyber Endeavour 2012 participants, and emphasized how Cyber Endeavour is a great venue to share ideas, build upon what we know, and identify and clarify what we don't know. COL Diaz provided an overview of the Cyber Commander's Cup and Cyber X-Games, and how these events sharpen the development and training of ARIOC Cyber Warriors. Highlights of his comments include:

1. **ARIOC is a combat and cyber force multiplier**. The ARIOC was established in the 1990's by General Hensley, who recognized that cyber and information operations were not going away. The General saw the ARIOC as a ways and means to influence people in and through cyberspace.

2. **ARIOC is Army and Joint.** The ARIOC has five battalions of citizen soldiers in sixteen states, and performs services for Army and Joint commands to include Army Cyber Command and 2nd Army at Fort Belvoir, their primary customers.

3. **ARIOC Warriors are exercised and trained to fight in Cyber: Cyber Commander's Cup.** A primary evolution of ARIOC Cyber Warriors is the Cyber Commander's Cup, a competition that in 2012 was comprised of six teams who were tasked to fight (defense and offense) in a realistic, operational cyber environment, and engaged in four exercises over a three day. These teams collectively achieved their objectives in virtual networks, and future competitions will bring the fight into the cloud environment as ARIOC transitions their virtual networks to cloud platforms. These competitions support the development and maturation of Cyber tactics, techniques and procedures, and enhance Cyber training readiness. The Winner of the 2012 Commander's Cup was the Western Information Operations Command (WIOC), under the command of LTC Murray, in one of the closest competitions to date.

4. **Cyber X-Games – Bringing the Fight to the Community.** The ARIOC serves as the Technical Lead for Cyber X-Games, one of the primary components of Cyber Endeavour. Cyber X-Games provides an operational environment for exercising offensive and defensive cyber techniques and practices. Cyber X-Games consisted of the following cyber-attack and -defend competitions.
   - Targeted Response and Analysis Challenge - Network
   - Black Box Penetration Testing
   - Incident Detection and Reporting Challenge
   - Preventative and Defensive Measures

   Organizations that participated in the Cyber X-Games included ARIOC, NSA, USSOCOM, USCYBERCOM, Fort Gordon, Air Force Research Laboratory, Dell, McAfee, SecureWorks, and SRC. The 2012 Cyber X-Games Champion was Scientific Research Corporation (SRC).

# PANEL I – CYBER POLICY AND OPERATIONS

*CAPT Robert Goodwin, USN, Chief, Dynamic Network Defense Operations (J34),*
*U.S. Cyber Command*

CAPT Robert Goodwin served as the moderator for the first of four panels, and provided an overview of U.S. Cyber Command and the five key pillars (enduring principles) that are critical to winning the war in Cyber. Highlights of his panel remarks included:

1. **Enduring Principle 1 – Global Situational Awareness.** The first enduring principle is achieving global situational awareness, as you can't fight what you can't see. Global situational awareness is critical to maintaining a strategic and tactical understanding of the military cyberspace domain. It enables our decision makers to make risk decisions, and helps ensure prospective cyber activities do not interfere with ongoing operations. Six associated areas of interest to USCYBERCOM include:
    - Current and near term threat environment
    - Identifying global threat anomalies activity
    - Vulnerability of DoD systems and underlying infrastructure
    - Prioritizing key cyber factors, e.g., training, that allow operational risks in DoD networks
    - Current operational readiness and capability
    - Knowledge of ongoing operations

    USCYBERCOM relies on situational awareness at the local level with HBSS, with 80% of the feeds to SIPRNET and 0% for NIPRNET. Regional level situational awareness is problematic. DISA and NTOC collocation is a good idea when looking at boundary defenses. USCYBERCOM needs to know what the Combatant Commanders are doing at the perimeter level to complement efforts.

2. **Enduring Principle 2 – Authority to Act in Defense of the Nation.** The Authority to Act in Defense of the Nation is comprised of three primary authorities:
    - Department of Defense and Intelligence Community, with authorities to act in detection, prevention, and defense.
    - Federal Bureau of Investigation, with authorities to act in investigation, prevention, and response.
    - Department of Homeland Security, with authorities to act in resilience, preparation, and protection.

    We need authorities, legislation, and rules of engagement to support Cyberspace Operations. There are numerous policy and procedures that govern current operations. In order to thwart cyber attacks on the nation in near real time, as close to the point of origin, the appropriate authorities must be granted, and delegated to the right level for us to see, block, and maneuver against malicious activity. Authorities and policies need to enable, and not hinder, procedures to establish unity of effort (and preemptive responses in real time) with USCYBERCOM, NSA, and other Government agencies with these authorities.

3. **Enduring Principle 3 – Trained and Ready Cyber Teams.** We need teams to build capacity to conduct multiple operations in the Cyberspace domain that can defend DoD networks, defend critical infrastructure and the defense industrial base, and conduct contingency operations. Some USCYBERCOM training initiatives include identifying and integrating National Guard and Reserve components, as well as repurposing personnel (e.g., system administrators) to work more advanced, complex systems and tasks (e.g., Joint Information Environment).

4. **Enduring Principle 4 – Defensible Architecture.** The current infrastructure is not defensible. USCYBERCOM is coordinating across the services and agencies to make it more defensible, as the adversary continues to find avenues of approach faster than we can defend. Command and Control (C2) is critical to understanding the implications on the Global Information Grid (GIG) in order to take corrective action. The Joint Information Environment (JIE) is a key initiative that seeks IT Architecture effectiveness with the cloud and thin client. Keys to achieving a defensible architecture include:
    - Reducing the number of enclaves (attack surfaces)
    - Growing capability to rapidly reconfigure our networks
    - Providing mobile (secure) devices when forces need them

5. **Enduring Principle 5 – Operational Concepts.** Operational Concepts include USCYBERCOM detecting in Phase O, deterring in Crisis Phase, and defeating in Conflict Phase. We need to defend the .mil domain, and be ready to defend our nation's critical infrastructure and networks that are not .mil. Key aspects of this principle include:
    - See – situational awareness, common operating pictures, understanding adversary capabilities
    - Block – defense in depth, host computers and systems at network boundaries, hunting to conduct counter-reconnaissance to prevent adversary/insider threat access
    - Maneuver – maneuvering beyond our boundaries, seizing initiative to maneuver within friendly and adversary networks.

*CAPT James Imanian, USN, Lead, DoD Joint Information Environment, U.S. Fleet Cyber Command / U.S. Tenth Fleet*

CAPT James Imanian provided an overview of U.S. Fleet Cyber Command/U.S. Tenth Fleet, and discussed current FLTCYBERCOM/10th Fleet initiatives and burning issues. Highlights of his panel remarks included:

1. **Organization.** FLTCYBERCOM/10th Fleet was established in January 2010 as the first iteration on how the Navy mans, trains, and equips its forces and operates its networks. FLTCYBERCOM has Title 10, 50, and 14 authorities that give it some unique capabilities by consolidating these authorities that in the past were located in different commands. FLTCYBERCOM supports USCYBERCOM Offensive Cyber Operations, Defensive Cyber Operations, and DoD Information Network Operations (formerly DoD GIG Operations). FLTCYBERCOM is currently shifting resources from DoD GIG Operations to Offensive Cyber Operations. Within the Navy, FLTCYBERCOM Command is an Echelon II command under the CNO, and 10th Fleet is an Echelon III command.

2. **Policy.** FLTCYBERCOM/10th Fleet has many already in place, although they need some further delegation and definition.

3. **Challenge – Operating in Cloud and Cellular Networks.** The Cloud is not how the Navy operates, and the Cloud is seen as both IT and a Tool. What the Cloud does give the Navy is an ability to consolidate and enhance data centers and provide a service oriented architecture. The Navy and DoD are not there yet, although there is much FLTCYBERCOM/10th Fleet wants to do in the Cloud. Need to find a good end-state and application area, e.g., big data analytics.

4. **Current Initiative – Cyber C2.** Cyber C2 is a transitional model to find out what is needed at the COCOM level. FLTCYBERCOM serves an executive agent for COCOMs at the middle tier, day-to-day operational level, such as with the Fleet Combat Centers. In supporting USCYBERCOM, FLTCYBERCOM needs to provide a Joint Cyber Element, while the Navy also gives FLTCYBERCOM mission sets requiring the same people and skill sets.

5. **Current Initiative – Joint Information Environment (JIE).** JIE is sponsored and supported by the DoD CIO, USCYBERCOM, and Services. The primary goal of JIE is to collapse DoD networks so USCYBERCOM can manage the remaining few networks, and create a single common security architecture. JIE includes collapsing SIPRNET, and not just NIPRNET. JIE focuses on network normalization, network services, enterprise services, and governance. The adversary demands it, the budget control act is fact, and USCYBERCOM and Services cannot operate the way it does.

6. **Burning Issues.** Some of FLTCYBERCOM/10th Fleet burning issues include:
   - Cloud Security and information spillage. The Intelligence Community is well ahead of DoD on the Cloud. Need a secure, scalable model.
   - Mission partners. As classified domains collapse, the need to allow mission partners into these domains increases. Need classified security gateways instead of cross-domain solutions.
   - Development of Cyber talent. The U.S. may have 30,000 world class cyber warriors, but they need an estimated 300,000.

*Mr. Michael MacDonald, Office of the Chief of Naval Operations (N2/N6)*

Mr. Michael MacDonald, assisted by Zach Abraham of SPAWAR Systems Center Atlantic, provided an overview of ISR Lite, a foundation for the Navy Tactical Cloud. Highlights of their panel remarks included:

1. **ISR Lite is the foundation for the Navy Tactical Cloud**, which leverages and implements the NSA Cloud Reference Architecture within the Navy/Fleet environments. Policy and doctrine are being worked as the Navy moves forward.

2. **The Navy is taking the NSA Cloud Reference Architecture (IC Government Cloud)**, shrinking it to one rack, and configuring different variants so they can put it on a Carrier (ISR Heavy), Cruiser and Destroyer (ISR Lite), and Submarines and Aircraft (ISR Ultra Lite). ISR Lite is the innovation proposal that extends the NSA Cloud Reference Architecture to the tactical environment.

3. The **ISR Lite prototype is undergoing a Limited Objective Experiment (LOE),** which will initially be focused on ingesting sensor data from platforms (SIGINT, FMC, SLQ-32 EW, SPY Radar, etc.) with cyber limited (need to start with crawl). **The primary goal is to ensure that the NSA architecture for a Cloud Computing Environment (CCE) can be demonstrated in a tactical environment**. The LOE deals with five-six different sets of data and four different networks, which creates a Certification and Accreditation challenge. The LOE is limited in scope to prove relevance in a tactical environment, and will demonstrate the prototype's ability to organize data – ingest, store, control, and disseminate data to the DoD enterprise through a ghost machine interface. The LOE will include denied, degraded, and intermittent networks, and looks at ships that do not have high bandwidth connections and thus an inability to send all extracted data off the ship. The LOE will be conducted in disconnected (laboratory) environment with canned data the first time around. The next step includes conducting an Afloat LOE in an actual network connected environment, which will advance ISR Lite's TRL.

4. **ISR Lite capabilities and methodology.** ISR Lite enables Navy platforms to send more of what they collect with their sensors and systems off the ship by reducing what they collect to a meta-data subset. Transparency of TS/SCI, SECRET, and UNCLAS data is achieved by cell level tagging which provides more agility and security that general record tagging. The discovery set of that information (1kb) is sent off the ship to shore locations. Distributed queries by shore locations find the discovery meta-data first, and then shore locations request full data off the ship (as required). The ship sends full data where it is then re-ingested, and the shore location serves as the custodian (not owner) of the data.

5. **ISR Lite Widgets.** Widgets for the ghost machine (Denver) were developed by SSC Atlantic. The Navy is awaiting NSA governance for widget common model what will enable the Navy / SPAWAR to build that framework so widgets can be shared on a "store front." Nine widgets were developed for ISR Lite, to include FMB Playback, Searching and Display of Data, Mapping, etc. These were developed from a maritime perspective, to ensure maritime needs such as ships' movements through an AOR or the fusion of SIGINT/EW tracks into a Common Operating Picture are accommodated.

6. **ISR Lite Accreditations.** Accrediting ISR Lite will be challenging, as there are specific accreditations that are required to include the SIPRNET edge, JWICS, NSA Core Nodes, and NSA Gateway.

7. **ISR Lite Future**: With increased interest by the Navy and Fleet, ISR Lite would seek to expand it focus and thrusts to include adding FMB data, Enterprise data, IBS feeds, Combat systems, and C2 systems, and create a bridge that connects the Navy/Fleet tactical to strategic environment and aligns the National Enterprise to extract and provide back to organic platforms. ISR Lite would also have variants for the Carrier (ISR Heavy) and Submarines/Aircraft (ISR Ultra Lite). Building the talent for sailors to successfully operate ISR Lite and conducting forensic analysis is something "way out of the box" for what they normally do today.

*Ms. Brenda Khoury, Chief, Information Assurance Division, U.S. Special Operations Command*

Ms. Brenda Khoury provided an overview of what U.S. Special Operations Command (USSOCOM) looks like from an operational perspective and how USSOCOM supports that on the network side, then closed with issues they are currently working that tie into a number of issues discussed earlier in the panel. Highlights of her panel remarks included:

1. **USSOCOM – Operational Tempo**. Over the last 18 months, the USSOCOM OPTEMPO has been at its highest level in 25 years. There is an article in www.defensenetworkmedia.com that provides a Special Operations Year in Review on what has gone on across USSOCOM. USSOCOM deployments 10 years ago were few in number, and the number of nodes USSOCOM supported was even fewer. Today, there are 650-750 deployed nodes that are supported per day, and this does not account for garrison structures USSOCOM supports.
2. **USSOCOM – Global Combat Command.** USSOCOM has four Service Components – AFSOC, MARSOC, NSWC, USASOF – and six Theater Components that puts USSOCOM in a global position, one that is unique over the other GCCs.
3. **USSOCOM – SOF Provider.** USSOCOM is a Title 10 Special Operations Force (SOF) provider, and under MFP 11, has the authority to operate its own networks and provide networks when SOF units deploy. USSOCOM support 45 garrison locations and an estimated 66K personnel, 12K of which is a steadily deployed force.
4. **USSOCOM Tactical Employment of HBSS**. Everyone has a different definition of tactical. USSOCOM is more tactical because teams of 6-10 deploy to the field with what they carry on their back. This poses a challenge as a USSOCOM operational network provider, as USSOCOM troops are not necessarily trained in networks/defensive measures.
5. **USSOCOM CIO Responsibilities**. The USSOCOM CIO is responsible for purchasing IT equipment, Certification and Accreditation of field systems and networks, and integrating Service systems and connecting into them.
6. **Policy and Resourcing.** There are too many policies and the length of time to get policy to the field is laborious and slow. There are lots of developmental efforts that are creating networks that USSOCOM cannot touch.
7. **Burning Issues.** Some of USSOCOM burning issues include:
   - Mobility for the operator, and providing SOF Forces' devices that they can plug into networks
   - Command and Control networks
   - Technology availability – technology will be an enabler, but cannot be relied upon to be available
   - SOF forces need to also operate disconnected from the cloud network
   - There is little support from cellular environment (cell networks taken down when things go down during engagements)
   - Distributed data centers in the Cloud. Collapsing theaters into a single domain creates interesting challenges from an operations and security perspective.
   - Tool implementation across DoD – DoD tends to look at a one-size fits all (e.g., HBSS), and that does not necessarily work within USSOCOM
8. **Initiative – Joint Cyber Center.** The U.S. Secretary of Defense is moving forward with the integration of Cyber Support Elements at USCYBERCOM. USCYBERCOM obtains forces from MARFORCYBER (predominantly). USSOCOM is committed to working with Theater Components with integration of Cyber Support Elements when USSOCOM has personnel in theater.

*Col Marc Jamison, USAF (Ret), Director, Strategic Ventures, L-3 (Former Joint Functional Component Commander – Network Warfare (J3) and U.S. Cyber Command J35.*

Col Marc Jamison, USAF (Ret) shared some perspectives on operating in cloud and cellular networks based on his past military and recent corporate experience. Highlights on his panel remarks included:

1. **Operating in Cloud and Cellular Network Challenges.**
   - Mobile – operating at the edge – is where the challenge will be.
   - Weapon systems are 'old school technology' with apertures wide open. How do we protect systems that accomplish the mission?
   - Bringing your own device (e.g., cellular phone, IPad, etc.) and connecting to a government network brings efficiencies and effectiveness, but we need a solid game plan to defend.
2. **Understanding the Environment.** The U.S. has limited insights as to what is really going on in the Cyber Battlespace, and no way to display (clearly) how cyber forces are/were affecting the bigger battle. What is needed is a Cyber FEBA and Plot.
3. **Supporting (Better) the Warfighter.** We lose the Cyber discussion up front with combat arms officers and operators when we don't address their issues, or discuss how to help them (e.g., JFACC) accomplish their objectives and priorities. They have no time to do Cyber Warfare for Cyber's sake. Developing a Cyber Order of Battle and Counter-Cyber operation plans for current and potential adversaries can facilitate discussions with combat arms officers on how Cyber can support their mission and objectives.
4. **Trained Cyber Warriors.** We need to get the offense and defense guys together first, and then quickly get the joint community working together at the same location.
5. **Cyber is Whole of Nation, Not Joint.** JIATF-Cyber had 27 different organizations and agencies, each of which needed to understand what is going on. State / CIA equities need to be included and understood. We need to go beyond Joint and Inter-Agency to industry, who owns 90% of networks. We also need to work with industry to understand trends and challenges, and to develop an enduring strategy on how to model and think through the infrastructure so we can defend the network.

*Panel I Questions / Open Forum Discussion*

CAPT Goodwin opened up the panel for questions and comments from participants, highlights of which included:

1. **What do we lack in educating the workforce?**
   - Programs of Record, which are slow to evolve and need to be included in acquisition process.
   - Training the acquisition workforce.
   - Joint Cyber Course and Catalogue – there is a lot of data to start developing a Cyber curriculum.
   - With Cloud Computing Environments, need to get information to school house with deployment of these capabilities (programs of record).
   - Training agile enough to introduce new skill sets we ask our troops and analysts in the field.
2. **In kinetic warfare, there are after action reports and standards. Are there standards for Cyber, and if not, will they be available, and if not why?**

- Joint Effects Board is looking into Cyber effects, especially in Joint Exercises.
- Broadly stated standards, no. Highly specified and focused, increasingly so.
- On the defensive cyber operations side, there are many metrics and measurements, but what does it mean and what are we going to do with all the data? Are we winning and are achieving success is what we should focus on.
- What operations are not being conducted because of cyber-related issues, denial of service, or other situations is what we should be concerned with.
- What are needed are measures of performance and effectiveness, to highlight the value of our cyberspace operations and activities,
- What is also needed are cyber operational assessments. Are we doing things right and are we doing the right things?

3. **How are we doing in identifying and defending/countering zero day exploits?**
   - We are doing better, but we are still not that great in blocking and tackling known vulnerabilities.
   - With HBSS, part of our defense in depth strategy, we are buying time at the boundary level. At the local level, need to improve defense and mitigation.
   - Until recently, the U.S. has not forced the adversary to use zero day exploits.
4. **Is consolidating and collapsing our networks a good idea, and if we put all our eggs in one basket, do we gain or increase risk?**
   - With JIE, let us keep a few baskets open, but let us defend one basket well. We don't defend any of them very well today – we do not have many Cyber Jedis.
   - Cloud architectures offer ways to defend the basket well, as data and sensors aren't on network.
   - USCYBERCOM does a better job at protecting boundaries, and if we shrink the attack surface, we will get better, and succeed.
   - We need to consolidate and collapse, as limited manpower postures and budgets preclude us from protecting each device and network. We need to move from thin clients to zero clients.
   - Collapsing networks will drive the U.S. to look at defense in a different way, and how we structure the devices to perform functions. This will not be business as usual, and we will need to look at layered and risk based concept.
5. **Who are the IT Governance Proponents?**
   - USCYBERCOM and DoD CIO.
   - The move to thin clients and tactical systems is part of the CIO strategy.
   - While the DoD CIO puts out policy, the Services supplement these policies so now you have a Service unique policy.
   - As a Joint provider, Service components state they have to follow their Service policy over the Joint policy – creating potential conflicts and increased policy confusion.
   - Central to JIE is that while the DoD CIO has plenty of authority, it is not exercised at this time.
   - There are also an estimated 540 governance boards directly/indirectly related to JIE/IT.
6. **What is the Governance for Tool Development?**
   - The Services drive innovation at the mission applications level and develop baseline.
   - Does DISA provide tools if there are Service tools already, e.g., Army Records Management?
   - Governance for tool development in three months, not five years, is needed.
   - In a field study of federal agencies, DoD came in dead last in Enterprise IT Architecture planning.

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

Dr. John Arquilla shared his perspectives on why he believes Cyber War is here today, as well as the different faces of Cyber War. Highlights of his presentation include:

1. **Cyber War is here today, and will shape military and security affairs tomorrow.** Cyber War has been coming for the past 20 years, and despite claims otherwise by the former Cyber Czar, it is here today. Cyber War is about fighting the war in cyberspace, it is about information in conflict. The U.S. lives in an age where there are two dozen wars that are all irregular, not mass-on-mass. Our adversary is hiding in the vast virtual world, and it will be crippling if we lose this war. It may be difficult to completely defeat the insurgent/adversary in cyberspace, but the U.S. can make it inhospitable for them to operate in this "military domain." We need to create the information edge that won World War II, to gather knowledge to act intelligently in war. The greater the knowledge and information edge, the less mass the U.S. needs to win the Cyber War. **Cyber War has four faces.**
2. **First Face of Cyber War: Some say Cyber War is not real war because it does not look like a "Patton War."** Stuxnet took out Iran's nuclear site centrifuges – what if 1000 centrifuges were taken out? Cyber War, or Cybotage, can have similar effects comparable to direct actions, special operations, and irregular warfare. Flame/Stuxnet was a watershed moment, as it converged the physical and virtual (cyber) worlds.
3. **Second Face of Cyber War: The whole business of espionage in the virtual world.** Virtual Human Intelligence. Protracted Intrusion. Cyber Espionage. Moonlight Maze / Titan Rain were two of the first high profile cyber events that focused on exploiting R&D on Fortune 100 companies. The adversary continues to expend every effort to get our R&D to improve their own weapons, and we are hemorrhaging intellectual property.
4. **Third Face of Cyber War: You can wage this kind of warfare without engaging armies in the field and navies at sea.** Will cyber warfare be a form of strategic attack? It can be destructive, imposing costs but not necessarily casualties. Is this likely to have an effect? Imagine wars of pernicious viruses let loose every few weeks, and then imagine we don't know who is doing this. This could have a strategic effect, a cheap way (cost imposing strategy) to do physical damage on our critical infrastructure in addition to having a psychological effect.
5. **Fourth Face of Cyber War: Cyber use in battle – information resources empower, but also imperil due to our dependencies.** We are developing and operating information systems with a man in the loop. What if our ten major automated systems were disrupted, e.g., Air Tasking Order?
6. **Strategic versus Tactical Cyber Attack:** Cyber Attack may or may not achieve strategic aims in the war, but employing tactical cyber war effects similar to close air support could achieve combat objectives.
7. **Cyber War is here.** In every era of technological change, there has been an associated development in military organizational change, doctrine, and strategy. Why do we not believe this is not the same with Cyber? This is not an exception. **This technology revolution (Cyber) needs to have an agenda of**

**broader introspection and reflection** in our own practices. A correct idea is worth running with and has value over time. Ignoring ideas, no matter how long it takes, cannot be wished away and is not a way such ideas are defeated.

*Questions and Answers*

1. **Will Cyber War be less likely given the onset of interconnectedness of nations from an economic and commerce perspective on the internet?** One of the greatest illusions (historical perspective) is that with the latest technological advance, making war would be too costly – do not concur this will be the case.
2. **Does the U.S. need a Cyber 911 to serve as a catalyst?** Similar to the "Harbor Lights" in 1941 in which German U-Boats had a happy time sinking our ships in harbors due to the illumination of cities, today, the lights are on in Cyberspace. Until we can turn of these lights, which we did in WWII that substantively reduced the number of vessels sunk in port, the adversary will have a happy time in cyberspace in stealing our intellectual capital and compromising our systems. We have to start now in turning off the lights, to include the more ubiquitous use of encryption instead of cowering behind firewalls.
3. **How can anyone say there is no Cyber War.** Estonia. Korea. Saudi Arabia. Iran. They all encountered cyber attacks. While we have the luxury of debate, people and nations around the world are falling under attack, and their systems are under attack. Cyber raiders continue to prey on those with wealth (such as the U.S.), and it is a hay-day for cyber piracy, all of which highlights the serious vulnerabilities of societies to cyber attack. **The U.S. is a great power, but also the greatest target in the world.**
4. **If a NATO country encountered a Cyber Attack, could the U.S. respond in kind?** Allies under sustained cyber attack can call upon allies to come to their defense. **The Pentagon recently stated the U.S. does not have to respond to a Cyber attack by Cyber means – this is a deep and powerful statement that could have a deterrence effect.** The Pentagon is thinking ahead and this is healthy – the interesting point is that how can this (or any future) Administration say that Cyber War is not real when Allies could potentially call the U.S. to respond to their cyber attack?
5. **Is openness on vulnerabilities and attacks a positive thing?** Many organizations are not reporting attacks, and not sharing vulnerabilities that could illuminate weaknesses. We need to be careful with announcing vulnerabilities, as there are situations where full openness can create chaos and be exploited by the adversary. **Guarded Openness** may be what we seek to achieve, recognizing we have to share, but guardedness guides how to apply to military affairs.

*COLJoel Bagnal, USA (Ret), Vice President for Cybersecurity and Innovations, L-3 and*
*Former Deputy Assistant to the President and Deputy Homeland Security Advisor*

COL Joel Bagnal, USA (Ret) provided an overview of government's role in Cyber, and some perspectives on industry's role in developing innovative solutions to some of our national cyber challenges. Highlights of his presentation include:

1. **2006 – Cyber 911.** In 2006, President Bush received briefings highlighting domestic intelligence activities and significant incursions into our networks, to include the Joint Strike Fighter. The adversary entered U.S. classified and unclassified systems and defense industrial base undetected, and

extracted specific data (also undetected) which intimated substantive reconnaissance having taken place prior to extraction. The adversary also left behind autonomic devices (undetected) during the extraction process for future exploitation. This series of events led the current administration to meet with senior leadership from the Department of Defense and Government, and following a five hour discussion, they undertook a policy effort to develop the Comprehensive National Cybersecurity Initiative (CNCI).

2. **CNCI.** CNCI was largely a military led effort, but in peeling back the onion, it was evident that there was going to be some challenges in determining who was responsible for cybersecurity when there were seventeen (17) agencies and departments within the federal government having responsibilities for cybersecurity at the time. Additionally, what was not realized and accommodated at the time was the fact that an estimated 85% of the IT supporting Federal, State, and local government is provided by the commercial sector. CNCI is a $42B initiative, with $21B already expended supporting 12 critical actions, and 7 enablers to shore up cybersecurity in our nation starting with the .mil domain, continuing with the .gov domain, and then providing incentives to the private sector in shoring up the .com/.net domain. This was done in part by clamping down the network, and in particular the access points to the network, and then deploying network sensors under this topology. However, this was not enough, as there was a huge proliferation of mobile devices that created millions of new end points, as well more sophisticated exploitation and attacks from autonomous botnets and malware. In 2007, there were 35K malware variants developed per day, in 2012 this increased to 120K per day.

3. **Understanding and Countering the Strategic (Cyber) Threat.** A CNCI imperative is to understand the Strategic Threat. There is much discussion and agreement about the advanced persistent threat, but there is also the transfer of intellectual property and theft of national secrets to consider. There also the faces of Cyber War that Dr. Arquilla addressed that need to be considered. **From strategic perspective, we are already owned in Cyberspace.** The adversary operates in our networks every day. Key activities we need to undertake include:
    - We need to develop resilient systems to ensure that no matter what the adversary does (exploit or attack), we continue to perform mission essential functions of the U.S. Government without degradation. Regardless of where the adversary impact is coming from, we need to have the systems to allow that resilience to transpire.
    - We need deterrence, and the best defense is a great offense (a position the DoD unveiled with the Cyber Strategy). We need to shift from cyber protection to cyber offense and deterrence.
    - The private sector, as it did during the industrial, mobility, computing and information revolutions, needs to assist the government apparatus in building cyber solutions for our military to remain a superior force. **There needs to be a Cyber Manhattan Project, a public-private partnership**, that develops deterrence policy that matter, focuses on public debate on cybersecurity enhancement.

4. **The U.S. is (currently) losing the Cyber War.** It is time and grace and other elements that have kept us from bleeding as bad as we could.
    - In 2013, the FBI could have more agents focused on cyber-terrorism and cyber-crime than terrorist investigations.
    - The greatest threat to national security is the transfer of intellectual property, which has been never greater than today (we are bleeding intellectual property and capacity)

5. **L-3 Cyber Strategy is to invest (modestly) in 12 technologies (cylinders of excellence**). L-3 is also developing an Internet Isolation Capability (setting up virtual sessions on the Internet, secured via encryption and VPN tunnel). It was recommended that the DoD and Intelligence Community transfer their state-of-the-art cyber capabilities to the private sector. Corporations also have a responsibility to help the government, through public-private partnerships, to create a national set of solutions to national security issues.

*Questions and Answers*

1. **Was the Current Administration's admission that the U.S. produced Flame/Stuxnet a positive and sign of the future?** How this was exposed through leaks was horrible, but this may serve as a deterrent to future activity. This also helps all appreciate that everyone is getting hit and we should not keep secret the $Billions we are losing each year to cyber exploitation and infiltration.
2. **Does the U.S. have a Cyber Deterrence Force?** This does not exist yet until we adjust our behavior, and the threat is ahead of us.
3. **U.S. corporations need to shift their mindsets from keeping vulnerabilities and intrusions close hold**. Google cited as potential model as it dealt with China. U.S. behavior likely not to change until a major catastrophe occurs.
4. **Is someone in the government going to state the obvious and define cyber warfare?** There is no definition of cyber warfare, but the national debate on cybersecurity is healthy. Counter-terrorism and economic crisis are of current greater importance than cyber so legislation pieces of the Hill are being pushed down the priority list. The U.S. also does not want to give up its civil liberties, which in turn creates increased vulnerabilities in cyberspace. There needs to be a robust federal debate to get real resources applied.
5. **When do you think Cyber Policy will enable us to go from defense to offense?** Within the DoD Cyber Strategy, there is already a move afoot to shift focus and resources from defense to offense. We do need overarching policy and doctrine. Within the private sector, there are 18 sectors of the economy that with thousands of companies having little to no cyber prowess and capabilities. The private sector (today) is not allowed to conduct cyber offensive activities, and could benefit from government and military technologies through the appropriate technology transfer agreements.

*Mr. Gib Sorebo, Assistant Vice President, Chief CybersecurityTechnologist/Cyber Law Specialist, SAIC*

Mr. Gib Sorebo served as the moderator for the second of four panels, and provided an overview of Cyber Law and Ethics, and their distinctions. Highlights of his panel remarks included

1. **Cyber Law and Ethics.** Cyber Law is the proper authority to act as we have seen and can. Cyber ethics are checks on abuses that the law cannot really cover (what we do when no one is looking). Since we cannot cover every incident, ethics reminds us that we do have a higher obligation than following the letter of the law.
2. **There are jurisdictional challenges with law in Cloud and Cellular Networks**. In the cloud, data (an asset) transfers from one jurisdiction to another in a matter of milliseconds. There are also a different set of laws within the public and private sector on gathering data for evidence to capture individuals during conflicts.
3. **Other countries do not like our "Cyber" criminal justice and investigation process** that manages hackers.
4. **There is a desire to protect data and infrastructure and a need for offensive and hacking back** to deter future actions or neutralize opponents from doing future attacks, but no cogent policy or framework that would allow.
5. **Laying out a cyber legal framework is challenging**. There are many cybersecurity laws that have been written for many reasons, such as FISMA, DIACAP, etc. However, intellectual property is not regulated whatsoever. **U.S. laws are mostly data and sector specific rather than all-encompassing like other countries with their laws**. The Federal Government is implementing systems based on varying requirements which drives up costs and oftentimes no real benefit. Law enforcement is dealing with wiretap and consumer privacy acts. Military and Law Enforcement are dealing with Title 10, 50, and 18 challenges, which impacts prosecution decisions – following the wrong Title is potential cause for evident not being admissible in court.

*Dr. Dorothy Denning, Distinguished Professor, Department of Defense Analysis,*
*Naval Postgraduate School*

Dr. Dorothy Denning shared her perspectives on why Cyber is not only here, but good, and highlights of the principles of unnecessary risk and harm. Highlights of her panel remarks included:

1. **Cyber War is here. It is not only here, but good.** A qualifier is warfare in not always good, and so cyber warfare is not always good, especially if you are the victim.
2. **Cyber War – More Moral than Kinetic.** If we look at cyber operations, in particular cyber attack, it can offer a more moral way of accomplishing a goal than kinetic attack.
   - Cyber attack is not always moral or always good, but in those cases when the U.S. has a just cause and goal to begin with, and while abiding by the principles of the law of warfare, if you

can conduct the war by a cyber means it could be more ethical than by kinetic means. The reason why it that cyber attack is more humane, kinder, and gentler that a kinetic attack (with the cyber attacks we have seen so far, nobody gets killed).

- As for physical damage, there may not be any, and it is generally about restoring bits vice rebuilding property.
- Cyber attack is more humane, causing less harm and may also pose less risk to those carrying out the mission.

3. **Principles of Unnecessary Risk and Harm**. Bradley Strawser identified two basic principles that directly apply to Cyber War – the principles of unnecessary risk and harm. Commanders give subordinates an order to accomplish a goal that is just, and have an obligation to ensure activities to achieve that goal to not incur unnecessary harm and risk. In the International Law of Conflict, there is proportionality and necessity. Managing cyber attacks remotely poses less risk to those carrying it out.
   - These principles could be applied to Stuxnet.
     - o Assumption: It is just to disrupt Iran's nuclear program.
     - o Justification: It is a good objective to disrupt the program by destroying centrifuges with kinetic attack. We envision cases for achieving the end state for using cyber attack, i.e., Stuxnet or SOF forces with explosives conducting a physical attack.
     - o Impacts: Stuxnet was employed and achieved the end state by not getting folks (SOF forces) killed, although there was some collateral damage. This last point is not trivial, as Stuxnet did get out to 100K targets in other countries to include the U.S. and utilities. Explosives would not have gone beyond the facility. There is a long term effect (impact) of the code being out there, as people with more nefarious goals may build upon the code.
   - The principles would not apply to situations where cyber war caused electric generators to blow up, power grids to go off across the country, planes to crash, and other situations that caused huge hard to people and environment.
   - The principles would apply to intelligence collection on networks, as it does not risk our agents or pressure double agents for better data since data is there for the taking.
   - There would need to be a case-by-case analysis, as it would be tough to apply this as a general principle.

*LCDR (Sel) Elliot Oxman, USNR, Senior Legal Counsel, Office of the General Counsel,*
*U.S Department of Energy*

LCDR (Sel) Elliot Oxman shared his perspectives on what being a Cyber Security Attorney at the U.S. Department of Energy means and what types of projects fall under that category. Highlights of his panel remarks included:

1. **DOE budget priority is National Security (Nuclear)**.
2. **DOE CIO is at the cutting edge of Cloud Computing**. DOE was the first federal agency to sign up a commercial vendor for cloud computing services at a national laboratory.

3. **DOE encountered several issues bringing onboard Cloud Computing.** The first hurdle was with the State Department. At national laboratories, ITAR security needs to get okay to do our own work in our laboratories. Since DOE needs that compliance, this meant that data location and servers had to be in the U.S., and compliant with FISMA. The second hurdle is CFIUS, CFIUS is an inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person ("covered transactions"), in order to determine the effect of such transactions on the national security of the United States. With Cloud Security, countries no longer need to acquire a critical U.S. asset to learn the vulnerabilities of that asset for future use. Through due diligence a foreign person can look at the Cyber Security Defense Plan for a company they are thinking about acquiring. Once they review that plan, they no longer need to acquire the company (avoiding CFIUS), because they have identified the company's vulnerabilities. CFIUS mitigation includes educating government acquisition/contracts personnel to pay attention to the Cloud Computer Service Provider after the contract is signed, as they may be U.S. today and a foreign entity in the future.

4. **DOE CIO bringing DoD capabilities and security measures to its national laboratories.** DOE national laboratories are critical to the national defense and intelligence community. As DOE national laboratories are contractor operated, there are some things the government can do to protect itself that it cannot do to protect the private sector and defense industrial base. FISMA required DOE to have protections in place, because these computers may have been contractor operated but were still government owned and FISMA compliant. This allowed DOE to bring in security measures to protect the intelligence community projects DOE worked, e.g., affirmative consent log-on measures.

5. **Protecting the Power Grid: Assistant Secretary for Electricity Delivery Energy Reliability at DOE**. Ensuring the resiliency of the power grid is a never ending affair, and the power grid is largely private sector owned. DOE cannot regulate a power company and direct them to do certain actions, although they can provide information on the threats and where they 'have been hit.' These companies could say, 'yes, we need your help do not know if we can justify spending the dollars," or refuse to accept they have been hit in the first place. This latter point is critical, as DOE does not own these companies that represent a huge part of the U.S. critical infrastructure, but needs them to succeed in ensuring the resiliency of the power grid. DOE also initiated a public-private sector outreach program that is a first of a kind that includes the White House, Justice Department, and Department of Homeland Security due to the many equities in play, and with the ultimate goal of protecting the power grid.

6. **DOE Intelligence (IN) Component.** The White House is standing up and strengthening the "Insider Threat Program," that involves the Intelligence Community and DoD. One issue DoD has is how to look out and do research without telling the adversary what they are looking at. Because DOE deals with advanced technology just looking tells the enemy a lot. How can DOE misattribute its Internet searches and surveys, and what does that legally mean? Is this covert / clandestine collection, neither? These are not settled issues, and DOE cannot jump out and do things if they have a legal position.

7. **DOE Protection to Private Sector – 4th Amendment Issue.** If DOE provides protection to the private sector, they need to do so without turning them into government agents. DOE does not want to lose their ability to go after bad actors because they unknowingly were monitored by the government. DOE has designed programs to protect the privacy of the U.S. citizens and companies comprising the critical

infrastructure – many of these programs scrapped since they were too close to government monitoring. Balancing people's expectation of privacy with protecting critical assets/infrastructure not an easy task. DOE needs to limit information it gets from the private sector. DOE needs to continue providing notice that users of DOE systems in the private sector have no expectation of privacy. Finally, DOE requires consent log on browsers (banners) are included on government systems. Having this notice/consent requirement, DOE legal staff contends this protects against litigation from the private sector when they state privacy was taken away. We live in a world where the private sector can bring on litigation – the above measures protect both DOE and private sector.

8. **Laws have not come close to catching up with technology.** The more federal surveillance and wiretap technology, and acts that are in place within the government, the less likely the private sector will work with DOE.

*Mr. Jack Beard, Assistant Professor of Law (Space, Cyber, and Telecommunications Law Program), University of Nebraska College of Law*

Mr. Jack Beard shared a contrarian position (than those of earlier speakers) that Cyber War is not here, and that it is not here legally. Highlights of his panel remarks included:

1. **Cyber War is not here, and it is not here legally.**
   - Estonia was a victim, but they did not go to the UN Security Council.
   - Iran was the victim of Stuxnet, but they also did not go to the UN Security Council to complain.
   - We are entering a world of cyber espionage and cyber sabotage, and we need to look carefully at the legal framework of Cyber War.
   - Lawyers do not answer questions the way warfighters want them to answer.
2. **Cyber War in the Fifth Domain.** Cyber War is an overused phrase of every unpleasant action on the Internet. War has no "legal meaning" anymore outside the few U.S. statutes that evoke it – there is the war on poverty, war on drugs, war on illiteracy. The "war model" does not apply to most military activities in cyberspace, and is really dangerous as a precedent if evoked.
   - We need to ask two legal questions:
     - Do these cyber activities justify using U.S. using force against the country using them against the U.S.?
     - Once the U.S. is in an armed conflict, which of these acts become the trigger the "law of armed conflict" that has war criminals and unlawful combatants?
   - The phrase "Law of Armed Conflict" continues to be replaced with 'fuzzy terms' such as International Humanitarian Law and Human Rights Law.
   - If a military strategy/objective is Cyber War, military planners responsible for a Cyber Attack may now be responsible for determining if it is okay to kill civilians. With kinetic attack, military planners usually have the answer with persistent surveillance. With cyber attack, this could be a large unknown.

3. **Cyber War – The Legal Construct.** There are two legal constructs that need to be considered:
   - Do hostile cyber attacks alone justify the use of armed force by states under the *"jus ad bellum, or laws of war?"*
   - Does the Law of Armed Conflict apply to hostile acts in cyberspace under the *"jus in bello, or laws in war)?* Are these acts "armed attacks" and "acts of violence?"

4. **Prevailing Consequentialist Approach**. Prevailing/presumed consequentialist approaches include:
   - If cyber attacks cause the same effects as conventional attacks (injuries, death, damage or destruction), then an armed response by the victim state is appropriate *(jus ad bellum).*
   - Once an armed conflict is present, International Humanitarian Laws applies to cyber attacks if they cause injuries, death, damage or destruction as armed attacks/acts of violence *(jus in bello).*

5. **Cyberspace is only "Space" in a Metaphorical Sense**. With the exception of physical nodes and networks, we aren't in a world or terrain we control or possess or occupy. We are in a world of information. Treating information like conventional weapons will lead us down difficult roads, with many perils if correlated with conventional or nuclear weapons.

6. **Information as a Weapons and Target – Problems in Analogous Reasoning.** The origins of weapons are different than "whose weapon it is." The widespread availability of information means that almost all combatants have the same information. There are so many computers/information systems that are available, and so many players and actors involved in cyber actions. When someone accesses information, they could go into an adversary system but not infringe on a territory (much different than crossing a nation's airspace or territorial waters). Many cyber actions are acts of persuasion, hard to equate to some acts of physical violence and kinetic action that we are used to. Complete control of information is difficult, and exploiting information raises questions on the content of information - are we exploiting bank information or C2 systems? Espionage is not governed by the Law of Armed Conflict, and thus is the case with Cyber Espionage. There are also different layers of cyberspace – attacking one does not necessarily translate into attacking all layers.

7. **Origins and Availability of Information.** What is the Cyber Battlefield, and what are unprivileged belligerents? Are we really going to consider evil doers operating from Starbucks as "belligerents?" The invisibility of actions in cyberspace and anonymity, and ability to remotely control privately owned systems, makes it difficult to identify the origin of information and to attribute a cyber activity to a particular state. It is not going to be enough to identify a computer and attribute that action to a particular state, and what creates more legal issues is the fact that most of this capability is in the hands of the private sector. There are also low barriers to entry – we tend to ignore and/or forget how much technology and information is available to the adversary.

8. **Cyber Acts and the Jus ad Bellum.** Cyber has real trouble fitting into "Armed Force, Armed Attack, and Act of Aggression" when the U.S. is attacked. There are a lot of bad things that hurt countries and the U.S., but that is does necessarily mean this is an act of aggression. Even if the U.S. could identify the source of the cyber attack, could these attacks be attributed to state agents? Are these states responsible for cyber attacks from their territory? Can State responsibility be imputed? There are cases where the State had made deals with private actors (not going to attribute) provided there is some level

of control, e.g., irregular warfare. Bots and malware know no boundaries, and many attacks are launched from friendly countries.

9. **Access and Control of Information.** There is really no breaking and entering a system to gain access to information, other than using a thumb drive or other physical medium. To prepare the battlefield, to determine vulnerabilities, and to conduct precautionary information, the U.S. may need to penetrate adversary systems. Is that action going to serve as a trigger for cyber war – likely not. Cyberspace is not a natural construct, and is subject to replication. What does it mean to disrupt information or deny it? Regardless, this cannot be associated with the law of armed conflict, and falls back into the domestic laws of all countries related to espionage, fraud, crime, etc. Would the British Intelligence action to replace bomb making information on an Al Qaeda website and replace with a Cupcake recipe serve as a trigger for cyber war? Doubt it. Controlling and confining information is also difficult, and the confining acts themselves may be problematic.

10. **The Jus in Bello in Cyberspace.** If an armed conflict is present, attacks are defined as acts of violence against the adversary? Is consequence alone the key, or is a violent act required? There is no question that exploitation of data is severe, and that damaging consequences are possible, or that cyber theft, larceny and fraud are criminal offenses under domestic law. However, espionage is not an armed attack or act of violence, and exploitation and theft focuses attention on what constitutes “content.

11. **Stuxnet.** Stuxnet was recently identified by the U.S. Administration as having its origins in the U.S. Despite the damage it did to Iran nuclear power plant centrifuges, the cyber espionage (Flame) and sabotage (Stuxnet) acts did not necessarily constitute a hostile cyber action in the context of Cyber Warfare. Iran did not complain to the U.N. Security Council, and if it did, would this provide the precedent for similar actions to the U.S. using the U.S. cyber precedent? Was Flame/Stuxnet an instantiation (as would be the case of similar actions across the world) of pressing a button and causing harm, or the nature of cyberspace and the users of information?

12. **Layers of Cyberspace.** There are two layers of cyberspace:
    - The top level, which consists of the information environment and cyberspace
    - The bottom level, which consists of the physical, syntactic (informational), and semantic (cognitive) layers or dimensions. Increased emphasis is being placed on the cognitive element.

13. **Cyberspace is “In and By Computers.”** Information going to systems, information going to humans.

14. **Military Information Operations.** Military information operations includes:
    - Influence operations, electronic warfare operations, and network warfare operations
    - Counterpropaganda operations, psychological operations, military deception, counter-intelligence operations, and public affairs operations
    - The focus is on target audience and shaping the perceptions of target decision makers.

15. Conflicts in Cyberspace. Are they appealing images, or complex realities? Lawyers apply one set of laws, while countries find it difficult to apply these laws to new cyber threats. The LOAC cannot (legally) be applied in the face of uncertainty.

Mr. Gib Sorebo opened up the panel for questions and comments from participants, highlights of which included:

1. **Do covert and clandestine authorities help or hurt us?**
   - Up to the 1970', covert activity was not defined and was permissible. Today, it is permissible but requires Presidential certifications (checklists and certifications).
   - The U.S. has not made a concrete statement that it conducts covert and clandestine cyber activity, although statements have been made on overt activity.
   - Covert activity can violate domestic laws. If someone operating a drone in Afghanistan and Pakistan from the U.S., this person could be subject to their domestic laws.
   - U.S. has little regard for other country's domestic laws. Other countries are trying to block U.S. discovery laws. Our attitudes that we do not necessarily care if we violate European laws may bite us in the future.
2. **From an ethics perspective, if we recruit cyber agents (assets), there is a risk we place that asset. Are we not bound to them?**
   - Some individuals are taking responsibility for certain actions. There are always risks that we will expose activities and the people doing these activities.
   - In conducting legal reviews, military planners need to know that doing certain cyber actions with cyber agents may make them targets (probably not what they are thinking about though).
   - If operatives placed at risk by "big government leaks," leakers should go to jail, and not the operatives who may have been caught in the fray.
   - Time for some self-reflection within the U.S. U.S. admissions (leaks) of Stuxnet details likely resulted in some Iranians being killed. From an ethical viewpoint, this could inhibit others from working with the U.S. in the future.
3. **Do we need to define Conflict in Cyberspace?**
   - This might not be in our best interests to define. What are the incentives? Who would follow these rules? Transnationals/adversaries would not, but we would be accountable.
   - There are many cases for not defining. If you define X, you are bound by X.
   - As the adversary gets better and better with low-cost technologies and information available, attribution is going to be problematic for the U.S.
   - As long as we are at the cutting edge of technology, best not to define. What is needed is clarity on operations authorities and parameters.
4. **Regarding the doctrine of public and private necessity, is this a civil libertarians' battlefield?**
   - There will always a balance between defending our nation versus civil liberties.
   - The FBI has received permission from the courts in countering cyber theft, but did not from all users.
5. **Have authorities been aligned for cyber counter attack?**
   - There are some that make an argument that we are impotent to responding to an attack because we get bogged down in definitions (when our adversaries do not).
   - The U.S. may be reluctant for bringing out its best, e.g., as discussed in Libya. Once used, you got it out there for all to exploit.

- Senior U.S. military leadership has stated that he could not envision using cyber attack on a bank account  unless the bank was bad (e.g., military object).  Was this a policy statement?  If the bank is a legitimate military objective, why not, and the law should not stop.

6. **Do we need Cyber Rules of Engagement?**
    - We have a lot of cyber tools, with the choice on their usage influenced more by policy versus legal considerations, but at some point the lawyers will say that "going to this stage" will entail these legal consequences. Need to consider.
    - The vast majority of what we do is defensive, and there will be a host of issues that we will continue to address from a legal perspective (e.g., EINSTEIN II monitoring across agencies).
    - There is an effort within Congress to make cyber attack subject to the "War Powers Resolution," which will help define cyber rules of engagement (and make more relevant).

*Mr. Brian White, Managing Director and Chief Strategy Officer, Chertoff Group, LLC*

Mr. Brian White shared his perspectives on where we are from a Cyber Offensive capability, and why we need some more policies for Cyber Offense. Highlights of his presentation include:

1. **Stuxnet – U.S. Cyber Offensive Action against Iran.** Stuxnet targeted industrial software, and instilled fear in Command and Control (C2) operators around the world who are relying on the same platform to operate their capability from refining to power generation. If the allegation is true that U.S. and Israel is behind Stuxnet, does this foreshadow new concepts of war?
2. **Flame – Largest malware employed by the U.S**. Flame sits there and monitors computer behaviors transparently. It was jointly developed, and employed together, so more targeted intelligence could be gathered.
3. **Potential Cyber Conflict between U.S. and Iran?** The DoD affirmed its intentions to respond to a cyber attack with conventional forces. If Iran responds with its own cyber attack on U.S. and Israel based on Stuxnet and Flame, does that justify the U.S. responding with conventional forces?
4. **Cyber Mutually Assured Destruction.** During the nuclear arms' race in the 1950's and 60's, the U.S. put into a policy that was not a given then, mutually assured destruction. This has served the U.S. well for over 60 years. Are we going to put a similar policy for the Cyber domain, supporting the former Secretary of the Department of Homeland Security, Michael Chertoff, comments that the Cyber threat is the most complex, most novel, and most serious threat to National Security since the onset of the nuclear age.
5. **Global Cyber Arms Race.** The Pentagon is dramatically speeding up the development and fielding of cyber weapons and systems in order to give warfighters capabilities to go against specific cyber threats in a matter of days. The Office of the Deputy Assistant Secretary of Defense for Cyber Policy is also working overseas on establishing treaty regulations for Cyber. There is a strong potential for a Global Cyber Arms Race. There is a commercial aspect to this race, as the private sector is developing the cyber capabilities and delivering to those being most targeted. Most of the destructive activity is happening outside the government, to those key sectors, key companies that produce most of what the U.S. needs. The potential crippling of the power grid from a cyber attack would have a catastrophic national impact comparable to a physical attack.
6. **Companies are encountering sustained, persistent threats and are taking matters into their own hands.** In the nuclear age, we had clear strategy and standards. The current "continuing" debate in Washington DC on information sharing and standards is good, but the real issue that needs to be debated is strategy and doctrine in the Cyber Age. The U.S. needs a strategy that stresses dialogue and answers key questions. It is not just a military .mil problem, and we need to address how a private organization can equip and take action against those who seek to do them harm in cyberspace.
7. **Our society does not expect an institution to be responsible for major security threats.** On one side of the argument is that the government should own a monopoly on cyber defense and be totally responsible for public and private networks, operating network defense, and lessening the insider threat. On the other side of the argument is that government should disclaim any responsibility in this

market, leaving the market and individuals to address these issues. Both are unrealistic, and there needs to be a shared approach.

8. **Key questions for the government to consider.** The U.S. (and government in particular) should begin a serious discourse and answer the following questions as a start.
   - What is an attack, and how often should it be used?
   - What is not an attack?
   - What is traditional espionage?
   - What is the line between exploitation of vulnerability and an attack?
   - What does the loaded word, Cyber War, mean? Where and when does it begin? Who determines when it begins?
   - Are we going to treat cyber attack the same as a kinetic attack? Is that practical?
   - Is Flame/Stuxnet the first certified cyber exploitation and attack this past four years? Does it foreshadow new methods requiring the Executive Branch and legal to come up with doctrine and rules of the road?
   - How do we justify the use of cyber capabilities in war – from the politics of the decision to the actual going into war? Will the government continue to avoid the private community in this debate as the government tries to do something in this domain?
   - Regarding the private sector...
     - What constitutes the right of self defense?
     - What are the limits of self defense?
     - How much does the government want the private sector to do self defense, and should this be encouraged?
     - Does the level of state defense intervention vary based on the criticality of the infrastructure, e.g., is the energy sector different than the pharmaceutical sector?

9. **He who seeks to defend all in Cyber, defends nothing.** The Department of Homeland Security, in 2002, had to address what infrastructure was truly important. In their HLS definition, DHS defined critical infrastructure as everything that is important, in essence stating the nothing is more important than the other.

10. **Intellectual Property.** Intellectual Property is predominantly private industry issue, and the state has a greater role when deploying capability to private institutions.

11. **Strategy Development – The Wild West. There is no [real] cyber strategy**, and as a result there could be serious undesired consequences as our nation continues to face the onslaught of cyber attacks. Government agencies really need to change their viewpoints of policy and legality. Four years ago the National Cyber Security Center stood up, but their authorities to deal with deal with terrorism in the cyber realm is antiquated, one reason why there needs to be strategy that is executable, comprehensive, and agile.

12. **Is it time for the government to consider outfitting a company with offensive capability?** In-Q-Tel is helping shape security by developing and fielding a software application to allow industry to take actions into their own hands. Not suggesting that this actually take place, as a private capability without a strategy and authority and rules of the road can be destructive.

13. **Laws and strategy need to accelerate to keep up where we are with technology.** NSA is shy about any public role, does this need to change? There are also a limited number of people in government who can develop the tools, technology, and tradecraft in Cyber. With a finite number of cyber

professionals, we are left with cyber coordinators instead of having people onboard to deal with the hard issues and challenges in cyber.

14. **Potential strategic solutions, new paradigms**. Our solution set should not be a strategy and courses of action on what we can do with existing rules and tools.
    - We need to create new rules and tools based on a doctrine that sets forth our strategic objectives about roles and responsibilities of the government and private sector institution.
    - This cannot be just about technology either.
    - The public and private sector intersect in so many complex ways that was unimaginable, but may result in the government having to be part of the solution in defending them.
    - As the workforce changes, so must the law.
    - We need to find ways to better deal with non-state actors with Internet access who are doing increased damage with little to no barriers to entry.
    - We should not privatize the network, but we should not militarize either.
    - Cybersecurity needs to be mandated versus voluntary standards, with increased information sharing.
    - We need to narrow our universe of what is truly important, and requires attention, to national protection.
15. **Moving Forward in the Cloud.** As we move forward, an actionable idea could be developing a Cloud where private industry could put information about signatures and attacks, what they have seen, then allow government to analyze for appropriate responses.
16. **Developing a Cyber Offensive Posture.** The U.S. needs to move more aggressively in developing its cyber offensive posture if we are going to have a viable deterrent. The U.S. needs to have a great show of force (Stuxnet was a beginning), and we have the greatest military in the world. We do not need to be shy, we need to develop cyber supremacy, and we need to create some fear. **The current standards and defense dialogue is not going to put the right laws and policies in place to enable us to move forward in Cyberspace (Defense and Offense).**

*Mr. Harry Wingo, Program Manager, Veterans Outreach, Google*

Mr. Harry Wingo provided an overview of Google "Cultures of Innovation in Cyber" and his role in bringing more Veterans onboard. Highlights of his presentation include:

1. **Google Community Outreach to Veterans**. Mr. Wingo's charter and passion is bringing more veterans onboard with Google, and contends that more is required based on the debt Google (and our nation) owes its Veterans. As the wars in Iraq and Afghanistan wind down, there will be a transition of over one million veterans over the next five years into the workforce. It is estimated that 29.1% of the younger folks (enlisted) leaving active duty are unemployed. The economy is tough, and those in the audience who are (or were once) officers need to show some leadership in helping these troops move to the employed.
2. **Google Overview.** Founded 13 years ago, Google has grown into a company with 31,000 officers and employees in more than 70 offices in over 40 countries. Its mission is to organize the world's information and make it universally accessible and useful. Google is not a conventional company, and does not intend to become one, instead emphasizing an atmosphere of creativity and change.

3. **Google's Culture of Innovation.** In the private sector and military, cultures of innovation are mutually beneficial, although each could use some translation as to the other's culture. Google specifically seeks to bring Veterans into the Silicon Valley, and prescribes to certain key principles.
   - Focus is always on users, with everything else falling into place.
   - Focus on the hearts and minds (bigger picture).
   - Cross-pollinizing is critical, provides different perspectives
   - Getting STEM programs to be more engaging is an important contributor to successful, capable employees (this is the way we do it is anathema)
   - Code (software) is mightier than the sword (especially in Cyber and Cloud Computing)
   - Google employees work in small (family size) units. People have responsibilities, all are expected to participate, and there is a more direct line to outcome and effects.
   - Try outs are hard in Cyber at Google. As new things come into place, Google provides room for creativity and does everything it can to release the Jedi.
   - Ideas come from everywhere, and 10% of an employee's time is free time where they are allowed to work on innovation projects.
   - Every week (Friday) Google senior leadership engages its employees over a 1 ½ hour period. Anyone can speak up and this is expected. Employees can have access to video conferences and get information normally reserved for the board room, instilling increased trust and respect.

4. **In Cyberspace, Google touches billions each day**. Google – 1 billion searches each day. Chrome – 250 million users. YouTube – 50 hours of footage uploaded every minute. Android – 850,000 activations each day. Mobility provides key challenges, and underscores what Cloud Computing is all about at Google. Google has its data centers, and the computer serves as the door to where you go at Google.

5. **Google Innovation.** Google innovation includes Google X, the skunk works at Google. Google Glass provides connectivity to the Cloud. Driverless cars, mapping the ocean floor and the Art Project are other innovation programs that ensure Google employees work on cool stuff that matters. In addition, Google's Cyber Wallet enables mobile payments in Afghanistan, Google provides information quickly to the troops, and Google X is supporting the NPS CORE Laboratory in their Lighthouse Project.

6. **Veterans in Google**. In 2008, Google created an Employee Research Group to investigate bringing on Veterans. SOF Veterans and Google got together, and there was substantive discussion and information exchange of how military skills transition to the civilian world (may take some rethinking in Cyber). Other topics included how the military could organize and better engage the private sector.

7. **Recruiting the Cyber Force.** The DoD and military need to rethink metrics for recruiting cyber professionals regarding entry requirements, and find better ways to integrate those national guard and reservists with cyber skills and proficiencies into their operations.

8. **Google Code Jam – Creating a DoD Equivalent?** Google's Code Jam is a competition that is open to the world's top computer scientists, which each participant initially given four hours to write code. The 100 top coders participate in final sessions that approach the passion of the Olympics or March Madness. <u>Recommendation</u>: Do a similar Code Jam in the DoD at pre-commissioning and other times during one's career. The DoD Code Jam could become the Services' Commanders Cup for football, in this case applied to Cyber. Ranges could provide constant scrimmages supporting recruiting events, bringing Cyber talent to the attention of recruiters.

# Panel III – Educating the Work Force: Balancing the Current Force with Generation Y

*Dr. Hy Rothstein, Director, DoD IO Center for Research and Senior Lecturer, Department of Defense Analysis, Naval Postgraduate School*

Dr. Hy Rothstein served as the moderator for the third of four panels, and provided some insights into the challenges associated with developing educational programs and curriculum that supports strategy and the operational art. Highlights of his panel moderator remarks included:

1. **2002 Defense Planning Guide and Information Operations.** The 2002 DPG looked at Information Operations writ large, and emphasized the need to increase awareness and educate folks on the increased role and value of Information in War. This resulted in an Information Operations Roadmap with fifty-seven recommendations, a handful of which focused on education. In this study, there were key educational findings, to include:
    - Information-type education across DoD is inadequate
    - Education is too narrowly defined
    - Education is disconnected from strategy and military art
    - Education options in existence is not good enough
2. **Strategy is strategy, and war is war, and we do not need niche strategies**. We need to normalize the stuff we are talking about in operations and strategy (in context of both Information and Cyberspace Operations) across the Defense Department and make it part of the Operational Art. This normalizing needs to start in pre-commissioning programs.
3. **NPS stood up a Department of Defense Information Operations Center for Excellence as created a Joint Information Operations Curriculum**, focused on Information in War, and where information sits in war, from an operational and strategic perspective. This curriculum avoids creating an overly technical, narrow program. There are several skill requirements in this program done to take the operational and blend with the technical, to include:
    - Military Art of War
    - Emerging Security Challenges
    - Analytic Methods
    - Information Systems and Influence
    - Intelligence Processes and Application
4. **Building a program rich and deep is a challenge**, and one that spans the educational arena for Information and "Information in Warfare." **We need rich and deep programs, and Cyber is one of them.** NPS is doing a good job although still has some challenges in building both broadly and narrowly defined programs. The problem is that this may not be done across the DoD educational system very well.
5. **Cyber is an information art, which is part of the operational art.**

*Dr. Deborah Goshorn, Assistant Professor, Systems Engineering/Cyber Group,*
*Naval Postgraduate School*

Dr. Deborah Goshorn provided an overview of the Cyber Systems and Operations (CSO) curriculum that supports Department of the Navy objectives to maintain warfighter readiness in an era of reducing budgets by maximizing Cyberspace Operations effectiveness. Highlights of her panel remarks included:

1. **Cyber Systems and Operations (CSO) – Initial Requirement and Sponsors.** The CNO, nine months ago, developed the requirements for and directed the stand-up of the CSO Masters' program under the sponsorship of OPNAV N2N6. Supporting Flag/SES leadership included:
   - Commander, U.S. Fleet Cyber Command/10th Fleet
   - Deputy Director of Operations, U.S. Cyber Command
   - OPNAV N2N6F
   - Vice Director, DISA
   - Assistant DCNO N2N6

2. **CSO – Desired Outcomes.** The CSO curriculum supports CNO Executive Board requirements, and ensures officer readiness to take decisive actions to achieve operational success, to include responsibilities for naval networks, accountability for application of offensive and defense cyber capabilities, and continuing to operate safely in denied or compromised environments. The curriculum meets Department of the Navy Objectives (FY12 and beyond) to maintain warfighter readiness in an era of reduced budgets by **maximizing Cyberspace Operations effectiveness**.
   - Emphasis on Operations
   - Emphasis on System of Systems
   - Emphasis on Big picture Problem Solving

3. **CSO Educational Alignment to Cybersecurity Workforce Framework.**
   - CSO aligned with Fleet Cyber Command mission areas
     - Defensive Cyber Operations
     - Offensive Cyber Operations
     - DoD GIG Operations (DoD Information Network Operations)
   - CSO aligned to National Initiative for Cybersecurity Education (NICE) functional areas
     - Security Provision
     - Operate and Maintain
     - Protect and Defend
     - Analyze
     - Operate and Collect
     - Support
     - Investigate
   - CSO focuses on education and training of the Cyber Workforce at the "Leadership and Future Decision Maker" level (Level II)

4. **CSO has GIG Systems of Systems / Infrastructure Foundation.** CSO focus is on what Navy Information Warfare Officers, Information Professional Officers, and Intelligence Officers will see in the future (5-10 years), from a Global Information Grid (GIG) Systems of Systems and Infrastructure perspective. The CSO leverages the PEO C4I Master Plan (Navy Technical Reference Model), PEO IWS Common Objective Environment and Service Oriented Architecture Core Services, and Intra-PEO Memorandums of Agreement.

5. **CSO has eight sponsor driven, concrete requirements** that include:
   - ESR#1 - Cyber Functions and Fundamentals
   - ESR#2 - Military Applications and Cyberspace Operations
   - ESR#3 - Organizational Construct and Policy
   - ESR#4 - Cyber System of Systems Engineering, Acquisition and Program Management
   - ESR#5 - Independent Research (Masters' Thesis)
   - ESR#6 - Joint Maritime Strategic Planning
   - ESR#7 - Cyber Infrastructure within the GIG
   - ESR#8 - Space

6. **ESR#7 – GIG Infrastructure as a Network Centric System of Systems**. A description of ESR#7 was given to highlight NPS focus on satisfying stakeholder requirements and missions.
   - Mission / Operational Requirements
     - DoD GIG Operations (DoD Information Network Operations)
     - Defensive Cyber Operations
     - Offensive Cyber Operations
     - C2, ISR, and Combat Operations
   - Perspectives (Sponsor)
     - Top Down Systems
     - Middleware Systems
     - Bottom-Up Sensor and Combat Systems
   - Framework: Cyber, C2, ISR and Combat System of Systems GIG Framework
   - Core Infrastructure Systems
     - Networks and Communication Systems
     - Power and Energy Systems

7. **MS CSO is achieved in six quarters, over 1 ½ year period.** CSO courses, as stated above, are oriented on the following four orientations.
   - Mission
   - Policy, Ethics, and Management
   - GIG Infrastructure Technical Foundation
   - Joint Professional Military Education (JPME)

8. **CSO Cyber Wargames.** Cyber Wargames are developed and played twice a year with varying scenarios, as an integral element of two courses: CY4700 (2-5) Cyber Wargame - Blue Force Operations and CY4710 (2-5) Cyber Wargame – Red Force Operations.

- To ensure the curriculum and Cyber Wargames do not get old:
  - Cyber infrastructure will migrate from existing laboratories on campus to obtaining on-loan actual Naval systems from stakeholders
  - Cyber dynamics will include hardware, software, systems, global technologies, TTP
  - Users include students, faculty, stakeholders (e.g., USCYBERCOM, C10F, C3F, NIOC San Diego) with desired resources used from PEO C4I, NCDOC, etc.
- To shape Cyber Wargaming/CSO curriculum), NPS taking inputs from several stakeholders.
- Cyber Wargame courses are conducted at the tactical, operational and strategic levels.
- Cyber Wargame courses have technical underpinnings, to include CONOPS, Design, Architecture, Implementation, Test and Integration, Demonstration, and Documentation.
- Cyber Wargame courses are about integrated learning that include (integrates) Cyber Policy, Cyber Operations, Cyber System of Systems Architecture, and Cyber Intelligence Automation.
- Cyber Warfare courses include the NPS Joint Information Operations Range (JIOR) node.

*Col George Lamont, USAF, Director, Exercise and Training (J7), U.S. Cyber Command*

Col George Lamont provided an overview of USCYBERCOM/J7, issues and challenges, the right mix of education, current initiatives and future thrusts, and take aways/recommendations. Highlights of his panel remarks included:

1. **USCYBERCOM Mission and Operations:**
   - USCYBERCOM stood up in 2010, and achieved FOC in 2011.
   - As the Joint Warfighter responsible for cyberspace, the USCYBERCOM mission is to operate and defend, prepare, and when directed, conduct full spectrum military cyberspace operations.
   - USCYBERCOM focuses mostly on operate and defend lines of operation, with a small, dedicated effort planning for full-spectrum military operations.
2. **USCYBERCOM perspectives on the Cyberspace Workforce** are shaped by joint warfighter mission requirements. We need to build education and training strategies that are as agile, capable, multi-tasking, and dynamic as the workforce we are building.
3. **Issues and Challenges.** The YouTube video, **http://www.youtube.com/watch?v=YmwwrGV_aiE,** "Did You Know 3.0?" revealed some key insights to the development of our future cyberspace professionals.
   - The biggest challenge is that we do not know what we don't know. What will be the emerging technologies? What is the next game changing appliance and application? How will we and our competitors be using cyberspace in the future.
   - We do not know that the future demand for the cyber workforce is going to be.
   - What we do know is that Generation Y (70 million strong) is entering the workforce now and will be co-mingling with the other three generations (Traditionalist, Boomers, and Generation X). They will bring unique attributes and will create new management challenges.
     - They think in multi-tasking context, being able to split time between multiple projects and diversions.

    - They believe they can achieve anything, and will be suspicious of those who believe they can't.
    - Leveraging technology is second nature to them rather than something they have to learn and use.
    - They will have their own agendas and will seek opportunities where those agendas can be realized.
- The very thing we need, stability in the workforce and a united effort, will prove to be the most difficult things to achieve.
- We are educating and training a generation that is very different that the previous two generations, who are not afraid to ask why, question the answers they get, and then leave when they do not like the answers (it is estimated that Generation Y employees will have 10-14 jobs by the age of 38).

4. **What does right look like?**
    - This is a workforce in transition. USCYBERCOM has spent the past several years to catalogue and understand our workforce that is part of a broader effort we call the Joint Cyberspace Training and Certification Standards.
    - One of the outcomes of that effort was the identification of 42 work roles with associated tasks, knowledge, skills, and abilities coupled with proficiency levels necessary to meet USCYBERCOM operational requirements. This construct maps with NIST's NICE construct.
    - As the domain, technology and competitors changes, so is the future demand for the workforce. We are projecting that today's workforce is predominantly manned to "operate and maintain" cyber infrastructure. Five years from now, it is projected the force will be more heavily invested in both "protect and defend" and "offensive operations" missions and lines of operation.

5. **Trained and Ready Cyber Teams – USCYBERCOM Enduring Principle #3.** USCYBERCOM believes so strongly in educating and training the force that he has made it one of his enduring principles and strategic vision components. This principle includes a lot of important ideas that are centered around standards, certification of people and organizations against those standards, and a meaningful way to manage the workforce. There are many thrusts to accomplish this strategy:
    - Build Cyber Teams
    - Standing Watch (24/7)
    - Quick reaction Force
    - Integrate Guard and Reserve
    - Recruitment Plan
    - Standardized Training
    - Establish Joint Certification
    - Standardize, Manage, and Track Workforce

6. **Current Initiatives and Future Thrusts.** Developing the workforce is a team sport. Our focus is on leveraging the expertise, but this also requires a methodology that allows us to provide requirements and understand what the gaps are today. More importantly are the relationships that we build across

the community, with academia, industry, and government that allow us to benefit from the body of experience and knowledge that exists. While this is occurring, we are in the business of transforming the workforce and figuring out what is next, obtaining some sense of what we do not know, and investigating in those activities and educational strategies that have the potential of getting us where we need to be. There is no one size fits all, and we need to focus on how we can build on the next level of operations. Current initiatives and future thrusts (partial list) includes:

- Joint Event Life Cyber
- Joint Cyber Training Certifications and Standards
- Cyber Training Initiative (discussed at Cyber Endeavour 2011)
- Joint Cyber Training Plan
- Cyber Ranges
- Cyber Flag
- Tier 1 Level Exercises (COCOM)
- Joint Individual Certification
- Defense University Engagements (e.g., NPS, DAU, AFIT, JFSC)
- Carnegie Mellon
- Industry (e.g., McAffem Google, AFCEA)
- JMETs
- Service Training Plans
- Job Certifications
- Total Force (Guard and Reserves)
- NSA (ADET), OSD, CIA, DOS Engagements and Initiatives

7. **Key Take Aways – Challenges and Food for Thoughts**.
   - The first of two key challenges is that the future workforce population is trending down. There are concerns that there simply won't be enough people to do the work that needs to be done.
   - The second of two key challenges is that there future STEM graduates are also trending down. So as the labor pool shrinks, the percentage of STEM graduates shrink as well as the overall raw number of graduates.
   - The following questions (food for thought) are provided:
     - What are the real drivers influencing the trend lines?
     - What are some of the solutions (what are we doing about these trends)?
     - How do we get the right intellectual capital (brain trust) engaged in understanding these problems and crafting solutions?

*CAPT (Sel) Tim Unrein, USN, Director, Information Dominance Center for Excellence,*
*Naval Postgraduate School*

CAPT (Sel) Tim Unrein shared his perspectives on what Cyber Educations needs to be from an Information Dominance viewpoint, on how to balance the current workforce with Generation Y, and on how to breakdown current education stovepipes . Highlights of his panel remarks included:

1. **What is Cyber Warfare, and how does it affect the warfighting mission?** During a recent Terminal Fury Exercise, the battle rhythm was intense when the USS Blue Ridge SIPRNET went down, resulting in critical secure communications going down and missions degraded. Cyber affects all Naval warfighting missions. It is important to know how cyber affect the Navy's ability to project force, and how it affects the Navy, Marine Corps, Army and Air Force working together in a Joint Task Force in projecting force.
   - The network is a warfighting system incorporated into operational plans and considerations.
   - Information is ammunition, but how do you organize this information? All too often, it is not organized too well, and this needs to get better.
2. **Cyber Education needs to empower every warfighting domain and mission set (objective).**
3. **Cyber Education needs to begin with the user and all else will follow.**
4. **What Skills do Cyber Professionals need?** Department of Defense Information Network Operations (DINO) is a start. In the Art of War, there is a quote that directly applies, "Know your enemy and know yourself and you can fight a thousand battles without disaster."
5. **Cyber Professional Development / Education Considerations**
   - Know the Cyber Terrain. Its networks, firewalls, servers, and data centers. Know security workarounds when the network does not work.
   - Define the Cyber Structure and Single Points of Failure. Identify the ways to fix and mitigate, and help everyone learn at all levels in the chain of command.
   - We need to be Joint, Interagency, Whole of Government, and Whole of Nation. Our Cyber education programs need to follow suit. In the Cyber realm, what happens in one place impacts everyone. What changes in the Joint environment with second and third order effects also needs to be considered.
   - What can we do about it? Clear rules of engagement models that are well understood in the event someone does harm. In the open press, industry has stated that they are tired of guarding the fence...and they now seek to train more Rottweiler inside the fence to have those attacking them feel the pain." We should follow their lead in the government and military, and develop a complete national approach with enhanced communications channels.
   - We need to catalogue "whole of nation" cyber capabilities and competencies.
6. **Balancing the Workforce with Generation Y (Challenge).** Cyber education in the Navy (at the officer level) begins with midshipmen, who are familiar with technology, they expect it, they are agile with it, but they do not always know what is under the hood. So that is where educating the Cyber Force comes in...midshipmen and officers (junior) need to know what the impact is and what to do if someone "pulls the distributor cap, or what happens when someone pours sugar in the gas tank."

*Dr. Ernest McDuffie, Lead, National Initiative for Cyber Education (NICE), National Institute of Standards and Technology (NIST)*

Dr. Ernest McDuffie provided an overview of National Initiative for Cyberspace Education (NICE), and perspectives on how education, training and professional development are complementary. Highlights of his panel remarks included:

1. **Principle Drivers for NICE**
   - Comprehensive National Cybersecurity Initiative (CNCI) (2008). CNCI has 12 mutually-reinforcing initiatives that are intended to establish a front line of defense against today's immediate threats, to defend against the full spectrum of threats, and to strengthen the future cybersecurity environment. Number #8 states that ..."we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees."
   - Cyberspace Policy Review (60-Day Cyber Review). As a result of this review, NIST inherited the CNCI #8 initiative. Key findings/recommendations included:
     - Promote cybersecurity risk awareness for all citizens
     - Build an education system that will enhance understanding of cybersecurity and allow the United States to retain and expand upon its scientific, engineering, and market leadership in information technology.
     - Expand and train the workforce to protect the Nation's competitive advantage.

2. **NICE Overview, Missions, and Goals.** In March 2010, NICE was formed and supported President Obama's decree and vision to conduct "a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century." NIST is committed to establishing public-private partnerships across the Federal Government, Department of Defense, Industry and Academia in order to educate and train the next generation workforce. Within the U.S., our students are turning away from STEM, and this impacts national security if this downward trend continues. Within the DoD, there are 80,000 – 240,000 cyber professional in its ranks. This pool has to be refreshed to accommodate a 10% attrition rate to keep afloat, which accounts for 8,000 – 24,000 new cyber professionals each year. This is going to be challenge, and we need to establish baselines.
   - Mission. NICE will enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population
   - Goals
     - Raise awareness among the American public about the risks of online activity.
     - Broaden the pool of skilled workers capable of supporting a cyber-secure nation.
     - Develop and maintain an unrivalled, globally competitive cybersecurity workforce.

3. **NICE Internal Component Structure**
   - National Cybersecurity Awareness (DHS) – Promote cybersecurity and awareness and responsible use of the Internet, and make cybersecurity a popular educational and career pursuit for older students.
   - Formal Security Education (National Science Foundation, Education Institutions) – Bolster formal education programs to focus on Cybersecurity and Science, Technology, Engineering, and Mathematics (STEM) fields.
   - Cybersecurity Workforce Structure (DHS, OMB, ODNI) – Identify competencies used in workforce planning, training and development, performance management, recruitment, and selection.

- Cybersecurity Workforce Training and Professional Development (DOD, ODNI, DHS) – Intensify training and professional development programs for federal cybersecurity workforce.
- National Institute for Cybersecurity Studies (NICS)
- Success Stories:
  - DHS touring cities, sponsoring local champions
  - Cyber San Antonio, San Diego, and Florida (Kennedy)
  - NSA Centers of Academic Excellence (166 schools)
  - Two-Year Schools/Technical Colleges
  - Global Institute of Cybersecurity Research (NSA, Boeing, Lockheed Martin)

4. **NICE Strategic Outcomes.** The primary goals (strategic outcomes) of NICE across the education space include:
   - Public Awareness – increasing public awareness of cybersecurity risks, responsible use of the Internet, and cybersecurity as a career path.
   - K-12 Education – developing the next generation of cybersecurity workers and encourage interest in STEM disciplines.
   - Higher Education – rating the competency and capability if information security professionals and practitioners.

5. **NICE Cybersecurity Pipeline.** NICE seeks to create a Digital Nation of Cybersecurity Researchers, Cybersecurity Professionals, Cybersecurity-Capable Workforce, and Cybersecurity-Aware Citizens. The Cybersecurity Talent Pipeline includes:
   - K through Middle School
   - High School
   - Universities, Colleges, Community Colleges, and Vocational/Technical Schools
   - Graduate, Professional Degree Programs
   - Training, Licensing, Certification Programs

6. **NICE Awareness Campaign.** The NICE Awareness Campaign includes:
   - Stop-Think-Connect (keeping the web safer for everyone) at www.stopthinkconnect.org
   - Partnerships with DARE
   - Public Service Awareness (PSA) Contests
   - Annual NICE Workshops
     - http://csrc.nist.gov/nice/2012workshop/
     - "Shaping the Future of Cyberspace Education – Connecting the Dots in Cyberspace Workshop," October 30 – November 1, 2012
   - Plan and execute Cyber City Tours nationwide
   - Launch and expand National Network
   - Improve Toolkit and general resources
   - Find new outreach opportunities and mechanisms
   - Coordinating with the Campaign and National Cyber Security Awareness Month (NCSAM)

7. **NICE Training and Professional Development.** Key NICE training and professional development activities include the NICE Framework, Training Catalog / NICS, Workforce Inventory, Training Gap Analysis, and Professional Development Roadmaps.

8. **National Cybersecurity Workforce Framework.** The Cybersecurity Workforce Framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas. These categories have served as a framework for multiple education and workforce development programs, such as the NPS CSO Master's Program. **The categories include operate and maintain, protect and defend, investigate, operate and collect, analyze, securely provision, and support.**

9. **NICE Strategic Plan.** The Strategic Plan serves as a framework for executing the initiative's mission and achieving its vision, identification of major goals and objectives, and was finalized after a public review period ending 3 October 2011 (achieving community buy-in).

*Mr. William (Bill) Waddell, Director, Command, Control and Cyberspace Group, U.S. Army War College*

Mr. William (Bill) Waddell provided an overview of the Cyberspace education system, military leadership in cyberspace, strategic challenges in cyberspace that needs to be included in cyberspace education programs, and strategic education to do list. Highlights of his panel remarks included:

1. **The Cyber Community has three primary groups, with calculations required to accommodate the different perspectives and focus.** Within the three groups, only the Department of Defense is responsible for U.S. national sovereignty. The three groups, and their perspectives and focus areas, are:
    - General population – vulnerability analysis
    - Business and corporate world – vulnerability vs cost vs risk
    - Government / Department of Defense / Interagency
        - Administration / Congress – balance privacy/civil liberties with protection in laws
        - Department of Homeland Security – Critical Infrastructure Protection
        - Department of Justice – Crime
        - Department of State – International Relationships
        - **Department of Defense – U.S. National Sovereignty**

2. **Education System.** Some of the planning factors and considerations for the Department of Defense and Government include:
    - Civilian education systems reduced in STEM graduates (significant downward trends). STEM graduates in 2012 (U.S. citizens) will number around 100,000. How many will really fit into the DoD/Government? Probably less than 1% of them.
    - Percentage of graduates eligible for government cyber employment. The estimated 1,000 STEM graduates that fit within the DoD/Government is significantly less than the 8,000 – 24,000 needed to accommodate for DoD/Government attrition.
    - Government monetary incentives may be the only way to attack more STEM graduates/cyber professionals into government service, especially with competition with industry/higher pay.

- Retention – Generation Y employees will have an estimated 10-14 jobs by the time they are 38, creating retention challenges. Experienced government cyber professionals are also moving to the corporate world or retiring, exacerbating the problem.
- Military physical and attitude requirements, and clearance requirements. The graduates and young professionals with the most capable cyber skills and educational background may not meet military standards.
- Leadership development. In looking at 2025 scenarios with cyber academic prowess unavailable or moving off shore, leadership is going to have to train their own (internal) personnel, a challenge in today's current budget climate and high operational tempo.

3. **Military Leadership in Cyberspace.** Some U.S. Army War College recommendations and requirements for Leadership and Commanders in Cyberspace are to:
   - **Know Thyself**
     - Cyber is the Commander's business, not just the N6/A6/J6.
     - Understand own capabilities and vulnerabilities
     - Educate, train, and prepare for vulnerability reduction
     - Practice, exercise, and be responsible for DCO/CND
     - Operations in a degraded/denied environment
   - **Know thy Enemy**
     - Understand the threat (CNE)
     - Establish counter-measures and counter-attack
     - Establish and understand Rules of Engagement (ROE)
     - Understand OCO requirements, effects, and capabilities
   - **Be aware of the Issues (Commanders Issues)**
     - Developing and ensuring awareness of ROE
     - Training and preparing the forces for the fight
     - Development of Intelligence (CNE)
     - Cyber Hygiene
     - Preparation for future operations

4. **Strategic Challenges in Cyberspace.** What the U.S. Army War College does in its classes is to develop a list of challenges they can walk out of the room and discuss accordingly. These include:
   - Defining a "hostile act" in cyberspace
   - Identifying Cyber Warfare and Hostile Intent
   - Intelligence pre-determination of attack
   - Attributions
   - Deterrence
   - Supply Chain Management
   - Managing a limited talent pool
   - Information sharing with industry
   - Ensuring protection of civil liberties
   - Developing the right skill sets for the future
   - Interagency de-confliction
   - New generation of threat

5. **Strategic To Do List.** Within the Department of Defense, the Educational System is 5-10 years behind reality. Some recommendations for the Department of Defense to consider includes:
   - Establish Cyber as a Joint and Service PME requirement – it is not listed in the 200 areas of the educational institution/school system. Wedging something that is not on the JPME list is very hard to do in academics. Until we get every student out of the list of institutions to get a solid understanding of cyber, we will remain behind the eight ball.
   - Preparing our leaders, to include making DCO success a command issue and increasing emphasis at service schools.
   - Establishing rapport between service schools and USCYBERCOM and service components
   - Conducting senior leader and GO/FO education
   - Conducting (more) exercises
   - Maintaining inertia in a fiscally austere environment

*Panel III Questions / Open Forum Discussion*

Dr. Hy Rothstein opened up the panel for questions and comments from participants, highlights of which included

1. **Does DoD 8570 support or complicate efforts to educate cyber warriors?**
   - Certifications are valuable, and are compliance factors, but significant portion of those achieving the certifications (e.g., CISSP) take the test and get certified, but are hardly qualified to secure and protect the network.
   - Current 8570 focus on IA is not enough (educating cyber warriors requires IA, but much more focus on CNE, OCO, DCO, DGO/DINO)
   - 8570/FISMA is not it needs to be – needs to be improved. Certifications are outdated and irrelevant (in many cases) to the dynamic changes in Cyber and advanced persistent threats – they need to be refreshed routinely (a certification five years ago does little good today).
   - Continuing Education Credit requirements are important, but what is their relative effectiveness, especially since is also based on the honor system?
2. **How do you "Exercise Cyber" more in Fleet and Joint Exercises?**
   - Make Flag Officers accountable for doing so.
   - Focusing on Naval Academy graduates makes them good in Cyber, but exercises help make them Cyber professionals.
   - Current exercises support COCOM OPLANS, there is no Cyber built into these plans today.
   - **According to the J. Michael Gilmore, Pentagon Director of Operational Test and Evaluation report, the quality of exercises is declining and "the cyber threat portrayed during assessed exercises remains consistently below that expected from a nation-state level adversary."** Networks have issues and vulnerabilities, so when Cyber has a major part in an exercise, it messes things up. Cyber needs to be included in the initial planning meetings.
   - At the Information Operations Summit, the Office of the Under Secretary of Defense for Policy, stated that there is a challenge in normalizing Information Operations, and that the Cyber part of that has been normalized days before Joint became important.
   - At the Flag Education Level, Junior Flag Officers attend the Executive Education IO Program at Maxwell AFB. At the Senior Flag Officer level, e.g., those en-route a JTF/J3 position, it is strongly recommended they attend an IO Course on the informational aspects of war, and incentivize.

- Unless the DoD community makes it a priority to put cyber into exercises, and incentivizes this for promotions and key jobs, cyber may never get a foot hold in exercises.
- USCYBERCOM infused flag/general officers into three major exercises this year at the one star level (Cyber Forward Element). That level of interest may not carry enough bandwidth to matter.
- Education at the NPS includes participating in quarterly exercises, which are COCOM sponsored events are opportunities to test IO/Cyber S&T and transition S&T.
- The Army's Senior Leader Seminar (O6 Level) provides a week long environment where they are exposed to Cyberspace Operations and Integration.
- NIST focuses on staff officer and leadership education and training in the private sector. NIST sponsors the Cyber Storm Exercises and competitions, such as US Cyber Patriot, US Cyber Challenge, and Cyber Olympiad (March Madness) that engages the public. NIST saw talent that could serve as potential recruiting targets for a federal employee, provided the hurdles are lowered or removed during the recruitment process.

3. **How do we get people in the "wings" ready?**
    - Self-education is the key, as there are not enough dollars to do so. As in the past, folks need to be responsible for some (if not most) of their training and proficiency (concept in Small Wars Journal). A little more difficult to do with current millennial generation (Generation Y).
    - We need an environment to keep skills and develop further, such as an environment for people to exercise in virtual worlds with state-of-the-art equipment,, e.g., Net, and engage in competitions.
    - The University of Alaska has virtual laboratory space to do just that, as do other universities.
    - Need to also focus on those individuals outside the formal education environment.
    - An HR issue is how to evaluate experience equivalence against a degree.
    - We also need cyber playgrounds, and not just show up in exercises. An example of how this can work is the Army War College partnership with the University of Maryland (Baltimore) where folks can log in and participate in workspaces (playground).
    - The wave of the future is Cyber test ranges with nodes and modes, e.g., NPS Cyber Siege and Joint IO Range.
    - Navy Center for Information Dominance (CID) brings officers and enlisted personnel together into the same playground.

4. **As we have done in the past with IO/Cyber tools, we need to get together as a "Whole of Nation" and catalog the diverse Cyber education, training, certification, and exercise programs.** What can the National Cyber Professional Community do now and in the future?

# Naval Postgraduate School Common Operational Research (CORE) Laboratory Overview and Capabilities

*COL Greg Wilson, USA, Co-Director, CORE Laboratory, Defense Analysis Department, Naval Postgraduate School (CORE Laboratory Overview)*

*Rob Schroeder and Sean Everton (Arab Spring Twitter Analysis)*

*Dan Cunningham (FARC Emergent Leader Study)*

*Patrick Dudas (Twitter Dynamic Network Visualization)*

COL Greg Wilson provided an overview of the CORE Laboratory and capabilities, and then had members of the CORE Laboratory provide an overview of three laboratory initiatives. Highlights of their presentations include:

## CORE Laboratory

### 1. CORE Laboratory and Capabilities Overview

- The Common Operational Research Laboratory (CORE) Laboratory supports field operatives engaged in irregular warfare and develops operators' knowledge, skills, and abilities in visual analytics. Three visual analytic methodologies – geospatial, temporal, and relational – are emphasized in the CORE Laboratory courses and research projects.
- The CORE Laboratory was an actionable, forward thinking idea of students in the Special Operations program, which includes 171 students (91 from U.S. Joint Special Operations), a new Colombian officer, and 30 internationals from front line states. This program included twelve individuals prior to 9/11 – since then the demand signal has significantly increased.
- Several years ago, an NPS student posed the question, "where are we looking at methods to illuminate networks and looking at the irregular warfare battlespace in a new way?" What are the new methodologies, how do we structure data, how do we visualize this battlespace? This student got seed money by reaching out to the OSD RRTO. With this seed money, NPS was able to stand up and spirally develop the CORE Laboratory which is now housed in the Department of Defense Analysis, and that today supports NPS Special Operations, Irregular Warfare, and Information Operations curriculum.
- In looking at irregular warfare analytical methodology, the CORE Laboratory slogan is "designed by operators for operators." The CORE Laboratory fuses advanced irregular warfare analytical methodology with world class NPS faculty plus operators (which is the real secret sauce) coming out of theater serving in Columbia, Philippines, Iraq, and Afghanistan.

2. **CORE Laboratory – Supporting the Human Domain.** What is exciting to the CORE Laboratory is that it supports USSOCOM and its new warfighting domain. As the Navy has the maritime domain and the Army the land domain, **USSOCOM has the "Human Domain**." The NPS CORE Laboratory will be the science behind understanding this domain that USSOCOM is charged with operating in.

3. **CORE Laboratory – Fusing Technology with Methodology.** The NPS CORE Laboratory partners with industry that enables us to operationalize our methodologies.
   - One of the first CORE Laboratory partnerships with industry involved **Palantir**, which is relatively new software used within the CORE Laboratory that combines data integration, search and discovery, knowledge management, and collaboration.
   - A second partnership with industry (Google) is **Lighthouse**, a project that uses smart phones and other light weight, cheap devices to gather social-cultural data. Early successes included the Combined Special Forces Operations Command in Afghanistan using eight phones from the Lighthouse project to map out, over a 90 day period, an Afghanistan network, where methods we used that allowed Commanders to understand the environment empirically vice intuition alone. These networks included kinship networks (to determine ties w/ Taliban) and ego networks (who to approach to engage and influence).
   - Additionally, building on Lighthouse, NPS CORE Laboratory students recently developed an iOS-based application called Improvised Explosive Device Network Analysis (IEDNA), which allows Explosive Ordinance Disposal (EOD) technicians to compile information about IED trends into a streamlined and accessible database.

4. **CORE Laboratory – Social Network Analysis.** Social network analysis is important in looking at the "Human Domain" in a way that currently does not exist.
   - Old school academics/analysts used code books to annotate the relationships between actors
   - New school academics/analysts use custom applications that can now move structured data into analytical packages, visualizing the network in ways that is not currently being done in the Department of Defense.
   - Social network analysis is not link analysis – it is about looking at the social space, and how individuals (actors) are connected to other individuals or objects of the same type.
   - Centrality measures are the most intuitive of metrics used, and includes Degree Centrality, Closeness Centrality, Betweeness Centrality, and Eigen Vector Centrality. These measures provide a different viewpoint in identifying actors in a network of interest (patterns of ties) and arcs (their kinship, family, business, and other relationships).
   - Through these metrics, the CORE Laboratory was able to "illuminate networks" and craft the appropriate strategy.
   - In the near future in support of OSD and USSOCOM, the CORE Laboratory will increasingly focus on the human domain and social networks, and this applies to social, topographical, and influence networks (and also to IED networks).

5. **CORE Laboratory Underpinning – Graduate Level Courses.** There are several graduate level courses offered by the CORE Laboratory. The NPS is seeing a lot of interest from international counter-

terrorism programs in these courses. The CORE Laboratory is building this sequence of courses and now starting to see them implemented (these methods) in the combat theaters and in some of our partner nations. Graduate level courses include:

- DA 3610 Visual Analytics – focuses on collection of data at a faster rate than our ability to analyze it – introduces new tools and technology that support the integration and fusion of this massive amount of data, especially geospatial, temporal, and relational data, so analysts and operators are better prepared to create a COP in their area of responsibility.
- DA 3600 Geographical and Temporal Dimensions of Dark Networks – focuses on the spatial, temporal, and relational dimensions of Dark Networks (dark networks involve covert and illegal activity such as drug trafficking and terror networks)
- DA 4600 Tracking and Disrupting Dark Networks – focuses at how to illuminate networked adversaries, developing a deep understanding on how to use Social Network Analysis metrics (e.g., topology, centrality, cohesion, brokerage) to better understand the relational aspects of dark networks and how to design intervention strategies for disrupting, destabilizing and possibly destroying dark networks.
  - Identify and describe these networks and their dynamics
  - Design intervention strategies for disrupting, destabilizing and possibly destroying dark networks once identified and described
- DA 4610 Dynamic Network Analysis (Capstone Course) – focuses on additional substantive and methodological tools for analyzing relational networks, paying attention to issues concerning the collection and preparation of relational data in software programs such as Palantir, Analysts Notebook, Excel/Access, social network analysis tools such as UCINET, Pajek and ORA (Organizational Risk Analyzer), explore dynamic network analysis where users examine the effects of actual ties and virtual ties.
- The NPS CORE Laboratory co-directors and professors encourage students to bring own data or code own data. If students don't have data, the CORE Laboratory has a canned data set. In coding data – students can bring their own, or if not, they can code data from international crisis group reports.

6. **Core Laboratory – Supporting Partner Nations.** The NPS CORE Laboratory and capabilities (e.g., Palantir, Lighthouse, and Social Network Analysis) are supporting Partner Nation Counter-Terrorism and Counter-Insurgency efforts in Afghanistan and Iraq, Thailand (Civil Affairs), Philippines (Foreign Internal Defense and Peace Process), and Colombia (Ministry of Defense Counter-Insurgency w/ FARC), Nigeria (General Officers), and North Africa (prior to Libya).

7. **Core Laboratory – Supporting Law Enforcement and Homeland Defense.** The NPS CORE Laboratory and capabilities are not all about supporting the warfighter. CORE Laboratory methods implemented with Lighthouse are being used by the Massachusetts Police and California Gang Task Forces.

## Arab Spring Twitter Analysis

1. The NPS CORE Laboratory conducted an Arab Spring Twitter Analysis of the 2011–2012 Egyptian revolution that took place following a popular uprising that began on Tuesday, 25 January 2011. This uprising was mainly a campaign of non-violent civil resistance, which featured a series of demonstrations, marches, acts of civil disobedience, and labor strikes, coordinated in part with the use of social media tools that included Twitter.

2. The NPS CORE Laboratory wanted to get a better appreciation on what was going on and behavior patterns exhibited in Tweets (short messages, 140 characters, with bumper sticker comments and phrases), as well as the directional ties between tweets. A network of 193,000 users was evaluated, and the CORE Laboratory used Social Network Analysis (SNA) centrality measures and other SNA algorithms to illuminate this network from "tweets alone."

3. Some key findings of the Arab Spring Twitter Analysis included:
   - NPS illuminated those groups of individuals with international ties
   - NPS gained a better understanding how Al Jazeera Arabic and Al Arabiya Arabic had thousands of users and conduits to frame the discussion, while traditional media did not
   - NPS identified a Mubarak Parody "false account" in both English and Arabic had a substantive following and debate.

## FARC Emergent Leader Study

1. The NPS CORE Laboratory, in partnership with the Colombia Ministry of Defense, conducted a Foreign Emergent Leadership study of the Revolutionary Armed Forces of Colombia (FARC), with a principal focus on the Internationalization of the FARC. Formally founded in 1964 as the military wing of the Colombian Communist Party, the FARC is Colombia's oldest, largest, most capable, and best-equipped Marxist insurgency.

2. Palantir was used by the NPS CORE Laboratory to illustrate FARC events and groups in which they have collaborated, and events involving the FARC and other terrorist groups. Information used in this analysis included public statements, court statements, and bona fide attacks. The data was analyzed and a visual representation of the geospatial and social network techniques were obtained. The analysis illuminated new dynamics of the FARC insurgency and narcotics efforts operating in Colombia and Venezuela, and highlighted centers of activity that changed over time and identified controversial camps of the Venezuelan border.

3. Using Palantir and other CORE Laboratory techniques, NPS students were able to illuminate the persons, political organization, and military organization of the FARC, friendship and kinship relationships, and potential emergent leaders if key FARC leadership (network nodes) were eliminated. It also flagged some of the less obvious relationships at the edge of the network, which provided increased insights on FARC power brokers and influence agents.

## Twitter Dynamic Network Visualization

1. The NPS CORE Laboratory developed a capability to conduct real time dynamic visualization that looks at information as it is being tweeted on Twitter.
2. With each Tweet having a hash tag, user name, location (geo-coded), the NPS CORE Laboratory is capturing these hash tags and exporting them, and information contained in these tweets, into a GX file (.net file) in order to conduct a series of network analyses.
3. Using social network analysis tools such as Gephi, NPS CORE Laboratory students and analysts are then able to develop a stream of tweets identifying the key community names and players (actors).
4. The NPS CORE Laboratory are investigating the right SNA tools at NPS (and partners) to better visualize and geo-locate Tweets (and component parts) from Twitter.

## Questions and Answer Period

1. **Is the NPS CORE Laboratory conducting social network analysis on malware coders, and the pedigree of the code?** Not yet, just started exploring.
2. **In Iraq and Afghanistan, did the folks using and consuming the analysis also collect on their smart phones and hand held devices?**
   - We are learning as we go
   - Training, educating, and building subject matter experts in the next effort
   - Looking to identify best operational and intelligence units to have capability to reside (it does not need to everywhere and with everyone)
   - Palantir is the key technology being used in these theaters (forward deployed units)
3. **Are there any issues in employing CORE Laboratory capabilities?** Yes.
   - CORE Laboratory capabilities are bumping up programs of record.
   - This is a DoD capability that is being requested by other communities, e.g., law enforcement and homeland defense.
   - There are some enclaves will not wanting to use this capability, as it competes (well) against their POR systems.
   - This is not just about NPS, it is about the operators, leaders, and decision makers.
4. **Are there any plans to incorporate NPS capabilities in Mexico, with their complex problem sets and organizations?**
   - NPS capabilities are not currently being used.
   - Law Enforcement / Border Security networks and actors within Mexico/U.S. border offer unique opportunities.
   - USSOCOM hosting workshop on Mexico, which will expose NPS folks to problem sets.

# Panel IV – Developing, Operationalizing, and Assuring Cloud and Cellular Systems, Networks, and Architectures

*Mr. Thomas Sweet, President, IO Centric Solutions and Cyber Endeavour 2012 Coordinator*

Mr. Thomas Sweet served as the moderator for this panel, introducing panel members and providing introductory remarks, then turned the panel over to the four panel members.

*Mr. Roberto Sandoval, Chief Security Engineer, Air Force DCGS Program, HQ AF ISR Agency*

Mr. Roberto Sandoval provided an overview of the Air Force Distributed Common Ground Station (DCGS) Security Information Event Management (SIEM) automated reduction and enterprise monitoring technology. Highlights of his panel remarks included:

1. **AF DCGS SIEM Requirements.** AF DCGS requirements came about as a change in security policy from DCID 6/3 to Intelligence Community Directive 503 (ICD-503) and the need under ICD-503 to constantly monitor AF DCGS networks and reduce audits. These requirements are derived from:
   - Non-compliance for audit reviews
   - New requirements for automated, continuous on-line monitoring and real-time alert capability
   - New requirements for centralized management and correlation of audit events
   - New requirements for audit reduction and reporting capability and additional levels of protection required for audit data
2. **AF DCGS Risk Management Framework.** The AF DCGS has a risk management framework (RMF) that includes the following six steps:
   - Categorize Information System
   - Select Security Controls
   - Implement Security Controls
   - Assess Security Controls
   - Authorize Information System
   - Monitor Security Controls
3. **AF DCGS Assessment and Authorization (A&A) Process (ICD-503).** ICD-503 brings security into lifecycle support. Leadership and workforce are trained on the system. The Air Force used to send teams out, generate a POA&M to correct issues, and provide interim or permanent authority to proceed. SIEM can do scans remotely, enabling resource and time savings as well as better results. The current process includes:
   - Configuration management processes ensure a stable baseline
   - Modifications to AF DCGS systems are approved through several organizations, including the PM security office
   - A detailed documentation package is approved through a boarding process prior to site delivery
   - After the modifications to the system are complete, A6SC Security Assessors will run test tools, perform ad hoc tests, then produce a test report

- After evaluation the risk of security vulnerabilities, the Authorizing Official will issue an Authority to Operate (ATO) with a POA&M.
- This POA&M is a list of security vulnerabilities that must be fixed. The site is given a suspense date, and if the vulnerabilities are not addressed by then, the ATO can be revoked.

4. **AF DCGS SIEM Technical Solutions.** The Air Force decided on ArcSight SIEM, a commercial tool that was advocated by the Office of the Director of National Intelligence (ODNI) for the Intelligence Community, that enables AF DCGS to meet the following two new requirements:
   - ICS 700-2 Use of Audit Data for Insider Threat Detection
   - ICS 500-27 Collection and Sharing of Audit Data

5. **SIEM Technological Solutions.** ArcSight SIEM technology provides real-time (or near real time) analysis of security information generated by network hardware and applications with the primary goals of enterprise monitoring and audit reduction.
   - SIEM solutions are critical in the rapid identification of internal and/or external attacks and nullifying the insider threat
     - Configurable triggers respond to activity automatically and/or to alert analysts
     - Proposed implementations provide enterprise level management of AF DCGS security logs, enabling analysts to see an attack that may affect multiple sites
     - ESM correlation engine and graphical representation of user events paint a picture for analysts to quickly recognize malicious activity
     - Active List capabilities limit the scope of an analyst's view of specific parameters, such as certain source and destination IP addresses, event types and specific users. This can be configured on the sport to view events associated with a suspected attack in progress.
   - SIEM technologies address the compliance and security needs of an enterprise by collecting security data from all critical assets on a network and presenting that data in a unified format via a single interface.

*Mr. John McLaughlin, Chief Security Architect, Systems Security Division, IBM*

Mr. John McLaughlin provided an overview of the IBM X-Force and key findings of a 2011 IBM X-Force Trend and Risk Report. Highlights of his panel remarks included.

1. **IBM X-Force Overview.** The IBM X-Force is a research and development organization at IBM that monitors the latest Internet threat trends, develops security content for customers, and helps customers and the public on how to respond to emerging and critical threats, thus providing a foundation for a preemptive approach to Internet Security.

2. **IBM X-Force 2011 Trend and Risk Report**. 2011 was considered the year of the security breach. The IBM X-Force provided a sampling of security incidents by attack type, time and impact. The conjecture of relative breach impact is based on publically disclosed information regarding leaked records and financial losses. The primary attack types include SQL injection, URL tampering, Spear Phishing, 3rd party software, DDoS, SecureID, Trojan Software and 'unknown.' Security breaches earlier in the year, such as Sony, were identifiable in most part (e.g., Sony encountered a massive SQL injection attack). What was noted and particularly disturbing were the number of unknown attack type, such as Epsilon in March 2011 and the preponderance of security breaches in the later months of 2011.

3. **IBM Security Systems Division sees key messages** in the IBM X-Force 2011 Trend and Risk Report:
   - New attack activity included:
     - Rise in Shell Command Injection attacks
     - Spikes in SSH Brute Forcing
     - Rise in phishing based malware distribution and click fraud
   - Progress in Internet Security
     - Fewer exploit releases
     - Fewer web application vulnerabilities
     - Better patching
   - The challenge of mobile and the cloud
     - Mobile exploit disclosures up
     - Cloud requires new thinking
     - Social networking no longer fringe pastime

4. **Vulnerability Disclosures were down in 2011.** The total number of vulnerabilities declined over an all-time high in 2010, but it is cyclical as IBM has seen a two year, high-low cycle in vulnerability disclosures since 2006. **In 2012 we expect to see an increase number of vulnerabilities across all software vendors and manufacturers**.

5. **Patching is getting better.** Another trend is that we help ourselves with better patching. In 2011, when vulnerabilities were announced, 58% patched on the same day and 6% patched on 1+ days, **but 36% did not patch at all.** There have been several instances of zero day exploits, but we are also seeing some Minus-1 day exploits, where we have an attack/exploit first, and the vulnerability is published the day afterward.

6. **Mobile OS vulnerabilities and exploits have arrived.** There has been a significant increase in total mobile operating system vulnerabilities over the past two years (slight dip in 2011), due to the increase in enterprise users bringing their own devices into the workplace. Attackers finding these devices have a lucrative new attack opportunity, which has been shown in the order of magnitude increases in Mobile OS exploits.

7. **Challenges of Cloud Security.** IBM saw a number of high profile cloud breaches in 2011 affecting well-known organizations and large populations of their customers. In general, things requiring a lot of interaction between the client and systems and that are data-intensive tend not to fit well into the cloud. Customers looking at cloud environments should consider:
   - Cloud appropriate workloads
   - Appropriate service level agreements
   - Life cycle approaches to deployment that include exit strategies should things not work out

8. **The Counter Attack – Three Tenets of Security Intelligence.** Security Intelligence is about detecting activity, providing some correlation, doing some behavioral analysis, and once that is solved, doing some predictive analysis. It answers two questions, “what just happened?” and “what are they doing?” Security Intelligence is enabling progress to optimized security, and includes information and

event management, advanced correlation and deep analytics, and external threat research. The three tenets of Security Intelligence are:

- Intelligence – ability to make sense of large amounts of security and compliance relevant data
- Integration – foundation of intelligence, enabling consistent, normalized analysis of disparate data
- Automation – element that brings Security Intelligence into the modern era by helping drive out unneeded complexity and reduce the total cost of ownership.

9. **This is not a technical problem, but a business challenge.** The IBM Security Systems Division contends that many of the 2011 breaches could have been prevented. Significant effort is required to inventory, identify, and close each vulnerability. Financial and operational resistance always encountered, so how much of an investment is enough?

10. **If IBM X-Force was running the IT Department.** Based on the results of the 2011 report, the IBM X-Force listed the ten actions beyond the basics if they ran the IT Departments.
    - Perform regular 3rd party external and internal security audits
    - Control your endpoints
    - Segment sensitive systems and information
    - Protect your network
    - Audit your web applications
    - Train end users about phishing and spear phishing
    - Search for bad passwords
    - Integrate security into every project plan
    - Examine the policies of business partners
    - Have a solid incident response plan

*Mr. Randy Fuerst, Chief Operating Officer, Oceus Networks*

Mr. Randy Fuerst provided an overview of Oceus Networks wired and wireless capabilities and insights on how the government can benefit from commercial R&D investments. Highlights of his panel remarks included:

1. **Oceus Networks Overview.** Oceus Networks is a U.S. based company with exclusive access to Ericsson technology for U.S. DoD, Intelligence Community, and State Department. Oceus Networks provides wired and wireless (cellular and broadband technology) to government and industry customers, to include 3G/4G LTE tactical networks. They also provide COTS turnkey solutions that transport information in even the most remote locations.

2. **Partnering with the Army CIO and Department of the Navy.** The Army CIO Office seeks secure solutions that the previous 2G/3G networks could not provide, which is provided by Oceus Networks' private 4G LTE tactical network. Oceus Networks is in the process of securing networks within the Department of the Navy.

3. **The Communications Gap.** Classic military wave forms are needed and will continue to exist, by commercial advancements with 4G LTE enables high bandwidth, high data rate applications. The military and government currently own spectrum that can support 4G LTE, and could benefit from commercial investments in 4G LTE to establish their own networks on their bases. There are lobbyists pressuring the current administration and Pentagon to rip that spectrum out of the DoD and auction it off to the carriers, or make provisions for them to use. Because there are so many existing military systems in that spectrum today, it is strongly recommended that before the government or DoD gives it away and then have to buy it back, e.g., Leased SATCOM. They should reconsider doing so and reconsider future requirements. DODIS leadership commented on the fact that they are using 3G in the battlefield when the commercial world is using 4G/ 5G, such as the 4G LTE. We (DODIS) need to leverage that capability so we can train as we can fight.

4. **Leveraging 4G LTE for Base Training and Testing (Recommendation).** The Department of Defense could leverage 4G LTE for training and testing on base. It is not about the network, it is the applications, data, proliferation of sensor information. The current tactical networks are choked with a lot of information and with so little bandwidth. Carriers are talking about a roaming license that can be used to bring your own device, which on a secure 4G LTE would mean increased coverage, capacity, and security for the troops as they conduct base training and testing.

5. **Supporting the Warfighters.** Oceus Networks 4G LTE solutions support warfighters, to include:
   - Enterprise and Tactical C4ISR Deployments on Bases (CONUS)
   - Tactical Army Deployment (Army Labs, NIE, and AEWE as well as deployed), from small units to theatre of operations
   - NAVAIR Operational Concepts (Sea Trial and UAV) involving the USS Kearsarge (LHD-3)
   - Coordination with NSA/DISA for 4G LTE encryption (FIPS 140-2 AES256)
   - 4G LTE Afloat Security Architecture with four VPN tunnels w/ AES 128/256 encryption for proposed phone security

6. **Network Management Control Center (NMCC).** Oceus Networks NMCC support 4G LTE and 3G Point-to-Point networks (non-propriety). The NMCC provides rapid deployment, network management, and security. Mobile device management includes over the air programming, configuring of single and multiple devices, application pushes, and compliance reporting.

7. **Concluding Remarks**: The government and military can (and should) leverage economies of scale and increase supply. They should offload critical data networks with resultant increase of performance by a factor of 100-10,000. They should also adopt commercial growth rate and stay there. They should secure solutions for data transmit and storage using FIPS 104-2/Suite B, and IA validated by J8 C4AD (JITC Certification Q4 2012 for fixed, mobile, air, and sea).

### *WO1 Eddie Contreras, Army Reserve Information Operations Command (ARIOC)*

WO1 Eddie Contreras provided his perspectives on cybersecurity innovation within the banking industry and the importance of analytics. Highlights of his panel remarks included:

1. **Security is 7% of the Information Technology Budget within industry (Gartner)**.
2. **How do you forecast security requirements and budget when you don't know what is coming from the threat?** Within my bank, there is a strategic plan that addresses a 3-5 year period, and much of the costs spent on security projects/innovation are analytics, social networking, and enhanced tools. How do you place a dollar value to security – if something does not happen (e.g., breach, exploitation)? How do you tell about threats when it does not happen?
3. **Analytics is integral to our solutions.** One of the first questions to ask is "what is it that we are really trying to secure is one of the first questions to ask?" The perimeter? End points? We then ask, "are there any other departments that have initiatives that need security, and do these need to be inside or outside the perimeter?" Analytics/metrics account for 20% of the budget.
    - Analytics is more than understanding where you are going
    - Analytics is about understanding where you want to be, and if you apply security to it, how to arrive in a secure manner.
4. **Strategy is key, freedom in its execution is critical.** There is a security strategy that takes a 3-5 year look and involves all departments and senior decision makers. In executing the strategy, a critical element in its success is having the freedom to adjust this strategy after a year. This is important as the threat cannot truly be predicted on the onset of execution, and analytics is the primary enabler of decisions made now and future.
5. **Security in cloud and cellular networks.** An estimated 40% of [our] banking is done in the cloud. Once you understand how to embrace cloud and cellular networks, they key is staying in step with industry and one step ahead of the adversary.

### *Panel III Questions / Open Forum Discussion*

Thomas Sweet opened up the panel for questions and comments from participants, highlights of which included:

1. **What was the first priority with analytics?**
    - Data centric modeling, securing the perimeter.
    - Identify important data (HIPPA, IP data, etc.)
    - Data mapping
    - What and how data impacts banking operations
    - 70% of data quite impactful with little security around it
    - Understanding the data with analytics

2. **Is SCRUM application STIG compliant?**
    - Two different answers.  At the enterprise level, application development should be employing Security as a Service (SaaS),, with authentication, data filtering, and other code modules residing outside the applications. Call services vice hard coding is important.
    - SCRUM is not for security systems.  It is an agile method for software/systems engineering. It requires less documentation, goes against development grain.  If you do use SCRUM for the rapid development of systems with secure features, recommend you at least incorporate security upfront.  Documentation and acquisition policy usually causes hesitation.

3. **Applicability of SDLC with mobile banking?**  If you build security into applications, you can monitor all activity that occurs during a session.  SDLC processes provides solid framework for banking.  Europe is ahead on online banking, but the U.S. is catching up.

4. **Vulnerabilities and Patching – Getting better or worse?**
    - Getting worse in general
    - Those who sell services to fix vulnerabilities might not want vulnerabilities to go away, as they make dollars on selling services.
    - If you ask for timelines of vulnerabilities/patches over last five years, and if the numbers are accelerating and following industry trends, software developers are producing less secure codes as time goes on, and may impact application decisions.
    - However, software developers generally produce 2-3 times the number of errors in their code that commercial off the shelf products.

5. **Is Zero-Day detection a holy grail?**
    - It used to be weeks after a vulnerability announced that exploit occurred. We now see an exploit occurring the same day a vulnerability is announced
    - In some cases, we are seeing an exploitation prior to the announcement of a vulnerability is announced
    - There will always be a defensive reacting to offensive, and are not getting ahead of kill chains.
    - We have a role in enabling this to happen, as 36% of us do not even patch at all.

6. **We need to think more about mission assurance and risk management.** We cannot secure and patch everything.  We need to focus on the most important security dimensions.  We also have to not taking sole actions on doing or not doing security measures if we are part of the enterprise, as we may transfer the risk to another organization (not good) if we do.

*Mr. Michael Lack, DARPA Transformative Applications Program, Director of Research, Invincia Labs*

Mr. Michael Lack provided an overview of the Transformative Applications Program, a secure Android-based mobile device supporting the warfighter. Highlights of his presentation include:

1. **Current State and Goals.** One and a half years ago, sharing information at the tactical edge was difficult. One of DARPA's goals was to break the acquisition model and bring the benefit of mobile applications to the Department of Defense. Another was to get a rich set of capabilities out quickly , using feedback from users to develop more relevant applications.

2. **TransApps Objectives.** DARPA set down the path of creating an adaptive multi-application suite across a broad range of tactical use cases. Other objectives included:
   - Developing a secure platform
   - Maximizing the use of state-of-the-art commercial technology at low cost, e.g., $300.
   - Soliciting and rapidly incorporating direct end-user input

3. **DARPA TransApps Pilot.** DARPA sought to develop the technology, get it out to warfighters via pilots. There are currently 2,000 devices in theater with security patrols putting mission live data into these devices and connecting them to CXI Coalition Classified Networks.

4. **TransApps Application Suite.** The TransApps pilot program is standing up its own applications store, beginning with the user in mind. DARPA sent some developers to be imbedded with the troops, which has led to several applications being developed in theater. **DARPA is fielding a new version of the system every three months.**

5. **DARPA is the first the field a mobile Android device in a tactical environment that can protect and store classified information.**

6. **TransApps Android Security – Starting from the Basics.** DARPA created a threat model for the tactical environment that addressed:
   - Physical Threats – adversary captures handheld device
   - Remote Threats – adversary attacks communications and/or introduces malicious code
   - Insider Threats – curious authorized user weakens defensives

7. **Attacks and Mitigations.** The goal was to lock down the platform to ensure security mitigations aren't bypassed. DARPA theorize potential applications for each class of threat.
   - Physical Attack
     - Mitigations to extracting sensitive data were FIPS 140-2 encryption of all tactical data, and enhanced authentication mitigating brute force attacks
     - Mitigations to access via USB were cryptographic and password based USB mutual authentication, and device driver and kernel hardening

    - Mitigations to tampering with devices were cryptographic based device integrity scans, and device hardening policy
- Remote Attack
    - Mitigations to capturing data in transit and denial of service is tactical radio protection
    - Mitigations to exploiting the remote interface are tactical radios form closed networks, and all other wireless interfaces removed from kernel
    - Mitigations to Trojan Applications is comprehensive application vetting process scans for viruses, vulnerabilities and other security risks
- Insider Attack
    - Mitigations to installing unauthorized applications is cryptographic validation prevents installation of un-vetted applications
    - Mitigation to setting modifications is password protected device administration of sensitive settings
    - Mitigation to enabling wireless radios is wireless interfaces from kernel
    - Mitigation to installing custom ROMs include device integrity scans

8. **Mitigations are directly built into TransApps devices.** DARPA built its own Android version to include a Customized Android OS and Linux Kernel that removed unwanted functionality, augmented built in capabilities, and developed additional capabilities. They also built a security stack that included securing data at rest and transit, hardening the kernel, authentication, application vetting and control, and device integrity checks.
    - Data at Rest protection includes encrypting data stored on devices using FIPS 140-2 approved crypto (AES) and using proven Encsf/FUSE and OpenSSL technologies.
    - Authentication protection includes user authentication such as boot and screen lock passwords coupled with data at rest protections, as well as administrator enforced password complexity and lock screen timeout. It also includes laptop / mobile device mutual authentications.

9. **Applications Testing and Vetting.** DARPA built an Application Testing Portal that includes users, developers, approvers and assessors. The portal includes automated toolsets that enable building applications from source, AV scans, Source Code and Static Analysis, and Dynamic Analysis.

10. **TransApps Certification and Accreditation Status.** OpenSSL v1.0.1 with FIPS canister v2.0 has completed FIPS 140-2 validation for Android 2.2. DARPA has also completed a limited NSA validation of data at rest protections. NSA recommended interim approval for use, and an ATO for Afghanistan provided a month ago. DARPA has also sponsored a STIG for Tactical Android Devices.

*Questions and Answers*

1. **What is the relationship between DARPA and DoD regarding this program?** There is a potential program of record conflict between DoD NetWarrior and DARPA TransApps pilot. There are plans to open up applications store to NetWarrior.

2. **Is there a plan to go wireless with TransApps?** Yes, at the FOUO level.

Mr. Arne Josefsberg provided an overview of his company, and perspectives on transforming information technology. Highlights of his presentation include:

1. **ServiceNow is transforming information technology.** ServiceNow is focused on Service-as-a-Service (SaaS) for Information Technology and developing Cloud Computing Platforms. Typical Information Technology development processes takes a long time, and by the time IT is built and its applications tested, requirements have been reset and is one of the reasons for being in the Cloud.

2. **The imperative for operating in the cloud.** Organizations do not have to, and should not, procure IT systems. Cloud platforms are built for rapid development and customization, and this is the new world order. The new world has two parts:
   - Very rapid development and deployment militates for SaaS / Cloud
     - Requirements changing rapidly, and we cannot afford 12 month projects
     - Implementation needs to be done in 1-2 months
   - Consolidate and streamline tools and processes across the enterprise (hard to do)
   - Transforming Service Management is what it is all about
     - Keeping it simple
     - Producing fast results
     - Ensuring absolute clarity
     - Keeping costs low

3. **ServiceNow focuses on Platforms as a Service**, with service level management, workflow, embedded reporting, ITIL best practices, business applications, and custom applications serving as their baseline.
   - Features as the top level operate on a common data set (it is all about the data) that is shared and integrated into key IT functions. This level is under the control of the CIO, and includes service portfolio, IT cost management, project and portfolio management, and governance.
   - The second layer is about supporting the customer, and includes service catalogs, and incident, problem, change, chat, knowledge, live feed, and release and SDLC applications.
   - The third and bottom layer includes assets and contracts, CMDB, discovery, and run book automation.

4. **Addressing Cloud concerns.** The two concerns mentioned include the reliability of the system (trusting the cloud provider) and security (is my data protected).

5. **IT Transformation Cloud Platform. ServiceNow's cloud platform includes:**
   - IT Management Applications, to include strategy, design, transition, and operations
   - Platform Services, to include content management, email, workflow, social, approvals, notification, search, and analytics

- Core Platform, to include database connectivity, role-based security, user interface, scripting, and forms and list management
- Shared Data, to include tasks, CMDB, and integrations

6. **Cloud security is important, and an enabler.** ServiceNow cloud security is enabled by:
    - Global mirrored data centers
    - Advanced high availability
    - Security architectures at the network, database, application, and data center layers
    - Centralized log management and correlation
    - Application security, to include encryption in transit and at rest
    - Compliance strategy

*Questions and Answers*

1. **Has industry been slow to gravitate and adopt the cloud?**
    - In general, yes. Cloud is cheaper and faster, and Cloud providers generally do better than IT departments in security
    - There is a huge seam in security, though, as the reality of potentially having to explain to one's leadership that something happened in someone else's data centers is definitely emotional.
2. **Are Cloud providers responsible for FISMA compliance?**
    - Cloud providers provide service to customers, and are responsible for 264 controls
    - Cloud providers are constantly audited by customers
    - There are many auditing controls
    - Interesting partnership

# BREAK-OUT SESSIONS

Throughout Cyber Endeavour 2012, participants, panel members, and distinguished guest speakers were asked to identify three to five topics for further open forum discussion, and to identify potential burning issues, potential solutions, and recommendations. Participants selected the following three topics, with each working group (session) having a moderator who provided an executive level overview of their sessions.

1. **Training and Education**
2. **Identification and Protection of Intellectual Property**
3. **Cyber and Information Operations Convergence and Relationships**

## Training and Education

1. **Training and Education topics for open forum discussion** included:
   - Definition between training and education
   - No DoD and Intelligence Community training and education catalog
   - Identify the scope of that training and exercise
     - Training plan for each level and segment
     - Strategic, Acquisition, Operational, Tactical
     - Man, Equip, and Train
   - Acquisition Workforce (training the work force)
2. **Primary takeaway. Where is that catalog that has all the education and training DoD and IC offer? This is important, as all can look to best of breed.**
3. **Training Requirements.** Training requirements were developed and placed into following columns.
   - **Providers – who do we thing provides some form of training?** Intelligence Community, USCYBERCOM, COCOM, NIST, NPS, Academic Organizations (e.g., Carnegie Mellon), IT leaders, National Laboratories, FFRDC, Industry and Forums (e.g., SANS, Global Knowledge, CISCO, Microsoft)
   - **Groups that training is focused on?** Acquisition community, operators and requirement generators, analysts, program managers, program and project sponsors, O5/06 Commanding Officers, Developers, etc.
   - **Subjects?** On the technical side, there is programming, scripting, protocols, operation systems, legal, rules of engagement, warfare, apportionment and proportionality, rapid acquisition, etc.
4. **Differences between training and education?** Training includes training (classroom, virtual, etc.) and certifications and qualifications, continuing education units.
5. **Recommendations**
   - USCYBERCOM J7 should task the education community to analyze and report how to include Cyber into the training infrastructure.
   - Develop a comprehensive Cyber education and training catalog across the DoD and IC.

1. **Identifying and Protecting Intellectual Property topics of open forum discussion** included:
   - What are the authorities
   - Prevention and deterrence
   - Liability
   - How to have an honest conversation
   - Aggregation

2. **Defending IP.** We need to have a concerted effort as to what is important – he who defends everything (IP) defends nothing. Context matters.

3. **Authorities.**
   - There is bleeding across authority lines. Who has the capability and who has the authority?
   - There are some regulatory policies already in place, e.g., ITAR
   - Defense / Federal Acquisition Regulations, some of which have regulatory powers included
   - May not be DoD Intellectual Property yet, but it is concern to the U.S. (forcing FOUO on someone comes with costs)

4. **Prevention and Deterrence.**
   - Speed of escalation a real concern (what if Russia initiated a cyber attack in the U.S.?)
   - Who has the capability, i.e., may not have all the capabilities, so how can you spin that capability up?
   - Cloud/cloud tools may help by concentrating power (threats are in one basket).
   - What are the gaps and mitigation?

5. **Liability.** What is the liability of inaction, and of reactions with and without proper authority?
   - Escalation and liability intertwined
   - During reactions, when you recover data, you are doing so with your own data and potentially someone else's data and platforms may be used against someone else.

6. **Honest Conversation.** There is not a real good platform (yet) that enables the government and community-at-large to say what happened to us, best practices, and lessons learned.

7. **Aggregation.** If you have aggregated these things, what triggers a response? The burning issue is a Digital Pearl Harbor. Has this happened? Need to have an armed response now, and if able to have aggregated, need a more proactive, stronger response.

8. **Theft of Intellectual Property.** Some of the themes discussed included:
   - Identification of IP. Some more important, context matters, cannot protect everything.
   - Authorities. Federal / State government, regulation bodies, ITAR on dual use authorities
   - DFAR – can we force FOUO on material to ensure greater protection?

- Prevention and Deterrence – Red Dawn scenario – how do we identify and distinguish state actors? Go Wolverines! Who has the capability to detect, attribute, and respond? Cloud may help here, and large gaps are here.
- Liability of action, inaction, and reaction. Normal escalation procedures nullified by speed of cyber attacks. What happens when recovering your data you come across toxic data?
- Honest conversation needed at multiple levels, to include communities (DIB, financial, etc.), with impacted victims, large gaps here as well.
- Aggregation. What will trigger a response? IP is not a life but its loss can have national level effects.

## Cyber and Information Operations Convergence and Relationships

1. **Cyber and Information Operations Convergence and Relationships open forum topics** included:
   - How do we tie IO and Cyber Operations together?
     - Recommendation: Spend a day at CE2013 discussing this topic.
   - Communications of that fusion is a gap we all understand
   - Focus more on IO over Cyber

2. **Fusion of the Information.** What are we doing with that information and how are we really communication that to the COCOM? What things and what tools do they need to have to better understand what they have in front of them?

3. **Social Engineering.** Social engineering of that includes tying things such as HUMINT and SIGINT into Cyber, and the speed in which we do not use Cyber to its full capability because of not knowing what one really has in regards to what one can work with in regards to Cyber.

4. **How do we get that to the physical, cognitive, and behavioral sides of Information Operations?** How is it that the IO person, at all levels of the organization, is using information and insight to his advantage to influence the operation? The IO operator, at many times, cannot identify what the problem is and how they relay that back to the Commander to get the issue and/or point across. At the speed (lack of) to which Cyber happens, we are unable to get a quick response to certain events.

5. **Information Operations – first time COCOM things do not fit into that box** that the Commander is used to having, as the boundaries of operations are shifting.

6. **Recommendation.** Propose at CE2013 that we'd like to spend a day focused on the integration and coming together of Cyber and Information Operations, to include TTP, best practices, and issues.

We would like to acknowledge and express our sincerest appreciation to our three gold and one silver corporate sponsor who played a critical role in making Cyber Endeavour 2012 a success, and for keeping our registration fees modest.

1. **Gold Sponsors**

- **L-3** is a top 10 defense contractor specializing in $C^3$ISR systems, aircraft modernization and maintenance, electronic systems and government services. L-3 is focused on solving our customers' toughest security challenges with high-performance computing, cybersecurity, analytics, intelligence, and next-generation IT services and solutions. We develop real-time active defense capabilities for both our own network and customer networks to protect against cyber threats at home and abroad. For more information, visit L-3com.com/STRATIS
- **Endgame Systems** provides Computer Network Operations software and services to meet customers' cyber security needs, including real-time data analysis, visualization, cutting edge vulnerability research, and implant development. Endgame Systems' solutions support a customer's full-scope cyber capabilities, while raising awareness of ongoing operations and emerging threats.
- **Oceus Networks** provides broadband solutions to government and industry that enable delivery of high speed voice, video and data communications. The company provides open, standards-based mobile and fixed infrastructure, as well as an extensive portfolio of public sector-focused solutions to simplify and expedite the deployment of wired and wireless broadband communications solutions. Privately US-owned and operated, Oceus Networks' headquarters are located in Reston, VA, with labs in Reston and Plano, Texas. For more information, visit www.oceusnetworks.com

2. **Silver Sponsor**

- **The Sentar|Athena Joint Venture** brings together two companies recognized for their Cyber/IT expertise and quality of service. This one-of-a-kind team unites Subject Matter Experts with years of experience in key Cyber Assurance and Information Technology efforts. Our team members provide support to a wide range of customers using state-of-the-art technologies and tools and are dedicated to providing valued-added services that improve the overall health and resilience of our customers' operations.