Cyberspace Symposium Proceedings

"Advancing Cyberspace Capabilities to Deliver Integrated Effects"

Qwest Center • Omaha, Nebraska • 7–8 April 2009


CYBERSPACE

Table of Contents

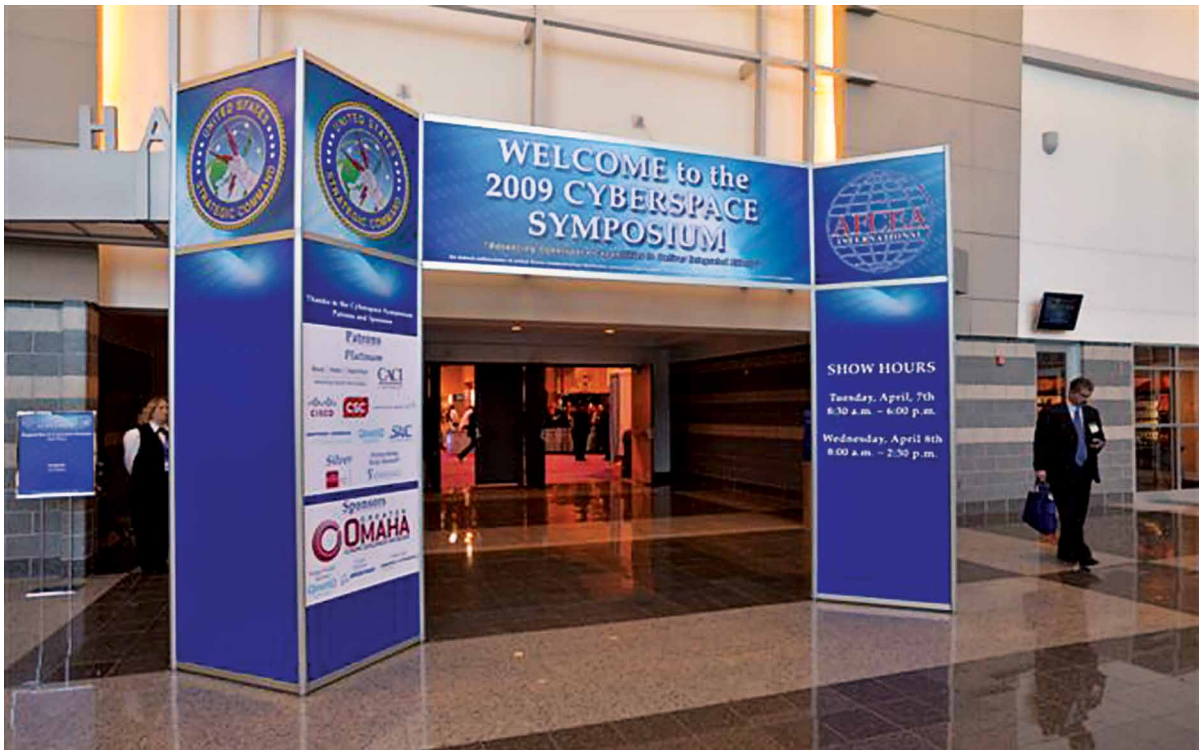
Foreword

General Kevin P. Chilton, Commander, United States Strategic Command, initiated this symposium to provide a forum for US Government, private industry, academia, and international partners to address the advancement of Department of Defense cyberspace capabilities. This inaugural event brought together over 1500 cyberspace practitioners from US and allied government, industry, and academia to share their perspectives on the challenges we face in strengthening the security of the cyber domain. While the multitude of challenges we face cannot be solved in a two-day symposium, our efforts significantly contributed to an increased awareness regarding industry best practices, common threats, and the shared vulnerabilities of the cyber domains.

We would like to thank all of our participants, particularly our keynote speakers, Mr. Scott Charney, LTG Keith Alexander, Lt Gen Harry Raduege, and Mr. Rod Beckstrom for helping to frame discussion during the symposium. Also, we would like to thank our co-sponsor, the Armed Forces Communications and Electronic Association (AFCEA), for their tremendous support in this collaborative effort.

We welcome your comments on this document and look forward to your participation at the 2010 Cyberspace Symposium.

The USSTRATCOM Symposium Team:
Elizabeth Durham-Ruiz, YF-03, DAF
Ron Moranville, YA-02, DAF
Don Harding, YA-02, DAF



Executive Summary

The United States Strategic Command (USSTRATCOM) and Armed Forces Communications Electronics Association International (AFCEA) co-hosted the inaugural 2009 Cyberspace Symposium at the Qwest Center, Omaha, NE on 7–8 April 2009. The event brought together cyberspace leaders and over 1500 cyberspace practitioners from across the U.S. Government, Industry, Academia and the International communities to engage on the theme—"Advancing Cyberspace Capabilities to Deliver Integrated Effects."

General Kevin P. Chilton established the below strategic objectives for the symposium. He kicked off the symposium by providing the audience a USSTRATCOM perspective on the challenges we face and what he considers the top three challenges—culture, conduct and capability.

Symposium Strategic Objectives

- Showcase USSTRATCOM as THE Joint Cyberspace Combatant Command (COCOM)
- Obtain senior leader perspectives (Office of the Secretary of Defense (OSD), Joint Staff, COCOM, Services, United States Government (USG), Industry, International)
- Provide USSTRATCOM a platform to showcase its cyberspace structure and strategic direction
- Provide USG, industry, international partners a platform to discuss cyberspace challenges
- Discuss options to alleviate shortfalls and capability gaps in the cyberspace domain (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities (DOTMLPF))
- Increase intellectual capital in this mission area
- Illustrate industry Best Practices and cutting edge technologies (*e.g.,* global interactive forums)
- Explore "touch points" and common threats/vulnerabilities of all domains (*e.g.,* .com, .gov, .mil)
- Strengthen Joint cyberspace relationships; encourage information exchange and collaboration
- Explore approaches to access/train and develop/retain cyber expertise and leadership
- CC host cyberspace Senior Executive Forum in conjunction with symposium (USG, industry CEOs)

The symposium included dynamic addresses from key senior military and industry leaders, who provided a broad global perspective to the challenges we face and offered an exciting and fulfilling few days for the audience to focus on advancing cyberspace capabilities to deliver integrated effects. The symposium was operations-focused and provided a venue to increase intellectual capital in the cyberspace mission area and set in motion an information exchange among key participants concerned with network challenges. The event offered a rare opportunity to network and share knowledge with other cyberspace colleagues, discuss challenges and solutions in track sessions, and hear firsthand from some of the top U.S. Government, Industry, Academic and International leaders on the challenges we all face and how critical a robust public-private partnership is to addressing these challenges. To address the strategic objectives identified by the Command the following agenda was developed:

Symposium Agenda—Tuesday, April 7, 2009

Time	USSTRATCOM Cyberspace Symposium—Tuesday, April 7, 2009
0700–0745	**Light Refreshments**
0745–0800	**Video Presentation**
0800–0810	**Presentation of Colors—USSTRATCOM Color Guard, National Anthem—USSTRATCOM "Command Performance"**
0810–0825	**Speaker Session One: Opening Remarks** Mr. Kevin Williams, Director, USSTRATCOM Global Innovation & Strategy Center Mr. Kent Schneider, President & CEO, AFCEA International Nebraska Lieutenant Governor Rick Sheehy
0825–0900	**Speaker Session Two: USSTRATCOM Perspective** Gen Kevin P. Chilton, Commander, USSTRATCOM
0900–1030	**Panel Session One: USG Perspective-Shared Situational Awareness** Moderator: ▸ BG John Davis, Deputy Commander, JTF-GNO Panelists: ▸ Steven D. Shirley, Exec Dir, DoD Cyber Crimes Center ▸ James Hass, Dir, Intell Community Incident Response Ctr -Trent Teyema, Dep Dir, Nat Crime Investigative JTF ▸ Sherri Ramsay, Dir, NSA Threat Operations Center -Mischel Kwon, Dir, US CERT
1030–1115	**Exhibit Floor & Networking**
Lunch 1115–1230	**Speaker Session Three: Industry Perspective** 1130–1145: LTG (ret) John Dubia, AFCEA International presents scholarship awards 1145–1150: Intro Mr. Charney, Mr. Kevin Williams, Director, USSTRATCOM Global Innovation & Strategy Center 1150–1220: Speaker: Mr. Scott Charney, VP Trustworthy Computing, Microsoft
1230–1315	**Exhibit Floor & Networking**
1315–1445	**Panel Session Two: COCOM Perspectives** Moderator: ▸ VADM Carl V. Mauney, Deputy Commander, USSTRATCOM Panelists: ▸ VADM Robert Harward, Dep CC, JFCOM -VADM Ann Rondeau, Dep CC, TRANSCOM ▸ VADM Nancy Brown, Joint Staff J6 -RDML Janice M. Hamby, USNORTHCOM J6
1445–1515	**Speaker Session Four: Integration and Synchronization of DoD-IC Cyberspace Operations** LTG Keith Alexander, Director, National Security Agency
1515–1545	**Exhibit Floor & Networking**
1545–1715	**Tracks: Session One** 1. Cyberspace Operations – Mr. Sami Saydjari, Founder/President, Cyber Defense Agency 2. Mitigating the Threat – Ms. Priscilla Guthrie, Director, Info Systems & Tech Div, Inst. For Def. Anal. 3. Cyberspace Deterrence – Brig Gen Susan J. Helms, USSTRATCOM J5
1715–1815	**Exhibit Technology Reception: Qwest Center Exhibit Floor & Networking**
1815–2015	**Omaha Chamber of Commerce hosts "A Taste of Baseball" BBQ buffet networking social: Qwest Center Exhibit Hall Floor Technology Reception: Qwest Center Exhibit Floor & Networking**

Symposium Agenda—Wednesday, April 8, 2009

Time	USSTRATCOM Cyberspace Symposium—Wednesday, April 8, 2009
0700–0745	**Light Refreshments**
0800–0930	**Tracks: Session Two** 1. Cyberspace Operations—Mr. Sami Saydjari, Founder/President, Cyber Defense Agency 2. Mitigating the Threat—Ms. Priscilla Guthrie, Director, Info Systems & Tech Div, Inst. For Def. Anal. 3. Cyberspace Deterrence—Brig Gen Susan J. Helms, USSTRATCOM J5
0930–0945	**Break—Transit**
0945–1115	**Tracks: Session Three** 1. Cyberspace Operations—Mr. Sami Saydjari, Founder/President, Cyber Defense Agency 2. Mitigating the Threat—Ms. Priscilla Guthrie, Director, Info Systems & Tech Div, Inst. For Def. Anal. 3. Cyberspace Deterrence—Brig Gen Susan J. Helms, USSTRATCOM J5
1115–1215	**Exhibit Floor & Networking**
Lunch 1215–1330	**DoD Perspective** Speaker Session Five: Securing Cyberspace for the 44th Presidency 1250–1255: Intro Lt Gen (ret) Raduege (RADM (ret) Stephen Oswald, VP, Boeing Inc.) 1255–1325: Speaker: Lt Gen (ret) Harry Raduege, Deloitte Center for Network Innovation
1330–1415	**Exhibit Floor & Networking**
1415–1545	**Panel Session Three: International Perspectives** Moderator: ▸ Mr. Mark Hall, OSD/NII, DoD-CIO, Chair Panelists: ▸ Australia, Air Commodore Andrew Dowse, Director General, Integrated Capability Development ▸ UK, Air Commodore Bob Judson, Head, Defence Targeting and Information ▸ Canada, Brig Gen John Turnbull, Chief of Military Signals Intelligence
1545–1600	**Break**
1600–1630	**Speaker Session Six: Cyberspace: The Long View** Speaker: Mr. Rod Beckstrom, Independent Cybersecurity Advisor
1630–1645	**Final Words from USSTRATCOM:** MG Abraham Turner, USSTRATCOM Chief of Staff
1830–2030	**CC hosted icebreaker for classified session speakers and Allied attendees:** Upstream Brewery Basement

Key Takeaways

After a brief analysis of the notes, transcripts and objectives, a number of key takeaways were compiled. The four key takeaways from the analysis are as follows:

1. An investment versus cost strategy (Human Capital Strategy) needs to be adopted for the development of cyberspace warriors by doing the following:
   – Institutionalize a process of education, training, certification, enforcement, and inspection
   – Build relationships among Coalition, Combined, Joint, Interagency, Civilian Sector Business and Academia, and Services to build skills, Tactics, Techniques, and Procedures (TTPs), and curriculum
   – Walk the "train as we fight" talk
2. Acquisition policies need to be reformed to evolve authorities, processes and portfolios to get the process done faster and make it more flexible.
3. National and international "legal frameworks" (*e.g.,* Laws of Armed Conflict (LOAC), Status of Forces Agreement (SOFA), Geneva Convention, treaties) need to be changed to accommodate threat response under the condition of uncertain attribution.
   – Attribution and the ability to, as accurately as possible, identify an adversary is extremely important
   – Proportionality (DIME [Diplomacy, Intelligence, Military, and Economics] actions), Rules of Engagement, cyber LOAC, declaratory policy, deterrence versus response to attack
4. Cyberspace culture (values, attitude, beliefs) and architecture need to be shifted as reflected in the table below:

Focus on:	**Deemphasize:**
Deterrence	Response
Payload	Platform
Data	Source
Single universal standard	Several standards
Virtual presence	Physical presence
Weaponization	Administration
New capabilities	Established capabilities
Trust	Doubt
Need to Share	Need to Know

Leaders reached a general consensus that threats to our cyberspace capabilities have a real and potentially devastating impact on our national security. They also acknowledged that there are limits on the efficacy of military force alone in meeting current and future threats. The collective and coordinated strengths of a broad range of government institutions, the private sector, academia, international partners, and the influence of culture are needed to effectively meet the challenges and threats. One critical point made in the symposium was that our networks must be sufficiently robust to allow for effective operations while under a cyber attack. Leaders also considered the issue of response actions by exploring the questions:

- What constitutes a cyber attack?
- How do we attribute attacks, and how do we act when attribution is in doubt?
- How do we measure response actions under the acceptable laws of war?

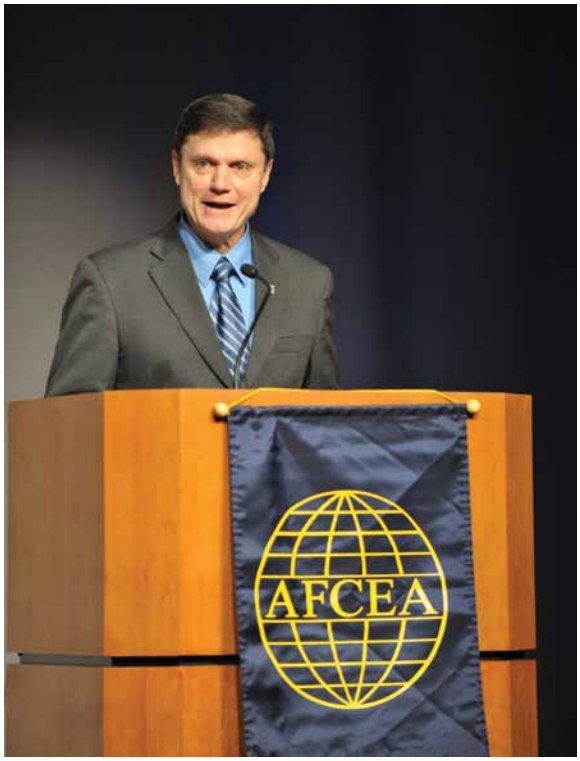
Key Recommendations/Action Items

A comparison of these takeaways with comments and questions during the symposium generated the following key recommendations/action items:

1. Establish national/international cyberspace focused relationships (*e.g.,* government, business, and academia) to embrace a culture of sharing.
   - – Field a scalable national level government, business, and academia common operating picture to which all entities can contribute their problems and solutions.
2. Update laws, guidance and policy as they apply to cyber (*e.g.,* make cyber laws relative to cyber attribution.)
   - – Make policy consistent, declaratory and enforceable (internal and external).
   - – Move to common standards, protocols and policies, all with accountability
3. Explore traditional and non-traditional sources for cyber manpower and expertise such as cyber militia(s) and cyber JASON. (JASON is an independent group of scientists that advises the United States Government on matters of science and technology. For administrative purposes, JASON's activities are run through the MITRE Corporation, a non-profit corporation in McLean, Virginia, which contracts with the Defense Department. The name "JASON" is sometimes explained as an acronym; however, in fact, the name is a reference to Jason, a character from Greek mythology.)
4. Build in security considerations from the ground up to include:
   - – Adopt a narrower profile and limit avenues of approach by moving to next generation capabilities
     - – Internet Protocol version 6–IPv6
     - – Signed code
     - – Thin-client architecture
     - – Address Space Layer Randomization—ASLR
     - – Secure non-IP based comms for critical C2, including Logistics info
     - – Trusted Platform Modules—TPM
   - – Make security a key acquisition consideration: verifiable, trusted sources
   - – Establish a DoD/USG cyber-focused risk/hazard assessment organization
   - – Standardize and automate security requirements and response actions as a force multiplier

Of the 11 strategic objectives set by General Chilton for this inaugural USSTRATCOM Cyberspace Symposium, one was achieved as a result of a Senior Executive Forum hosted by USSTRATCOM in October 2008. The remaining ten objectives were accomplished in the course of the two day symposium and subsequent classified sessions held at the Global Innovation and Strategy Center. This event allowed USSTRATCOM to offer a vision for the community and helped establish its leadership role in addressing the national security threats evolving in the cyberspace domain. The forum clearly helped establish a common understanding of issues and allowed for a wide variety of participants to engage national cyberspace leaders. This initial venue took big strides toward coalescing key issues and discussing those issues with a diverse mix of individuals possessing the knowledge, skill and experience necessary to begin addressing them. Future efforts to include collaboration on the recommendations for future action will provide a framework that will enhance the security of our nations' critical networks, both internal and external to the DoD. These efforts will provide new processes that will project the culture, conduct and capabilities that will be needed to operate at network speed in the ever changing cyber-centric environment.

Symposium Welcoming Remarks



Mr. Kevin E. Williams, SES, DAF
Director, Global Innovation and Strategy Center

Mr. Kevin Williams: Ladies and gentlemen, if I could please have you take your seats.

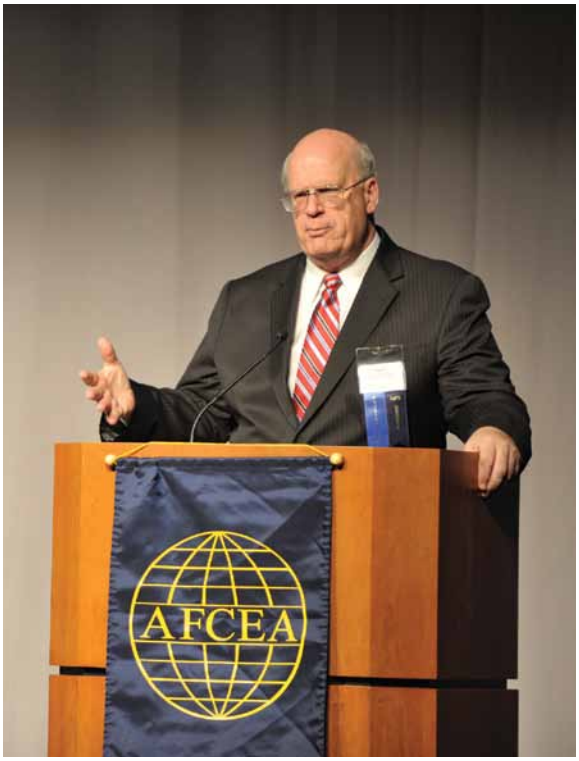
Welcome to the first cyberspace symposium cosponsored by U.S. Strategic Command and AFCEA International.

I'm Kevin Williams of Strategic Command Global Innovation and Strategy Center.

I would like also to thank everyone for taking time out of their busy schedules to come be part of this event. We've got a great agenda lined up over the next two days. Most importantly, we've got nearly 1500 people here composed of a cross section of the government, Department of Defense, the intelligence community, private sector, our allied nations, and academia, all of the way from our most senior leaders to people still attending college right here in Omaha. So it's going to be a great opportunity to do what they call crowd sourcing. We're going to challenge you to get into your track sessions, roll up your sleeves and dive deep into the effort to get us some new knowledge as we go, addressing our theme of advancing cyberspace capabilities to deliver integrated effects.

We're going to try something different here for Q and A sessions. There will be an e-mail address that will be put up on the screen where you can e-mail. If you don't have e-mail capability, you'll see there's a piece of paper at your table, and you can do just a handwritten response, and we will pick those up and send those into the moderator. We also provide feedback. We want to make this better next time. Please fill out the feedback after the sessions and capture your thoughts so we can improve. And just a reminder that we need all cell phones and PDAs on silent. And this is all unclassified, so let's be careful in discussions that we keep it at the unclassified level.

I would now like to turn it over to Mr. Kent Schneider who is president and CEO of the Armed Forces Communications Electronics Association.



Mr. Kent Schneider, President and CEO, AFCEA International

Mr. Kent Schneider: Good morning. I want to join Kevin in welcoming you to this first cyberspace conference. I think it's testimony to the importance to the subject when you look around the room and you see the number of people that have responded to a first-time event. I can tell you we do a lot of events around the world. The first time events are always problematic because people aren't sure exactly what they're here for. And to see this many people—with the mix of people that we have here—certainly says that we all realize how important this is.

Last year AFCEA began a series of events we call Solutions. And we did that at the request of OSD because they wanted a set of interactive sessions focused on current topics of interest.

We took the topics last year from OSD, but this year, starting in about July, we sent out letters to about 250 senior leaders around the world, including all of the combatant commanders.

And we asked them what the priorities were that we should address this year, and it probably would come as no surprise to anybody in this room that the number one topic about two to one over any other topic, was cyber warfare. The second topic, just for your interest and probably wouldn't surprise you either, was inter-agency and coalition information sharing, which, of course, comes right back to the subject that we're here to talk about because the more complex the environment, the more difficult it is to operate effectively.

So on behalf of the 33,000 members of AFCEA, I want to welcome all of you here. I want to thank General Chilton and the staff at STRATCOM who have just been terrific to work with, to help put this together. We look forward to the next couple of days.

I want to echo Kevin's point that we encourage you to not be spectators in this event. We've made it possible for you to send questions and comments in electronically, or you can do it with a piece of paper. But however you do it, we really want you to participate over the next couple of days and not just listen.

And I now have the pleasure to introduce your next speaker: Lieutenant Governor Rick Sheehy of the great State of Nebraska. Please join me in welcoming the Honorable Rick Sheehy.

Welcome to Omaha

Lieutenant Governor Rick Sheehy, State of Nebraska

Lt. Gov. Sheehy: Well, thank you, Kent, General Chilton and other guests. I am very honored to be here this morning for this first inaugural Cyberspace Symposium. We're very proud of the work that is done at Offutt Air Force Base and also at STRATCOM and I don't think we can probably say how honored we are to have them here. But it's great to have all of you here this morning because Nebraska has a lot of exciting things going on right now.

Yesterday morning, if you happened to be watching Good Morning America, you saw Nebraska ranked number one as the happiest state in the country. So, we're moving in the right way. The reasons they gave that we're happy is, number one, we currently are one of a few states that have a positive balance in our cash reserve in our budget. Currently at the state level, we are not having to reduce jobs and cut budgets. We have one of the lowest debt levels of citizens across the country, and also we have one of the lowest housing foreclosure rates. And so main street looked around the country and came up with the matrix of how to measure, and put Nebraska number one. I think Iowa is number two. Colorado, Missouri, some of the mid-western states were there. You know, the states that have the oceans and the mountains and the warmth, they are 48, 49th and 50th. So, we turn the temperature down a little bit for today and tomorrow just so that your minds are keeping sharp about what's going on here in the symposium. You're not having to worry about what's going on outside.

The Qwest is an amazing facility. The technology and the infrastructure that has gone into this building, it has held some world-class events. And I think the cyberspace symposium is also going to be world class.

But, you know, just a few months ago they transformed this area of the Qwest into a portable swimming pool for the Olympic Swim Trials. Just recently, it was also the home of the NCAA volleyball tournament. And so we're very proud of what is happening here in Omaha and also in the Qwest Center.

But, you know, I also want to say thank you to the men and women who are in our military. Here in Nebraska, the Lieutenant Governor serves as the Director of Homeland Security for the State of Nebraska. So I have the opportunity to be engaged and interact with our warriors here in the state and across the country on a very frequent basis. And I just want to say thank you for the sacrifice that you make in serving our country and serving our military, protecting our democracy and our liberty.

And even though today one of my responsibilities is the Presiding Officer over the Nebraska legislature, yesterday I had an opportunity to go through a closing of a chapter of ex-prisoners of war from the Vietnam War. World War II veterans were there and we had a ceremony in Lincoln. And you know, we think about the men and the women who served back in World War II, the Great War, and our other wars and how thankful we are. But then also today, I'm going to be representing the Governor for a pinning, recognizing some soldiers who were injured in Operation Iraqi Freedom. As a citizen, I think we all need to say thank you to the men and women who serve our country and the tremendous job that you do keeping us safe every day.

The world has changed since September 11th, and the other threats to our country, we know that threats continue to be developed by our enemies day-to-day. And so it's important for us to come together here in a symposium with military, government officials, and public entities to develop relationships and to share new ideas and new technologies, because we are now in a new war, and that war is cybersecurity.

And so I hope that you take this opportunity to reach out to everyone here. But also, more importantly, challenge each other because that is how we become better in the jobs that we do.

And so, you know, even at the state level, we are working very hard on cybersecurity—intrusion devices. The National Governor's Association has an association of homeland security advisers responsible to provide information to our Governors.

Just recently we have stood up a Cybersecurity Secure Communication and Information Technology Council, which is a council that I chair, because we are not integrated on cybersecurity and there are so many ways that those that want to get information or those that want to cause problems within our system have the ability to get into those systems. So it's very important that we're going to work at the local, the state, and the federal levels to ensure the safety and security of information. A cyber attack can be just as devastating to the military or to a state government as somebody using some other form of weapon.

So I am very honored to be here today and to say welcome to the State of Nebraska—welcome to Omaha. I know that your agenda in the next two days is very busy, but I think the information, the opportunity that it's going to provide you is going to make our country, our states, much stronger.

So I just want to say thank you for the opportunity to spend some time with you this morning. Hopefully you'll have an opportunity to get out and enjoy our state and the City of Omaha some, but enjoy the rest of your conference.

Chapter 1

Speaker—General Kevin P. Chilton, Commander, U.S. Strategic Command

Opening Remarks—USSTRATCOM Perspective

Speaker: *General Kevin P. Chilton, Commander, U.S. Strategic Command*

It's great having the Lieutenant Governor here. Mr. Schneider, what a great partnership with AFCEA. Thank you for being here. I want to recognize Lieutenant General John Dubia, who's worked so closely with the STRATCOM staff to make this historic first Cyberspace Symposium in Omaha hosted by U.S. Strategic Command and AFCEA a resounding success.

Flag officers from all around the world are here. Military members from every staff of every combatant command, from every service are present here today. We have friends and allies here from around the world that are participating. Great community sponsorship and support from the local community. And of course our industry partners from the great contract community that is so vital to this mission set are also here today, along with our STRATCOM men and women. Thank you all for coming and being a part of this conference today.

These are indeed exciting times at U.S. Strategic Command, and in fact exciting times in U.S. history. Particularly when we start thinking about what's going on in cyberspace.

So what's the origin of this first ever conference here at STRATCOM in Omaha?

When I arrived back in 2007 we started focusing on what was most important day in and day out in the command, and those are, our three lines of operations.

Of those three, certainly a mission set of deterrence is one that we well understand and have been involved in for many years in this command. Although I would point out it's going to be a new game and it is a new game in the 21st Century, obviously, as compared to the Cold War.

Space, we've been working that line of operation for quite a long time as well.

Certainly the least mature of our lines of operations and arguably one of the most important is the line of operation in cyberspace. When you look at what the President of the United States has asked U.S. Strategic Command to do—to direct the operations of the Global Information Grid that support our combatant commands and services all around the world every day, to operate it, to defend it, both in peacetime and at war; to be prepared to plan and when directed conduct offensive operations through this medium for this domain; to synchronize operations between combatant commanders in the regions and across the globe; and to be the principal advocate for the capabilities and needs for the warfighters in this domain—it made perfect sense to bring you all together here in Omaha to help us get our heads around this great mission set that we've been given, this daunting mission set we've been given.

I'll tell you what, we know we don't have all the answers, and often times don't even know what the right questions are to ask. That's why it's so important, if I could echo Mr. Schneider, for you to be a participant in this conference and not just a note taker. I'm going to encourage controversy here. I want to hear both sides of the arguments. And if there are three sides I want to hear the third side as well. I want you to challenge the speakers, challenge the panels, be involved. There's a lot we can learn and there's a lot we must learn.

You've heard Kevin Williams [GISC Director] talk about cyberspace as a domain. That's the way I think about it. In fact I try to break things down pretty simply for myself, just so I can get my head around it. We have the air domain, we have the land domain, we have the maritime domain, we have the space domain, and we have the cyberspace domain. The first three can be pretty much defined by geography or range of operation. The last two are absolutely global in nature. In fact they are agnostic to the artificial lines that we may draw on a map. They cannot care less about the location of continents and oceans. Space and cyberspace are cross-cutting domains, but they're every bit as much like air, land and sea—warfighting domains, domains that we can expect to be challenged in, domains that we

need to depend on to conduct full military operations as well as commerce that supports the economy. They demand freedom of action, each one of those domains, and so does cyberspace.

For the seas, the maritime domain demands freedom of action for commerce and in wartime for logistic resupply and movement of troops and ammunition and equipment forward to far-off theaters.

The global cyberspace domain is how we move information. It's how we move orders. It's how we move thought. We need that to be secure and available to us to freely operate in, both in peacetime and at war.

I'd like to give a little perspective on where I feel like we are in this great venture of taking on the mission set in cyberspace. I'm going to flash back, use my time in the military and set it back in the same period of time or the same length of time back in history.

I've been in the Air Force, commissioned for 33 years now, so I'm going to take us back to 1893 and I'm going to commission 2nd Lieutenant Chilton, graduating from the U.S. Military Academy at West Point where I probably spent a lot of time studying land warfare. I probably spent a lot of time studying lessons learned from the Civil War and increased firepower and the power of defensive positions versus frontal assault. I probably learned a few things about what happened to Custer in 1876 and operations in the west. I probably didn't think or was not educated one iota about the thoughts of how one might use a new domain for warfare called air beyond maybe balloons for artillery spotting.

1893. Why did I pick that year? Because 10 years later, in 1903, the Wright Brothers flew. Suddenly there was a new domain available. It was nascent, but it was there. And 33 years later, after being commissioned 2nd Lieutenant Chilton found himself in 1926. And not only had they added manned flight to that thought in that domain in World War I, he was thinking about how he was going to fight the next fight in that domain and how important it was to protect that domain, and the growing importance of that domain to commerce and freedom and transportation and the development of this country.

In 1976 when I entered the Air Force as a commissioned Air Force officer, I was one year past having turned in my slide rule and buying my first HP-35 handheld calculator for $275. The concept of a laptop or a desktop computer was not taught at the Air Force Academy when I was there. Yet 10 years later, in 1986, when I arrived at NASA someone came in and put this thing on my credenza, moved my files out of the way and moved some books out of the way and set this screen on my credenza and a keyboard and shoved something under my desk and said here is your computer. It was a Wright Brothers moment, if you will, in cyberspace for me.

Now, 33 years later, in 2009, I am dependent on cyberspace. I'm dependent on it in my personal life. This country's dependent on it for commerce and its economy. And warfighters around the world are dependent on it to conduct operations not just in cyberspace, but in every other domain. In thirty-three years this happened. Faster than the revolution of flight.

Just think about it. In 1981 there was this really bright young man named Bill Gates who said you know, I think 640K of memory is about enough for anybody to use. I can't imagine ever needing more than that. Bill Gates, 1981. Talk about change.

In 1991, I remember in NASA we upgraded the space shuttle main computer. We doubled its computing capacity from 128K to 256K. That's the computer we still use today to go to and from orbit in the space shuttle—256K. The pace of change in this domain has been absolutely astounding.

If I could continue on with the airplane metaphor and take us back to World War I, I think there may be some analogies there as well. In the early days of World War I the German aviators would be up and the French aviators would be up on the other side of the line, and really they were kind of looked at as non-combatants. Mostly what they were doing was observing or spying, collecting information from that domain. They were even known on occasion to pass close enough to see each other in cockpits and wave to each other as they went by—a rather gentlemanly approach to this new domain. We were enemies, they said, but we should not forget the civilities.

Now there's a legend told about one fateful day when a German and French pilot passed each other, and the German pilot must have had a bad morning because he shook his fist at the French pilot as he went by, as the Frenchman said in a rather blustery and caddish

way. Well, the next day when the German approached he hurled some sort of missile at the French pilot as he rode by, and the French pilot was so incensed that he dove at the enemy, and I love this part, drew a small flask of port wine from his pocket—and bounced it off the exhaust manifold of his boorish antagonist. I love it. Flying with a bottle of wine.

As the legend goes, that marked the end of courtesy in the air domain and the beginning of hostilities. What followed, though, was a dramatic change in three areas, in my view. There was a change in culture, in the warfighting culture, and how we thought about using this new domain. There was a change in conduct, in rules of engagement, on how we valued and treated this new domain of air. And there was a dramatic and measurable change in the capabilities and the treasure we would invest to develop those capabilities in this domain.

We have moved past the civilities in the cyber domain. U.S. forces and those of our adversaries now rely heavily on their computer networks for command and control, for intelligence, for planning, for communications, for conducting operations. But these architectures are vulnerable. In fact for more than 15 years the U.S. government and DoD networks have come under increasing pressure to attacks and probes from adversaries, as diverse as nation states, to the disgruntled individual or bored teenage hacker. And while we have detected illicit activity on our networks for more than 15 years and employ resources to offer a comprehensive multi-disciplinary approach to protecting our networks, we need to do more.

All of us, all of us—me included—are making it too easy for our adversaries to exploit our networks today. Like the World War I aviators we need a change in our culture, our conduct, and in our capabilities if we're going to advance the state of art and provide the protection and freedom of action we need in this domain.

Let me begin first with culture.

Cyberspace really grew up as a confluence of technologies that evolved in today's globally connected networks. In fact I reflected on my experience at NASA, I remember after they put that computer on my desk I successfully ignored it for about a month. I'd have to dust it on occasion and I would gripe about it being in the way of my in-box on occasion, but inevitably one day I missed a meeting. I asked the person who had organized the meeting, I said why didn't you tell me the meeting was happening? They said well, I sent you an electronic message. I said why didn't you just call me? Why didn't you just holler at me? We shared a desk in the same office. This person had moved on and I had not begun the cultural shift into cyberspace. And in fact what happened then, in my view, is the culture that we developed because of the way cyberspace grew was one of convenience. It wasn't convenient for this person to call me, and they couldn't be interrupted long enough or thought I was too busy to be interrupted as I worked at my desk so they sent me an electronic message. We didn't call them e-mails in those days.

Think about it. When there was a problem with your computer, who did you call?

The smart young technician, the information assurance person that works in your office. Or do you call the J6 or the A6, N6, G6, and say get down here and fix my darn computer—it's not working. And they did. And they do. And they come and fix those machines. And we developed this culture, in my view, that the cyber domain, the computers on our desks are there just for convenience. They are not part of a warfighting domain. But in fact, they are. And they are not just J6 problems. It is Commanders' business.

And this is a cultural shift that we must make. We must think about this domain and the tools in this domain and the readiness of this domain as commanders, as essential to successful operations.

When I was a wing commander of the U-2 [Beale AFB, CA] I reviewed the maintenance statistics on my airplanes every day. Why? Because I couldn't fly them if they weren't maintained properly and if they weren't prepared to operate. We need to review the maintenance statistics and the readiness of our cyber networks—we're commanders and we depend on them—and I challenge anyone to claim they're not—every day. That's a mindset change.

It's not a convenience any more, it's a dependency. We need to recognize that we need this domain and we need these systems to conduct our fight today and tomorrow. We need to recognize that we can fight in this domain just as an air-to-air fighter can

fight in the air domain; and we can fight through this domain and affect other domains just as an airplane can drop a bomb on a land domain and create effects across a domain. And as commanders we must appreciate the vulnerability of this domain, not just its importance. We have to transition from a culture of convenience to a culture of responsibility. We must recognize vulnerability—the vulnerability that one system can create here on the other side of the world, not just locally.

Every Soldier, Sailor, Airman, Marine in the military is on the front line of cyber warfare every day. If you think about the guards who guard your bases, who stand there at the gate and make sure only the right people come in and keep the wrong people out—that's everybody who has a computer on their desk in these domains today. They are part of the front line of defense and in fact they're engaged in cyber operations that matter every day, whether they know it or not.

Changing this culture is absolutely important and it's going to take, I believe, the longest period of time.

Conduct. How do we conduct ourselves?

If you look at every other domain and every other system, one of the first principles, one of the first things we focus on is our people and their training. Correct? Land warfare, sea warfare, air warfare, special operations. We think about the training of our people because we know, tools aside, that's our leverage point in any conflict.

I'm required to train on cyberspace security by my service, by my command, every year. I get a little thing that blinks up on my computer that says you are due for information assurance training, General Chilton. Get it done by this date. Once a year. Once a year! And I get to read and study year-old adversary tactics, techniques and procedures against an adversary who's changing those every day. Perhaps every hour.

We're not training right. We need to adjust that.

Inspections. As the commander of an aircraft wing I expect my higher headquarters to come down and give me an annual operational readiness inspection to make sure I can do the mission I've been given. So what did I pay attention to in the way of that machine? I paid attention to maintenance, logistics, the readiness of my air crews, their ability to fly the mission and do the job and get back.

What didn't I pay attention to? The cyberspace tools that I needed to get them off the ground. Where are all the tech orders now that our people use to maintain our airplanes? Are they on paper any more? Are they on classified networks? No, they're on unclassified networks and they're on laptop computers or handheld devices that are vulnerable. Change the tech orders on your maintenance manuals on the flight line and watch what happens.

Is cyberspace essential to operations today? Should we be inspecting the readiness of every organization that relies on cyberspace to conduct their operations? Should commanders care about that? Should they be graded about that? I believe they should.

When an airplane crashes, when a ship runs aground, if a tank goes off the road and rolls inverted in a ditch, what's one of the very first thing commanders do? They stand up an investigation board, a mishap board, because they want to get to the root cause, they want to fix the root cause. They study that, they take lessons learned, they promulgate it through training, and they make sure the force learns from those mistakes or learns from those tragedies. Then they also go down and find out why it happened and if there was any culpability involved in that.

Do we do that today in cyberspace? Do we have the tools to hold people accountable for not following rules and regulations? We do. We do. It's called the UCMJ. We've got all the authority we need to do that, but we can't get this backwards. We can't hold people accountable if we haven't properly trained and equipped them. We need to do that. Properly train, properly equip, properly educate, conduct mishap investigations when they happen, and then hold people ultimately accountable for their behavior.

There are lots of violations that occur today in cyberspace and on our military networks. It happens today. People think the rules don't apply to them, for whatever reason. Operational necessity is viewed in their minds, laziness, whatever. But I'll tell you what, when we do that there are adversaries out there who are today taking advantage of that misbehavior and that lack of discipline.

Another point on conduct. When we think about how we're going to conduct operations and ensure the defense of the network. This is anathema to many

many folks. It's the concept of centralized command and decentralized control. It's absolutely necessary in my view in this global domain that requires people to be compliant, requires hardware to be upgraded quickly, and requires defensive systems that are going to operate and work properly.

When I asked last year how many SIPRNET and NIPRNET machines were on the DoD network it took over 45 days to get the answer. I'm not sure I got the right answer after 45 days, ladies and gentlemen.

Now if I asked General Casey how many M-16s there were in the Army he could tell me, I'll bet, within 48 hours. I know Chief Schwartz could tell you how many M-9s there are in the Air Force because every one of them is signed in and signed out; there's 100 percent accountability for those weapons, that if we lose control of might be used to hurt somebody within the ballistic range of that weapon. And yet we have computers out there that we don't know the configuration of, we don't know the location of, we don't know who's on them, which if misused can affect operations on the other side of the world, not just in the room you're sitting in. Culture change, conduct change, and the way we address this.

I shouldn't have to ask how many computers are out there. We should know and we have the technology today. We need to deploy it so that we know every day what's on our network, what's plugged in, what its configuration is. Does it have the latest anti-virus injected in it and updated in it? Have the latest orders gone out? How's our training? Et cetera. That should be machine to machine and it should be automated. We can do it. We need to get on with it.

Changes to culture, conduct, capabilities. Our people need better tools out there today, particularly at the command and control level, at the operational level of war, at JTF–GNO, at JFCC NW, our operational component commanders who operate, defend and do the missions in this domain. They need the tools that allow them to better manage the operation of and the defense of this network at network speeds. As long as we're depending on the human element, which we can never forget, but as long as our principal dependence is on the human element and we operate at human speeds we will be outside the turning circle of our adversary.

We need to operate at machine to machine speeds. We need to operate as near to real time as we can in this domain. We need to be able to push software upgrades automatically. AOL does that on my home computer, why can't we? We need to have our computers scanned remotely with the latest anti-virus software. We need the host base security system deployed this year, not five years from now when we can afford it, because we can ill afford not to have these technologies available for us today.

We need common operating pictures, just like commanders in every other domain demand. Today if you look at our common operating picture in cyberspace, as General Pollett's command and control center, you will find places in the United States of America that are black holes. Black holes. Why? Because we don't know what's going on there. And you know what's around those black holes typically? The fences of one of our military installations, because we have put up artificial barriers to keep the centralized command and control authority—the mission assigned by the President to operate and defend, outside our perimeter. They say it's "my network." No, it's not. And a vulnerability in "your network" is a vulnerability to the entire GIG.

This concept of centralized command and control, decentralized execution I believe is absolutely necessary for our operations in this command.

But you know, at the end of the day I believe we ultimately have to be even faster than network speed if we're going to defend this network appropriately. How do you do that? I'm not defying the laws of physics here. You do it by focused high-tech intelligence. You do it by focused high-tech intelligence, focused all-source intelligence, that tries to get you out and anticipate threats before they arrive. You have to be able to anticipate them and when you can preempt those threats and preempt those attacks before they arrive at your base, post, camp or station, or at your laptop on your desk.

Finally, what we need in the capabilities area is more people. More people dedicated and focused in this mission area. The services are great at organizing, training and equipping air, land, sea and space domain forces. We need to move forward in organizing, training and equipping cyber forces to conduct these critical operations for the Department of Defense.

Ladies and gentlemen, today as you heard the Lieutenant Governor say, leaders in government, business and academia have moved from ruminating

about threats in cyberspace to treating them as real and present dangers. We know we must make this transition. We have seen government networks probed in the past, and I firmly believe these intrusions will only continue to increase as we move forward.

The cost has been in the hundreds of millions of dollars. We do a poor job of quantifying it, but they are real dollars and real costs. The cost has been in lost and exploited information that can be used against us in future conflicts to interdict our operations, to inhibit our operations, or put us in a position to be less effective in the other domains as well as in cyberspace.

Our challenge will be to prevent attacks on our networks and cross-domain servers by coming through our networks. Our challenge will be to find ways to interdict attacks when they've been launched. And when they are successful our challenge will be to make the adversary stop the attack.

I think the most difficult challenge that we have today will be the challenge of continuing to operate our networks when we come under attack. Think about any other domain. I think about my training in the Air Force. When we went to Condition 4 at the base for incoming ballistic missiles with chem/bio gear, chem/bio attack potential. Yeah, we got it for the initial explosion, but then we went out into that hostile environment with our MOPP [Mission-Oriented Position Posture] gear on and we fixed airplanes and we loaded airplanes and we got in airplanes, we took off and flew, we conducted operations in a hostile environment. That's what cyberspace is going to be, and the hardest thing is going to be to fight through attacks in the future and ensure that the domain continues to operate in at least an adequate fashion so we can continue operations in every other warfighting domain.

Ladies and gentlemen, this conference I believe provides a unique opportunity for all of us to get at the latest cutting edge ideas from a cross section of cyberspace stakeholders. From the technologists to the warfighters to the operators to the intelligence community to the wire pullers to folks in other domains who don't think much about cyber day in and day out but understand and know in the back of their minds they are dependent on this domain. You all are here today and we have a great opportunity as we move forward for the next couple of days to share ideas and challenge paradigms and look for the problems we need to solve and the potential solutions to solve them as we move forward.

Folks, I want to really particularly thank Mr. Kevin Williams and his [GISC] staff for the great work that they have done in putting this conference together and giving us this opportunity to get together; AFCEA for all the great partnership we have with you; for government, industry and academia partners who are here today, who have taken so much time from their busy schedules, to get us ready and go forward.

We've got an all star lineup of speakers and panelists that are going to entertain you, but hopefully more importantly challenge you, and I look forward to hearing your thoughts and questions over the next couple of days.

We must leave no stone unturned. The mission we have today in the U.S. Strategic Command is focused on DoD networks. But let's not fool ourselves. The threat to America goes beyond that. The threat to cyberspace entities in America that can affect our economy, our industrial base, our power and telecommunications, our banking, our finance systems, the threat is real today. We need to be thinking about how that is going to be protected in the future.

Remember, all of our DoD networks run on the same wires so there's synergy there in thought when we think about how we're going to move forward in both the DoD and the broader Department of Homeland Security effort to secure America against pending threats.

Finally, I particularly want to challenge everybody that's come from out of state, from around the country and indeed around the world, to take home what you've learned, what you will learn here in the next few days; to challenge people back home; share the information, share your ideas. But without you today going home and spreading the word we cannot begin to change our cyber culture, our cyber conduct or our cyber capabilities.

Thanks, ladies and gentlemen. It's great to be with you here this morning.

Chapter 2

Left to right—Ms. Sherri Ramsay, Mr. Steven D. Shirley, Mr. Trent Teyema, Ms. Mischel Kwon, Mr. James Hass, BG John Davis

U.S. Government Perspective—Shared Situational Awareness

Moderator
BG John Davis, Deputy Commander, JTF-GNO

Panelists
1. Mr. Steven D. Shirley, Executive Director, DoD Cyber Crime Center
2. Mr. Trent Teyema, Deputy Director, National Crime Investigative Joint Task Force (NCI JTF)
3. Ms. Sherri Ramsay, Director NSA Threat Operation Center (NTOC)
4. Ms. Mischel Kwon, Director United States Computer Emergency Readiness Team (US-CERT)
5. Mr. James Hass, Director, Intelligence Community Incident Response Center.

Objective
Create a shared situational awareness to focus on both operational and technological initiatives; establishing reporting criteria, consolidating reporting mechanisms, providing impact risk assessments, and represent some of the operational initiatives.

Key Takeaways
- Shared situational awareness is important to provide a common operating picture for leaders to make informed decisions
- There are challenges to shared situational awareness that need to be delicately balanced such as classification of information and sensitive organizational information
- The only way to improve shared situational awareness and indications and warnings to operate at network speed is through proper instrumentation across government

Panel Discussions
BG Davis: I would like to wish everybody a welcome and good morning. And a special thanks to the leadership at both STRATCOM and AFCEA for hosting the symposium and for allowing us the opportunity to come up here and hold a discussion with you this morning.

The world of cyberspace, as General Chilton mentioned, is the latest and newest warfighting domain for the Defense Department. But as he mentioned—beyond the Defense Department—I think we all recognize that the world of cyberspace is all about connections. And those connections present valuable opportunities and they also at the same time represent valuable vulnerabilities and risk that extend across government—across the international community—across the private and commercial sectors.

What we're able to do this morning in terms of the panel is bring together some of the significant cyber security center leaders from across government in order to hold a discussion, primarily oriented around the topic of information sharing and obtaining shared situational awareness, which is a necessary and a difficult job. I would like to introduce our panelists briefly and then I'm going to let them talk briefly about what their organizations do. And then we will use a scenario that has several segments in it in order to provide some context for a discussion to talk about the issues of information sharing and obtaining shared situational awareness across all of our centers.

First of all, from the Department of Homeland Security we have the Director of the US-CERT, Ms. Mischel Kwon.

Representing the Department of Justice, we have the Deputy [Director of] the National Cyber Investigative Joint Task Force, Mr. Trent Teyema.

From the intelligence community we have—from the Intelligence Community Incident Response Center, Mr. James Hass.

And we also have the Director of the NSA CSS, Threat Operations Center, Ms. Sherri Ramsay.

And from the Defense Department, we have the Director of the Defense Cyber Crimes Center, Mr. Steve Shirley.

And then I'll be representing the Joint Task Force Global Network Operations, as I'm the Deputy there.

So with that brief introduction, I'm going to go ahead and let each of our panelists just talk briefly about their centers, and then we'll begin the first segment of the scenario to foster the discussion. And we'll just start with Jim.

Mr. Hass: As John indicated, I'm Director of the IC-IRC. That really is a collateral duty for me. For my day job, I run information assurance for the DNI. That means by de facto, I also get to lead CI5, Cyber Initiative 5, which is connecting the centers. Since my little center is so small I would like to spend maybe a minute talking about CI5, and then I'll wrap up with a little bit about my center.

I'm not big on buzz phrases but connecting the centers is all about eight words and I think General Chilton said most of them this morning—cross domain—shared situational awareness—and network speed. In other words—a COP [Common Operating Picture] at network speed.

I was at a conference last week with General Alexander, and he made the analogy between cyber and missile defense. He wants to get cyber where missile defense is. In other words, we see an inbound missile and we can get the warning out.

I think we're getting close but we're not quite there. I'm happy right now that we've gotten to the point where we have good situational awareness on a missile strike. That may not sound like a big improvement to you all, but before Buckshot Yankee, which really was a very good thing for the connect-the-centers because the five of us talk more and collaborate more than we ever did before. But before Buckshot Yankee, we could have a cyber attack and it may take certain centers, and I'll name mine in particular, hours and days before we get the information out. After Buckshot Yankee, these five centers talk instantaneously, and it literally is a matter of minutes before—when one cyber attack comes out—that it's spread across the community—and that is a tremendous improvement.

CI5 is all about—like General Chilton said—we've got to get a common set of automated collaboration tools at network speed, so that we can get shared situational awareness, and I'm happy to say I think CI5 is going to get us there.

I'm going to talk a tiny bit about the IC-IRC. Its main jobs are to monitor the IC network—report threats—attacks and solutions. And that reporting also includes the other three centers. I actually call it "The Little Engine That Could" or "The Equal Opportunity Sponge".

DIA is our Executive Agent. We're a very small center—handful of folks—and we rely on the DIA Information Assurance Protection Center for our 24 x 7 ops.

Thanks to CI5, we're actually going to 24 x 7. We're getting a full collaboration suite—secure VTC—Tandberg—dynamic file share—instant messaging—which is where the other centers are going. And it's going to make a big difference. We're always going to rely heavily on the big three—NTOC—JTF-GNO—and US-CERT—to do our analysis because we're not going to have that type of analytical cell.

So I want to thank Mischel and Trent and John for the great support they give us and all of the collaborations and communications.

With that I'll turn it over to Mischel.

Ms. Mischel Kwon: So my name is Mischel Kwon and I'm the Director of US-CERT. And at US-CERT, we are charged with the response support and the defense of the .gov or the federal civil executive space. We're also charged with sharing information and collaborating with state and local governments, industry, and our international partners. We're tasked to interact and collaborate with all of these sectors and to disseminate reliable and actionable cyber information to the public as well. So US-CERT has a very vast and large responsibility, and without our partnership with all of the centers and our collaboration efforts, we would not be able to do this mission. So you'll hear a lot today about how we work together and how we collaborate together in order to not just support our own areas, but also the general public.

Mr. Teyema: My name is Trent Teyema. I'm the Deputy Director of the NCI JTF. And kind of where our lane is in the road or our area of the responsibility is cyber network investigations or cyber threat investigations. So where the NCI JTF is—it's actually an alliance of peers—a coalition of members from the intelligence community—law enforcement—and the DoD—by which we bring that situational awareness from domestic and international investigations to add that extra piece to the whole site picture—where you have computer network operations on one end and computer defense on the other end. We're right in the middle—doing those computer network operations—trying to bring fact from investigations to help the decision makers make appropriate decisions so we can respond and take the effort back to the adversary.

Mr. Shirley: Hi, ladies and gentlemen, Steve Shirley. The Defense Cyber Crime Center today is five organizations. A lab that has about 100 people doing forensic exams on intrusions and all of the digital media that support DoD customers, investigative and counter-intelligence, and info assurance requirements. We've got a training academy—trained 1669 people last year—and forensics examination, cyber investigation and incident response—an RDT&E [Research, Development, Test, and Evaluation] elements—an analytic group of about 25 people that sits in the middle of a blog, if you will, of about 20 agencies that are supporting this guy in terms of trying to paint a common operating picture, if you will, of persistent threats so we can cue operators to get out in front of different threats.

But the mission that is perhaps most relevant to this group this morning is partnering—a DepSecDef-directed mission to support the Defense Industrial Base partners—there are 29 of them today—in delivering cyber threat products to those partners so they can better defend their networks based on contributions from NTOC—from the FBI—from the service investigative organizations in their intrusion investigations—and from GNO. And to push those products to industry so they can refer events to us so we can do diagnostics on those events—do consultations—so we can better understand and help them defend their networks. By the way, how many—can I see a show of hands this morning of folks from the Defense Industrial Base? Good crew—29 major organizations today partnered with DoD in that initiative. Thanks so much.

Ms. Ramsay: Under the NSD-42 charter, NSA and NTOC have a responsibility for the defense of U.S. national security systems. As Mischel already stated, the Department of Homeland Security has a similar charge for the U.S. government unclassified systems—with support from FBI, Treasury and others. I think you can think of the NSA role primary as a support role to those organizations that have the direct responsibility for operating and defending the networks of the DoD and the rest of the federal government.

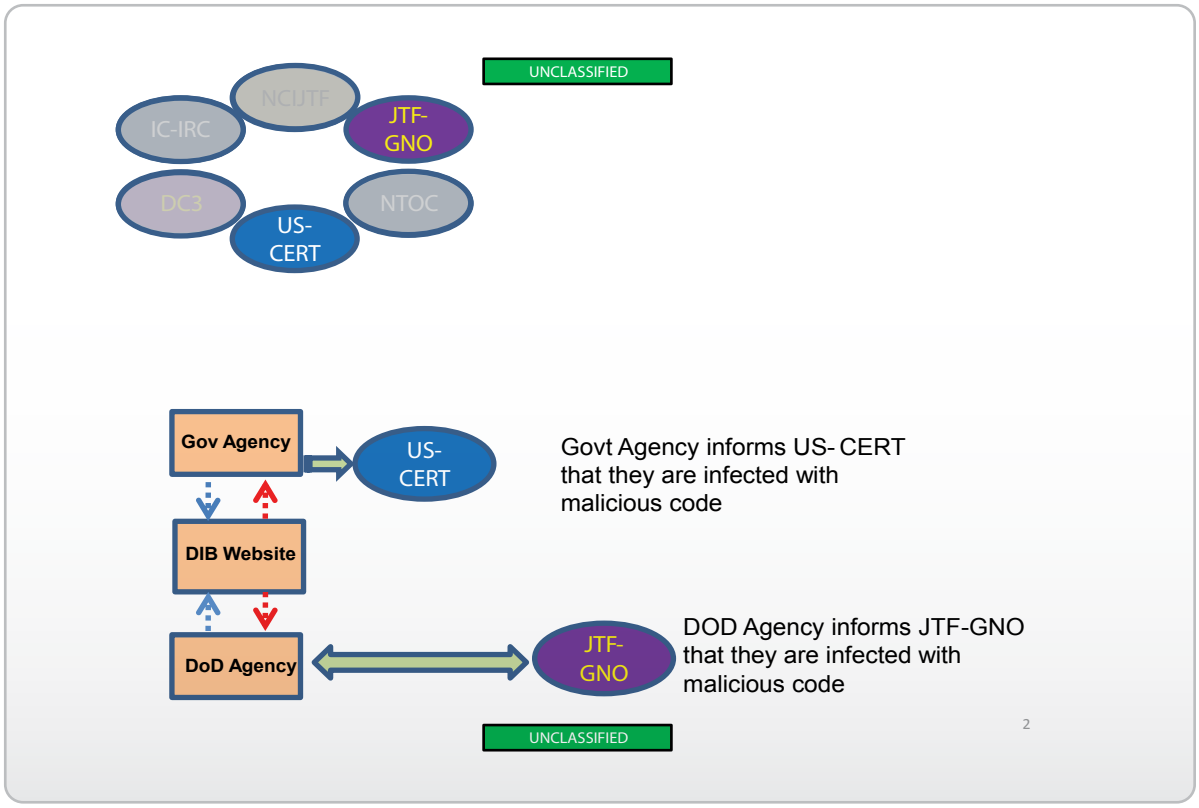
We are responsible for assessing and characterizing threats to U.S. national security systems. We support the detection of those threats and we play a role in enabling automated defense on those DoD networks and we are responsible for providing actionable information to those who have to respond to those threats. We have a lot of information given our IA mission and our signals intelligence mission that we can support to situational awareness and to providing a relevant common operating picture that General Chilton indicated that we so need just a few moments ago. And as such, we also bring a lot of players together. So we're really a venue for mission coordination.

So I think if you think about what NTOC's role is—we characterize the threat—support the situational awareness—and most of all we collaborate with our partners. So we play that support role to JTF-GNO as they own and operate the DoD's networks and as requested and authorized. We play a similar support role to DHS—to the US-CERT—as they operate and defend the .gov networks.

BG Davis: And I'll bring up the rear here in the discussion of Joint Task Force Global Network Operations. GNO is a STRATCOM organization. You heard General Chilton talk about STRATCOM's three main lines of operation—strategic deterrence—space—and cyberspace. Well, probably two of the biggest gears in that cyberspace engine are joint forces—Joint Functional Component Command for Network Warfare and the Joint Task Force Global Network Operations. Our responsibility is to direct the operations and defense of DoD's networks, and we call that the Global Information Grid or the GIG. We are responsible for operating and defending it and, through our command and control mechanisms, for making sure that information is shared internal to the Defense Department by organizations responsible for maintaining situational awareness, and establishing protective mechanisms, mitigating and responding to incidents when they occur and making sure all that is done as effectively as possible so that all of the other warfighting missions can occur.

My boss is Lieutenant General Pollett. He's right in front of me right now. He is the Commander of the Joint Task Force and he is also the Director of DISA. And DISA—the partnership that we have with DISA—in terms of the engineering and provisioning of capabilities across the DoD—is an extremely important interrelationship between those two organizations that gives us the capability to perform our mission. We have about 400 people in the JTF, and I can tell you that's not nearly enough. It is a full-time mission and—I know most of my other friends here are jealous—but it is a growing mission. And with that, I think we'll start.

If we have the slides prepared, what I would like to do is go to the next slide, please. Now what's on these slides is not important, but the discussion is what's important.



And so we'll take the first segment and although we'll try to hold about a 20 minute period at the end of this simply for questions, if you have questions as we walk through this, please feel free to take advantage of the procedure that Kevin [Williams] talked about.

This first slide is just meant to layout a fictitious scenario. And since we have so many Defense Industrial Base partners here in the audience, we thought we'd pique your interest a little bit. But what we're designing this to show is that a U.S. government agency and a Department of Defense agency go to a Defense Industrial Base website—a DIB website—and while searching its website for information about the DIB company, both the .gov agency and the DoD agency get infected by malicious code.

Nothing against the DIB community here, but we're—this is a fictitious scenario to drive the discussion.

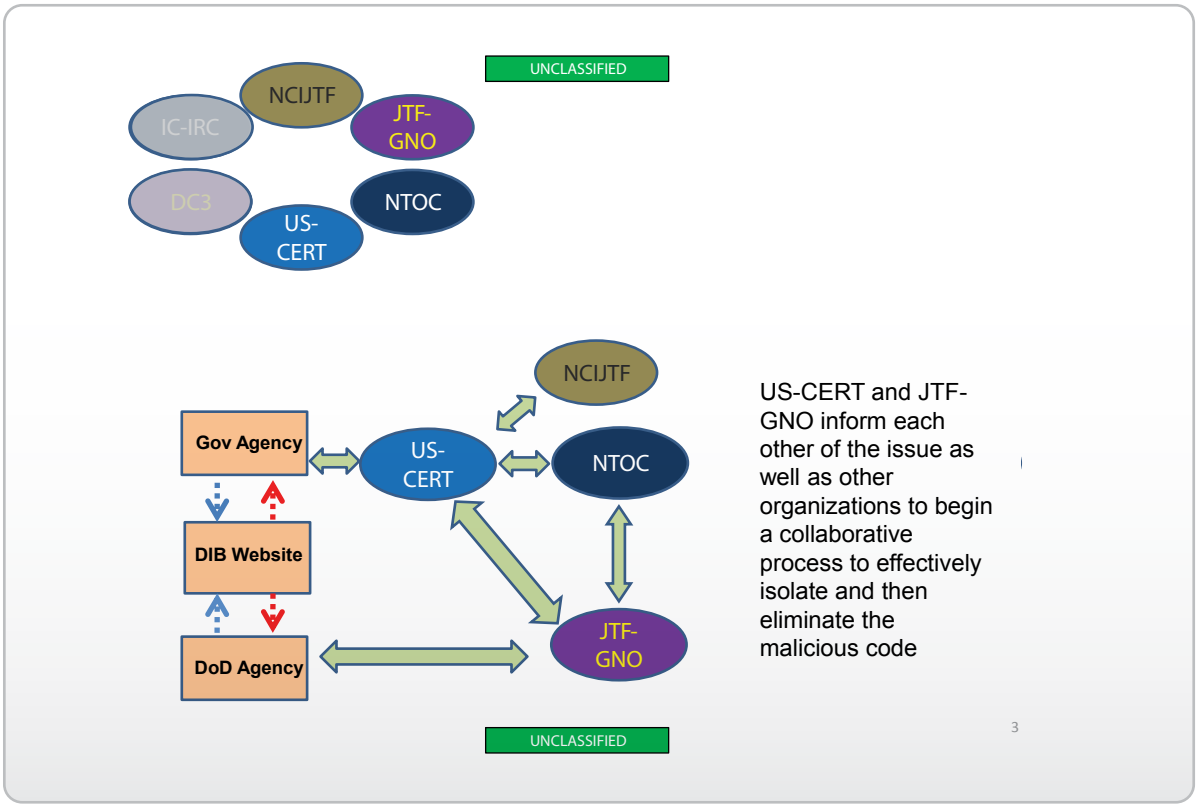
If we can go to the next slide, please. All right.

Now, the system administer for the .gov agency and the DoD agency notify their supervisory chain of command and the .gov reports the incident to the US-CERT while the DoD agency reports the incident to JTF-GNO. So at this point we're going to drive the discussion with Ms. Kwon in terms of discussions of what US-CERT's initial response would be given that initial scenario.

Ms. Kwon: Well, it's important to first qualify a little bit or explain a little bit about the .gov space. The .gov space does not have the luxury of having a GIG. And we at US-CERT do not have the luxury of having operational control of the .gov space. So depending upon which agency calls us will depend upon what immediate response we had.

This is because our networks in the .gov space are what they like to call a federated group. So each agency has control of all of their networks and within an agency each sub-agency may have separate control of their networks. So depending upon which sub-agency actually went to this DIB website would indicate what level of response that sub-agency or agency was capable of providing for themselves.

From the scenario, we said that a system administer initiated the action, which would tell us that this sub-agency did not have a security operation center. So I'm going to play that game today, just to make this a little more easy for us.



And with that, we would work with the agency—the department—to determine how much assistance they needed from US-CERT. At this point we would also reach out to our partners. We would reach out to the JTF-GNO. We would talk to them about the DIB. We would reach out to the NCI JTF—the DC3—and determine who owned the web sites—what was going on with the website—what other agencies might be affected who also use that website. We would also go to our Einstein product and look at where it was deployed and see if we saw any signs of the infection there as well.

We would also reach out to our partners up at the NTOC to see if they had information about the particular malware involved. And we would also look to deploy a fly-away team to the agency, if they did not have the capability to respond to the incident themselves.

BG Davis: Okay. Thanks, Mischel.

Participant at large: How often does that happen? Is that a daily occurrence?

Ms. Kwon: It happens in various different levels and circumstances. So, yes, we have incidents every single day.

BG Davis: You know, we deal with thousands of events every day and the challenge is sorting through all of those events to find the ones that are really important. If I could characterize what would be happening inside JTF-GNO with this—you know, with this scenario—the first question we ask is what happened? We've got to figure out what happened. And it's through analysis and through the partnerships that we have in many different communities—the law enforcement community—the intelligence community—our .gov communities—international partners—there's a lot going on just to answer the question and figure out what happened.

Our next question is probably even more important and that's, what's the operational impact? You heard General Chilton's discussion of this is no longer a convenience that's provided for, at least within DoD. These are capabilities that drive all of our other systems. They are weapons platforms. And so a key question for us—they're never enough resources to go around and solve every problem everywhere—you've got to focus on the ones that are really important.

So making a determination inside of DoD about what the operational impact of this one particular incident—among all the thousands of others that are occurring

on a daily basis—is a really key question that we have to come to grips with because we at GNO are trying to take a global look for STRATCOM at what the impact is going to be across the GIG. And if it's a significant impact, then the next question is what can we do about it? And we need to make sure that we have the capabilities—we have processes, tactics, techniques and procedures, playbooks, *etc*—that allow us to put orders out and take action as rapidly as possible to mitigate what has happened, and to restore capabilities as quickly as we can to increase the confidence in those systems that everybody is relying on—if it's a significant operational impact.

And the last question we ask is who else needs to know about it? And that's where we have mechanisms in the form of intelligence bulletins and activity reports and a whole series of products that are designed to go across a wide variety of organizations to share the information as rapidly as possible. Because if it's significant information, it's really important we're all connected, and even though it may not be something that has a direct impact on the DoD networks, it could very well have an indirect impact on them and we might be able to protect them all day long. But if the services that they ride over are degraded, the availability of those networks might be at risk. So we recognize there are indirect impacts that make it very important for us. It's a responsibility we have—to share this information as rapidly as we can outside of DoD channels. And a lot of these organizations—I have an LNO sitting inside Ms. Kwon's organization and she has one sitting inside of mine—and we have access at the right clearance levels all of the way up to very good information sharing that's done in real time. And it's like that in several other organizations represented up here.

Ms. Kwon: And I think that's an important piece to look at. We have lots of different issues here to look at. It's not just—and not to minimize this at all, it's not just how it's affecting our individual networks. It also has to do with these cyber events are no longer just us, right? These cyber events can affect everyone. We're all riding on the same fabric. And so with US-CERT's mission being so broad, we have to look past just what's going on in the .gov. But if we're also spreading this infection farther and wider to the state and locals—or if the state and locals have spread this infection to us—and we have to look at the problem on a bigger, more global way of looking at things. We need to take care of our networks—we need to clean up what is there—and get back to our mission. But we have to also make sure that globally the infection is also addressed—so spreading it—good information—sharing that information, as far and as wide as we can. As you saw in the conficker incident last week, where it was even on the news—it was in the press—because it's important in certain types of incidents that we clean up. It may not be as important what is actually happening to us, but the fact that malcode is on our machines and we don't have control over it is a problem. It's not one of those CIA—one of those confidentiality, integrity, availability-type things—that we can categorize. But we do need to get the message out that clean up is of the essence and very important to do. And I think last week was a very good collaborative week for us where we all did just that. We shared the information well. We got the information out to the public. We took care of our own networks, and it was a great example of us working together and collaborating together, even though it wasn't an incident that at the moment could cause us great pain.

So it's important to look at these incidents not as just a clean up effort—not as just a hygiene exercise—but also as protecting, not only our nation, but protecting cyber globally.

BG Davis: If I could just put the DIB partners on this, and turn the question to Mr. Shirley.

Mr. Shirley: In February of 07, DC3 was directed to stand up the DIB collaborative information sharing environment and what we began doing there—based on a collection of technical signatures from the NTOC—from GNO—from FBI—from the service investigative agencies—we began building cyber threat products for the Defense Industrial Base and these products were built as a two-piece suite, if you will.

Part A was an unclass set of technical signatures that the partners could use at their discretion to better defend their networks. Part B was a collateral secret description about why we thought Part A mattered—to give the companies the ability to do some risk and resource determinations but also some deeper contextual appreciation.

The quid pro quo there for providing that data was that the partners would agree—under a framework agreement each of them executed with DoD—would agree to provide us notice of events on their networks. So in this event, what we would likely see there is that a department would call and say we've got a piece of malware that we think is propagating across the network. They'd shoot us

a sample of that. It would come into the defense computer forensic lab. We'd begin some malware deconstruction. We'd provide that to GNO—to US-CERT—to NTOC—start characterizing that malware—understand how it rated on a network attack scale and again, give feedback about how we think it's going to operate on your network and start doing some consultation in trying to assess the extent of the damage across that net.

So that began, as I said, in February of '07 with a set originally of 16 partners, now up to 29. And an increasing battle rhythm—if you will—as we work to do this with more fluency and speed in terms of our dialogue back and forth with the partners.

BG Davis: Okay. I could ask the folks in the back to just do one more build on the slide there. As the US-CERT in this fictitious scenario and GNO are collaborating and informing each other about the problem, they also inform other organizations and we've already started that discussion. They can help out in containment and elimination of this one particular threat. I pose a question here to Trent in terms of what's the FBI's role at this point in this scenario and what information or actions would they be able to take in order to help?

Mr. Teyama: Yes, sir. What we would do at the NCI JTF is, based on the information that came to GNO, the DIB and US-CERT, we would then take that to follow up with logical investigations. We would trace it down to the CDC partner that was compromised and work with them closely, along with US-CERT. At the same time, we've gone out to several incidents where we're working the investigation together. I'm doing it from an investigative point of view—computer network defense point of view—and then we're going to try to take it from both the DoD victim and CDC victim and get it outside the defense line and trace it back domestically—leveraging federal authorities to trace where the point of origin is. In many cases, we may obtain more malicious code samples or additional indicators throughout the United States that will point it back to whoever the adversary is. We take that information. We share it back between the six centers so that we can leverage the next logical step, whether it's tracing back overseas or seizing network servers domestically, or going up on those servers to find out what actually is going on.

Really what we end up doing is closing that gap and providing further investigative information or facts so the decision makers can take action. If it's additional code, it goes to DC3, US-CERT, GNO, and NTOC, so we can all protect our networks.

One of the things I wanted to highlight is that the NCI JTF is actually made up of three spheres. We have a national security sphere, a law enforcement sphere, and an analytical group's sphere which is up at Steve Shirley's shop and it's basically those overlapping spheres that we're sharing information back and forth.

And the real return on investment that we're trying to do is the interviews—the victims in the field—the collection of evidence—and then taking that next step to figure out how we can give better visibility on the attack against the network.

BG Davis: Okay. And if I could just pose this to Ms. Ramsay in terms of the NTOC role at this point. How would you be able to collaborate and share in terms of assisting and solving the problem?

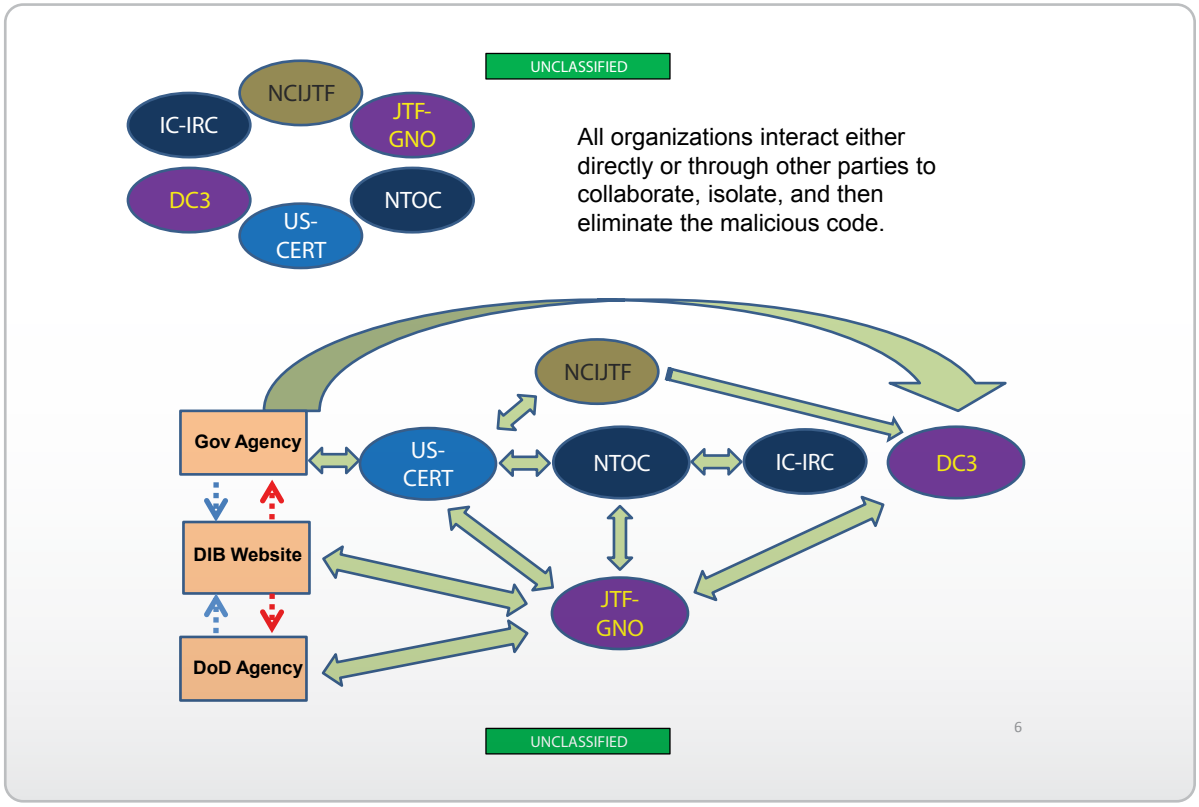
Ms. Ramsay: So NTOC's role at this point is—actually you'll see it will be throughout the scenario—is in a support role to the JTF-GNO and then, as requested and authorized, to the US-CERT and the FBI.

I think we would probably at this point reach out to the both the US-CERT and FBI and ask if they would be submitting a request for technical assistance to NSA to NTOC. That will allow us to lawfully and within our authority support them. We don't have to do that with JTF-GNO because it is within our authorities to help protect and defend those national security systems.

So our analyst would begin discussion. We'll assume RTAs, the request for technical assistance, are all in place. So our analyst would then begin discussions with the analyst across the board of all of the folks that are sitting up here.

And when we get a request like this, we sort of step back and going back to General Chilton's comments this morning, there's really four questions that we would need to be asking ourselves. The first is what's happening in global cyberspace because as we've all indicated, this may be happening at a unique point within the GIG or within the .gov networks. But what we really want is—to take a step back because it's all connected—is to see what's happening in global cyberspace. Is there indication that something is connected here?

Then we would reach out again to JTF-GNO and the US-CERT and try to understand specifically what our



systems are actually detecting because I think that's really important as to what we're seeing.

We then would want to help them look and see how are we postured, given what we're detecting and given what we see happening in global cyberspace. How are we really postured to go from here forward? And then we would start to postulate what can we do about it? What should we do next? What are our courses of action both with the .gov and the .mil networks?

So we would support them throughout as we ask all of these questions with initial response actions. We can support the question of what's happening in global cyberspace. With our signals intelligence mission, we actually can reach out to that and begin to task our collection systems to understand what's happening in foreign cyberspace to see if there's anything that's relevant there.

We also would reach out to our Information Assurance Directorate because of their IA sensors all over the U.S. grid to help understand what's happening there and we would task that as well.

We would then reach out again to our Information Assurance Directorate in terms of how we are postured to support JTF-GNO and US-CERT as they requested to see what vulnerabilities might have allowed this to happen. And I'll stop there for now and speak more as we go through the scenario.

BG Davis: We have a couple of questions that came in by e-mail from the audience. I'm going to go ahead and pose, I think, what might be interesting.

Thousand of events per day. How is it possible to effectively triage all of them for operational impact? Is the triage automated or manual? What is its perceived success rate? I'll take the first stab.

I'll tell you, sorting through thousands of events a day is impossible unless people are doing the basics correctly. In large measure, that's part of the problem. We have found that when we can do the basics right—when folks understand the importance of these networks as warfighting platforms, if you will—and they do the basics correctly—they update their antivirus—they comply with the directives that are established—we find that what we do is we begin to separate the wheat from the chaff, and yes in fact we can focus on the more significant threats that have the most significant operational impact to our ability to operate. But when we can't do the basics correctly, it is a significantly more difficult problem.

The triage process—there are automated capabilities. I think it goes without saying that they need to be improved. There is still very much a subjective leadership assessment that has to be applied to that in terms of what the operational impact is. But I think one of the success stories that I've seen in the past several months is that leaders have gotten much more involved in this particular line of business. And because they are involved in it, they are making decisions now about these things—rather than the typical technical community—not that that's not important, it is—obviously, you want to have your technical expertise involved in this to inform the leaders and give them the—what's feasible and what's not feasible—but you need to have leaders involved in making decisions that have operational impact.

So if we can get the basics down pat and do a much better job of that, I think we can do a much better job of separating out the more significant events that we need to deal with on a broad scale. Anybody else want to add to that?

Ms. Kwon: Well, as we look at moving forward and advancing where we are with the cyber initiative and we look at moving towards reacting in what we call network speed, in order to get to that point, we need to look at this issue in a bigger perspective and look at how we prioritize what we're looking at and how we prioritize the alerts that our systems give us and the incidents that we care the most about.

It's evaluating what the threat is—what attacks those threat actors will be using against us—and what vulnerabilities they then will exploit. If we have the capability to prioritize the threats and prioritize those attacks that those threat actors use, then we can fine tune the tools we use and the people we use to look at the attacks so that we're ensuring that we're addressing the most important. And I think that's absolutely critical. I think it is also important that once we determine what that priority is, that our detection tools are tuned for that, and that we are already working on those mitigation strategies when we prioritize what those threats and attacks are.

In addition, I think we call it in the civil government reflection—the reflection piece of this needs to start earlier. You all call it INFOCON. The changing of information assurance policies, procedures and technologies to make sure this isn't the whack-a-mole that we have been playing with lately.

So in order to structure ourselves and change sooner to do that hygiene—to do that normal upkeep earlier, more in advance—to know that that patch is more of a priority to our organizations and our missions because we have characterized that threat up in the early part before it has hit us—wouldn't it be great to open a master incident before it's affected any of our systems because we know a specific threat actor has a specific attack that would be targeting one of us. It's critical that we start stepping back a bit and looking at responding and securing our systems in a more proactive fashion. And I think the only way to do that is as a team because I think we all hold critical information to that threat analysis. So that's one of the ways of narrowing down the wheat from the chaff.

Mr. Shirley: One of the things that would help is to do the basic blocking and tackling drills a lot smarter than we do today. I tell you why I say that. I've got 20 terabytes of media that's sourced largely from the law enforcement counter intelligence intrusion investigations that affect about 70 different organizations, including a significant number of Defense Industrial Based partners, but also DoD agencies.

And when you look across that body of media from a forensic standpoint, there are a lot of very basic things undone. And I don't mean to say that by way of trivializing, far from it. But we see, for example, cases where a very large network—couple hundred thousand boxes—you've got a box sitting in a DMZ with a year out of date patch—is an initial vector into that network. You've got things that for instance cross a configuration of networks like that 90 gateways. The question then emerges, how do you manage 90 gateways? The answer is not well, whether that's a defense organization or a DIB organization. So if we do the very basic things, we begin to buy ourselves a hedge in some ways so that then we can concentrate on the more esoteric or sophisticated things. But to get those, the basic blocking and tackling sorts of actions done better than we do them today, I think that buys us something. Again saying that—not as directed at the DIB—but as everybody operates networks.

We as Americans seem to kind of hate that repetitive routine kind of operations, but what jumps out at me in this—I was talking to a CTO from a large core technology outfit and I was describing to him what I just told you, and he said—What you've got to understand, that to operate a network, you need to do about 400 very basic things right 24

hours a day, 7 days a week, 365 days a year and then once you get those things right, then there's where you begin to get into the territory where you can do innovation, but that's also where the risk is. And so we tend not to—Shirley's personal opinion—sweat the details oftentimes on the basic blocking and tackling things and we'll leave—metaphorically speaking—the back door open while we're guarding the front door with multiple defenses.

Ms. Ramsay: NTOC is currently working on a capability we call a decision support tool which we have—it's IOC right now—and this tool is to do exactly what we see as the challenge—and that is to take the analysis that's done by a person—at least the first level analysis—automate that—and so then that data can be looked at and when something breaks a threshold, then a tip off can go to a real analyst who can then start to look at the problem. And one of the things that is really important as we begin to use this tool is we'll need to collect data over time, and then go back and look at that data—do the trend analysis—because we have to figure out what thresholds do we need to trip before that alert actually goes to the person. And, of course, this tool—when we get this working—we'll offer it both to GNO, US-CERT, and any of the other users because we want to make sure that we have consistent set of processes—that we do analysis on a consistent set of ways—so we can share and be a cohesive team.

BG Davis: Anybody else? Okay. We have another question.

This one is an interesting question because I'm not sure this is specific to the topic of information sharing or shared situational awareness but it gets to the intent of the conference and as to thinking innovatively and not being held so much to the way things have been. We need to think pretty broadly here about solutions.

Assume that organizational barriers are resolved—accountability structures are defined—and you have at your disposal a well-trained and available staff. With those assumptions in place, what are the top three specific items on your to-do list?

And so while you're all thinking about that, I'll take a stab at it.

General Chilton, I think, started talking about this in his opening comments. The three biggest things for me would be to get ahead of this thing. We spend a lot of our time watching, monitoring, reacting, and it's difficult. That's a tough job in and of itself. But we need to get ahead of it. To really do this well, we need to think ahead of it and getting ahead requires us moving much more rapidly than we have. And I think my three would be this.

General Chilton talked about a focused intelligence collection plan. We spend a lot of our energy and intelligence and analysis figuring out what happened, instead of what's going to happen. And if we can begin to focus—and this is more than the technical side—this takes a variety of sources—but if we can focus on what's going to happen, I think that's one important step in getting ahead.

The second piece to me would be in the Defense Department, we have a defense in-depth strategy. We have many layers of defenses that protect our networks. But we try to keep everything out, and that's almost impossible. And when you have limited resources and assets, from a defense perspective, you really need to focus those where it's most important. So you've got to identify your critical capabilities. I'm not sure we've done as good of job as we need to in identifying what's really critical in order to focus our real energy in protecting around those things that are real critical. I think that will enable us to get ahead and to keep things from getting in in the first place so that we're not reacting.

And then finally I think the third thing would be we also have limited resources and capabilities in our mitigation and response and restoral capabilities. And we need to have procedures in place that allow us to posture those and to adjust the posture as appropriate to the threat and to what we in the Defense Department are getting ready to do. We adjust those postures so that—should we fail in the intelligence collection effort—should we fail in our protective measures against our most critical resources—then the flash-to-bang time with our response to mitigation procedures is reduced to the absolute minimum and we have a much quicker response capability. That would be my wish list for the future.

Anybody else?

Mr. Hass: I think the question was a great question, obviously from DoD because he says if we could get the organizational barriers and authorities solved we could move on to other priorities. Not

speaking for Mischel, but I think the IC and the .gov—that's our two biggest challenges. There are lots of organizational barriers in the IC. I know you guys don't believe that. And the DNI has authority limitations that make it sometimes difficult for us to be directive as the DNI. Assuming though that we can get those two hurdles behind us—which would be fantastic—I've got one priority and that's if the offense could inform the defense.

We've got some agencies out there that have a great offensive capability—we've got some COCOMs that have great offensive capabilities. If we are ever going to get to warning at network speed, offense has to play with the defense. And I would like to see us move down that path so we can get to warning at network speed.

Ms. Ramsay: I think General Chilton covered all three of mine in his talk this morning but let me reiterate—although I'm not sure I'll be nearly as eloquent as you did, Sir. First is we should focus on hardening our networks to make them defendable. This is eminently doable. The tools are out there. It takes a little money and a little wherewithal to just be able do that. In fact I don't think it takes that much money.

The second one which I think is just as important is the automation factor—and that is because speed is really important so we really need to put automated procedures in place so we can inventory—we know what's on our network—what state it's in. We need to be able to automatically deliver patches and more importantly or just as importantly I think is automated policy compliance. Today we actually have no idea. I don't believe the US-CERT or GNO has any way of finding out if our networks are in compliance other than going out and asking and having people self-report. I just don't think that's going to work.

And, thirdly, which I think is just as important as the first two, is really having that relevant common operating picture in a shared operational awareness. Today we operate and defend our networks in sort of enclaves or pockets, but let me tell you our adversary sees the network as one big network. They don't adhere to those boundaries at all so it's really important that we all have a common situational awareness of our networks.

Ms. Kwon: Well, from the .gov perspective, one of my first priorities would be a refresh of technology. I think a lot of the position we're in today is because it's often not funded. And the basis of protecting ourselves—the easiest way to protect ourselves at this point—is to refresh our technology and keep our technology at a state of readiness.

So my second priority would be life cycle management. An appropriate way of consolidating our networks so that they are manageable—so that we can tell what's patched and what's not patched—so that we can deploy updates and keep that newly refreshed technology up to date. Those would be my number one and number two priorities.

And then number three priority would be that prioritization, based on mission, of the threats and attacks so that we are sure that we are not backing into this vulnerability first, but we're looking face forward, threat first. And I think those would be my three top priorities.

Mr. Shirley: Since February of '07, I've talked to probably more industry guys than I have government guys and one of the things that jumps out at me is that we've got lots and lots of technology—we've got lots and lots of smart guys. What may be the toughest thing is, in working with the Defense Industrial Base and indeed government partners, is a culture of trust. And it's the—I think General Chilton mentioned it earlier but—culture is a big deal, and it's harder maybe for us to change that than it is for us to change the hardware. But one of the things with my Defense Industrial Base colleagues want to be sure of is that the government is protecting their equities in terms of their reputation in the marketplace—protecting their intellectual property—and the government is not going to do something to injure their competitiveness against their peers. If I had three things so to say—a trust culture—need to share rather than a need to collaborate—and then that would set up a collaboration as a muscle memory rather than collaboration as sort of an exceptional event. And as a community of interest—DoD—Defense Industrial Base—*etc.*—we're probably in the crawl, walk, run mode in that regard and maybe in a high crawl phase of the crawl, walk, and run continuum.

Mr. Teyama: I think from my lane, it's moving from just the .mil, .gov to also the .coms. The people that are victims out there are also retailers and industries that indirectly support the DoD—that have been targeted by adversaries. It's law firms. It's CEOs. It's the entire social fabric that we have here domestically in the United States. And I guess the first thing would be to bridge that trust or that information from the civilian world and bring it in so we could leverage

that information in the DoD and the intelligence community because there's a whole site picture out there that we may or may not be seeing because the victims are civilian/domestic victims.

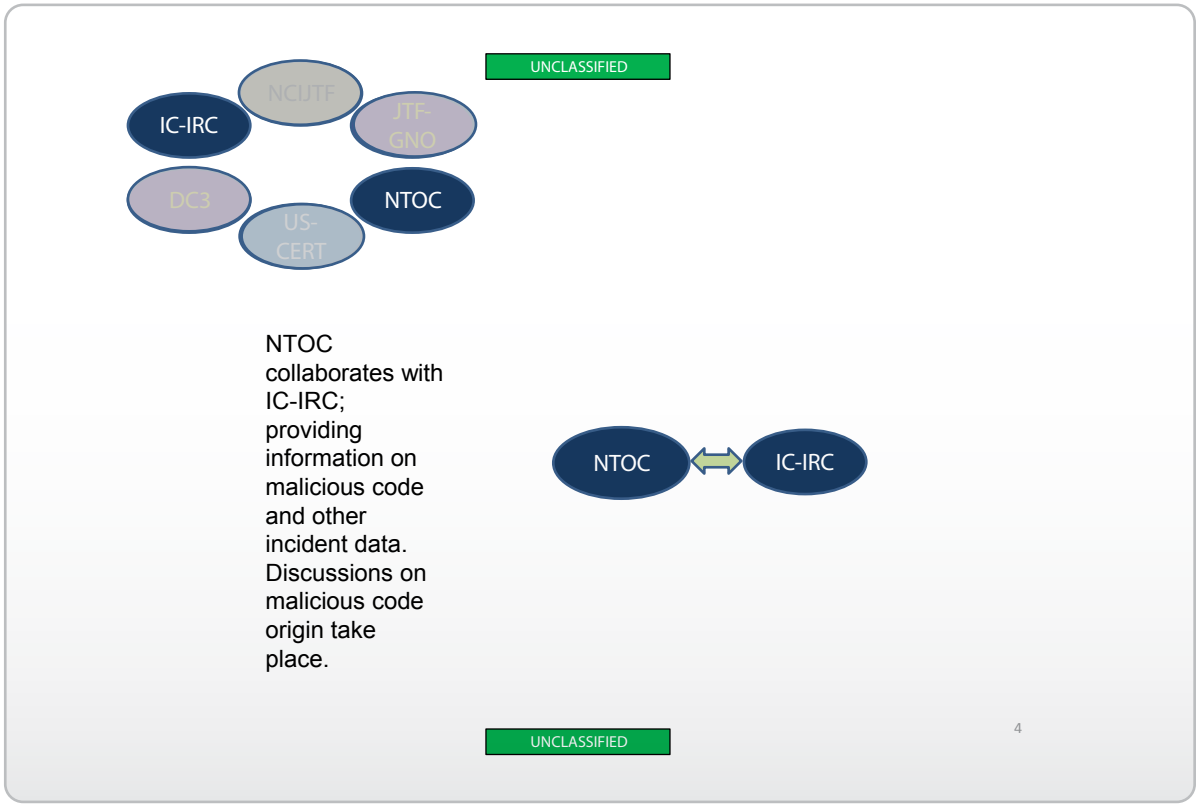
The second thing that I'd really identify, I guess I have two, is transitioning from a reactive mode where we're responding and I can give you the forensics—and I can tell you how a computer was hit—and I can tell you how it came in—and I can tell you what was stolen—and I can tell you what tools were used—but transitioning from that reactive mode to the proactive mode where we're using undercover operations and trying to infiltrate these adversarial organizations to provide that site picture. And then I guess the nirvana would be getting to predictive so that we're in such a position that we can see who is getting attacked before they are. In many cases, we've been that. Over the last year, for example—the NCI JTF has really only been around for over 18 months now—we've moved from the reactive phase up to predictive phase where we could see attacks coming in and being able to leverage against attacks before they actually made entry.

BG Davis: Could we go back to the slide that we had there and advance it one more build.

At this point now the NTOC is collaborating with the IC-IRC and doing the analysis on the malicious code. How would NTOC share this information or results in the collaboration between itself and the IC-IRC? Anything you want to add from what you've already discussed, Jim or Sherri?

Ms. Ramsay: I would just say—actually from a real world example that happened in the fall—what would happen is we actually would physically get together—which we did on Saturdays and Sundays on one interesting weekend back in the fall—and for lots of weekends after that—and actually really collaborate—look specifically at the classified networks—that we would work with the IC-IRC to see what was happening on those networks.

NTOC would partner with our Information Assurance Directorate specifically to do the forensic of the malware—to go out and do the defense of the classified networks. We have a team that does that. We also would partner with the Information Assurance Directorate to perhaps deploy on one of their blue teams that would actually go out and sit down with the system administrators and operators of the networks and look at the configurations.



Mr. Hass: First I want to applaud John Stein for setting this scenario up. It's a great way to impart knowledge and bring out questions but it also shows where we need to get to as far as collaboration of network speed. In reality, the IC IRC probably would have been drawn in on this early by either John or Mischel and the main job of the IC IRC would be to get out to the community that the attack has occurred, and here are the solutions to the attack. As we said before, all of the networks are connected. If folks don't think NSA-net isn't connected to NGA-net which is connected to CWE, they really are.

We had a recent example, there again unclassified, a yet to be named agency had a one-way file transfer that sent up a bad one-way file from the low side all of the way to the high side. That file went out on ICE-mail (Intelligence Community e-mail). We all know where ICE mail goes and we had a mess. So this is actually a case where IC IRC was actually putting out the first corrective notice, that—by the way of John and Mischel, and maybe even Sherri, but Sherri was probably out ahead of us—we had a problem. So the IC IRC job would be in this scenario, to just keep the IC informed. We have a small chance of adding value here since John feeds us—Mischel feeds us—and Sherri feed us. We actually take all of that and do a little bit of all-source analysis and when we puke it out to the IC IRC, and puke it to the other three centers and sometimes we might be an hour or two ahead of the other three centers so you might get to see—here's with a US-CERT says and here's what GNO says,…and maybe we can help a little bit in that way. But mainly, we're in the information flow mode in this scenario.

BG Davis: I've got three questions here. They are all related and so I want to pose this to you while we're talking about this. The first question is—could the panel discuss how they're working the issue of sharing threat and response information with other nations?

The other one is—how do you collaborate with Microsoft, McAfee, Norton and other commercial CND operators? So you've got an international aspects, you've got a commercial/private sector aspect.

And then the third related question—the panel spoke a great deal about communication, information sharing, amongst all of the agencies dealing with this incident. How much of the information sharing is machine to machine? How much is sneaker voice coordination? How long would it take to be aware of the situation and respond? Hours? Days? Weeks? So I think all of those are sort of tied together.

I know from my own perspective, we've had instances in the past where it was very important to get information shared on a very wide basis across international—many different boundaries—and because of the sources and methods issue—which is a real issue—it becomes a challenge in information sharing. And I won't make light of that challenge. It's there for a good reason.

So figuring out a way to balance the need to protect how you got the information to begin with, with the need to share it very broadly in order to respond and admittedly taking response after the fact, but getting something under control is a key challenge that I see that we have, at least from the DoD perspective. Anybody else have any comments?

Ms. Kwon: Well, I think events of last week have showed us that sometimes the answer to this question is, well, it depends.

Last week's incident had no classified aspects to it. And we needed to communicate as widely and broadly as we could. We did coordinate and collaborate with the security vendors, which was absolutely critical, because different vendors had different methods of cleanup that actually conflicted with each other and conflicted with the advice that some of us were giving our users. So that collaboration was very fruitful and is often very important. And that is a part of US-CERT's standard operating procedure—to reach out to the security vendors and collaborate and coordinate with them at the levels in which we can do that.

We also found in last week's incident, in particular, that we usually only collaborate with our partners. And what we found was that we really needed to collaborate with all of the international community so that is one of our lessons learned and continues to be something that we're striving to do with conficker in particular.

But again, you're right. It depends on what classification level—who the threat actor is—what the threat to our agency is. It's an analysis of how far you can actually collaborate with that type of information.

Mr. Shirley: Great question about how do we collaborate with Semantic—Norton—McAfee? Yeah, we do, but what I would ask you guys to think

about—we do a lot of discussion these days about public-private partnerships and how that's going to be good for us if we get it right so I'm looking for the smart guy/gal out there to show me the picture of here's how we do it right—in terms of the contractual issues—in terms of avoiding conflicts of interest—in terms of favoring one of those organizations over one of their competitors—but how we marry those things together so that we do this as a grand team sport that it's got to be to defend against aggressive adversaries.

There are probably a couple of good examples of public-private partnerships that I'm aware of. One we have at DC3 is where we've got a very close relationship with Carnegie Mellon CERT as they support the DIB collaborative information sharing environment. But I hear that question about how do you dance with McAfee or dance with Semantic, and so if there are any of you out there that have some really cool idea, throw a net over me and I would like to talk to you about it.

Mr. Teyema: Well, I can tell you from the FBI's perspective, and I'm actually assigned to the Cyber Division, we've for ten years been developing a long-term relationship with the antivirus vendors and software developers just because of the need to work the investigations.

As to the international investigations, we have a very robust partnership. There are several different outreach methods we do with our immediate allies, but then also, the Department of Justice has something called the 24/7 network where we have a setup around the world so we have a concept of fast-freeze/slow-thaw where a Ministry of Justice can contact the Department of Justice or the FBI and immediately make a phone call to start the wheels moving to preserve information so that we can start acting on it. And then based on sources and methodology, and also the classification of who the victim is and what we're working, we're able to share that very openly. We have over 45 links to embassies around the world and actively promote that sharing of information so we can close the information gap.

Ms. Ramsey: One of the activities that we perform in conjunction with DISA is to put out configuration guidance to the DoD for the products that they deploy on their systems. And so as a result of that activity, we along with DISA have a very robust relationship with a number of those vendors in really trying to understand their products and make sure that we configure it in the most secure way possible. So we have a number of vendor relationships.

I agree with Mischel in terms of the foreign relationships. I'll say it depends. As an intelligence agency and as member of the Department of Defense, we have a number of relationships with foreign partners, both from the signals intelligence side as well as the information assurance side. Of course our closest partners are with those English-speaking nations so we have a fairly broad and robust sharing relationship with them.

But I do agree with Steve. I think this is a brave new world here. I think it's going to take what people have labeled a public-private partnership to protect our nation in the world of cyberspace and I think hopefully what may come out of this week—and what I hope will come out of this week—is a number of ideas in how to really go forward, protecting all of the concerns of the private sector in terms of maintaining their market share and their profits. And also those concerns with the private partnership with us in terms of the civil liberties and protecting those as well, so hopefully we'll have some ideas on that that will come up at the end of the week.

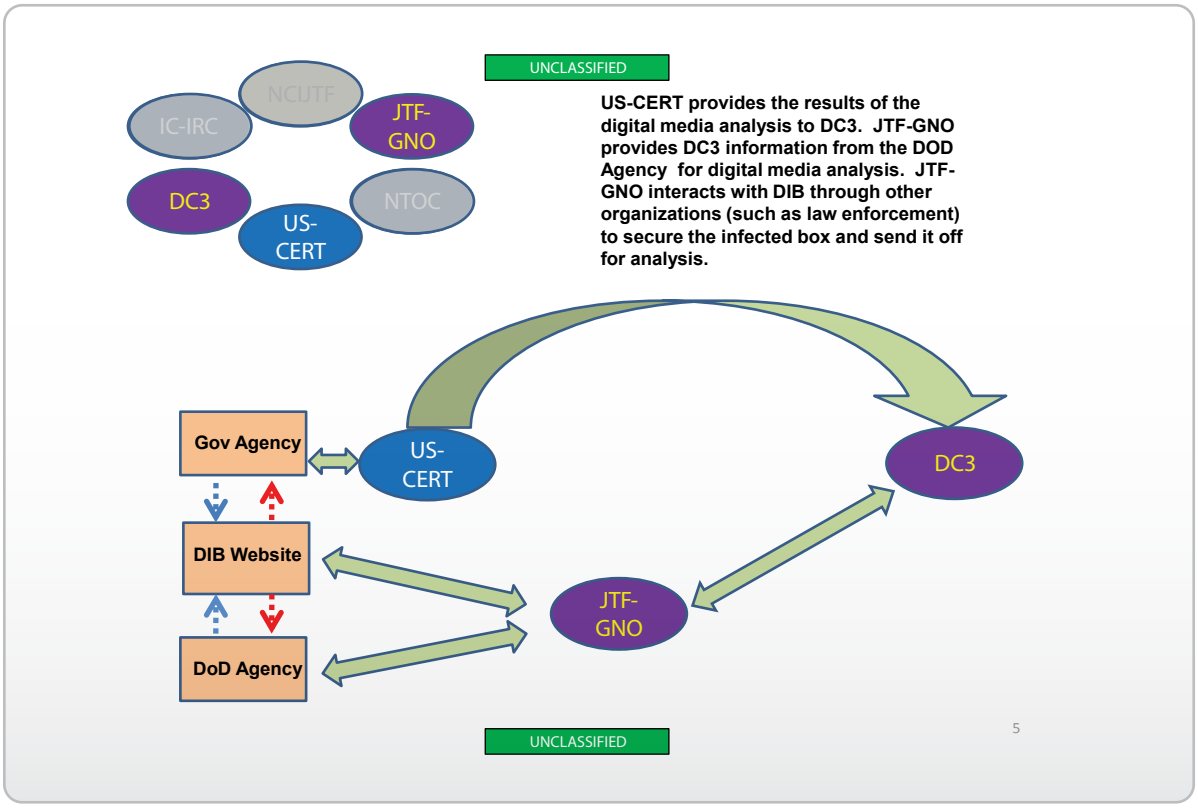
Mr. Hass: I'll just wrap up real quick to answer the other portion of the question—is it sneaker net—is it voice coordination—is it hours, days, weeks? That's what all of CI5 is about—connecting the centers.

Right now it's improved greatly. I can honestly say I think it's a matter of minutes and hours. Most of it is done with e-mail pushes or e-mail notifications to go to websites that have the information. There's a lot of telecons being made.

Eventually we're going to get to these shared collaboration tools that allow instant file sharing—robust file sharing—secure VTC, *etc.* That's where we want to get all of the five centers to. Three of the centers are there now. Once we get that in place, it will go from hours and minutes down to almost instantaneous I hope. That's my dream.

BG Davis: Okay. If we can move back to the scenario—if we could go to the next segment, please.

And here we've got the US-CERT providing the result of the digital media analysis to the DC3—GNO providing DC3 information from the DoD agency for digital media analysis—and us interacting with the DIB through other organizations such as our law enforcement counterintelligence cell to secure the infected box and send it up for analysis. Here's a question, why does US-CERT send information to DC3?



Mr. Shirley: Well, on the other hand it could be DC3 sending it to US-CERT. It would depend. We talked about this and in fact John and I traded hate mail back and forth for a couple days on this.

But we've had in the partnership with the Defense Industrial Base on a number of referrals that—a succession of event notifications but we've had in one case a major referral of media from a source affecting their network. So it could go both ways, could it not?

Ms. Kwon: Absolutely. And I think what's important here is when we do digital media analysis—analysis on any malware—that the information is shared amongst the partners and that we're not continually doing the same analysis on the same malware. Doing some coordinated effort in that regard—and I think that's happening today—I think we're actually doing a good job of that—but also ensuring that the NTOC has that information—JTF-GNO has that information—and security agencies have that information.

In the .gov side of the house, they are just coming up to speed on learning about many of our intrusion sets. And we've developed the joint agency cyber knowledge exchange meeting where we met every two weeks with the security operation centers that exist in the .gov space and we share at that time malware information and the type of analysis we've done—and DC3 has done—and other people across the space have done—so that our security operation centers are aware and alert and know how to respond—know how to detect the type of malware that's targeted at the .gov space. So I think the important thing to say here is that we're doing this analysis and that we are comprehensively sharing.

Mr. Shirley: There's a fairly small community of über geeks who can really when they—in terms of deconstructing malware and trading observations and comparisons on this—so all of these folks in this pretty small community tend to know each other fairly intimately after a while. And my guys know Mischel's guys—who know Sherri's guys—who know their counterparts at GNO and at the NCI JTF. And after we push the org chart off to the side—which sometimes gets in the way—it's those über geeks who know each other and have a very, very focused intellectual challenge in terms of the way that they collaborate amongst each other—is where I think a part of our success lies. If we can enable them with the tools and the pipes—as Jim Hass is working on—that they can talk speed of light to share their observations and technical analysis.

BG Davis: I would characterize the relationship between GNO and DC3—as a connection to the

larger DIB community—as just beginning at this point. And we don't share as much as we should or as we can. We're just now beginning to leverage—and once again this is about resources—having the resources to be able to do all of these things—but we're just at the front end of being able to share that information in terms of awareness reports and intelligence tips—and to leverage a network that our DIB partners can be on at the right classification levels to get this information on a routine basis.

I would just say that even though we're on the front end of providing information through Steve to the DIB community, we are also very interested in information flow the other way. Like I said, there's a lot of indirect impact. It may not be direct impact on DoD systems, but it certainly could be indirect and we're very interested.

And we've mentioned in terms of the question of sharing with international partners and with private sector, the intelligence issues are one issue. There is law enforcement—legal issues—that are other issues that can sometimes prohibit rapid information sharing. There's the operational issue. And I have a feeling that what might be inhibiting information flowing back from the commercial sector back to us in government are the financial issues associated with it. We've got to figure out better solutions to all of these issues. Anybody else?

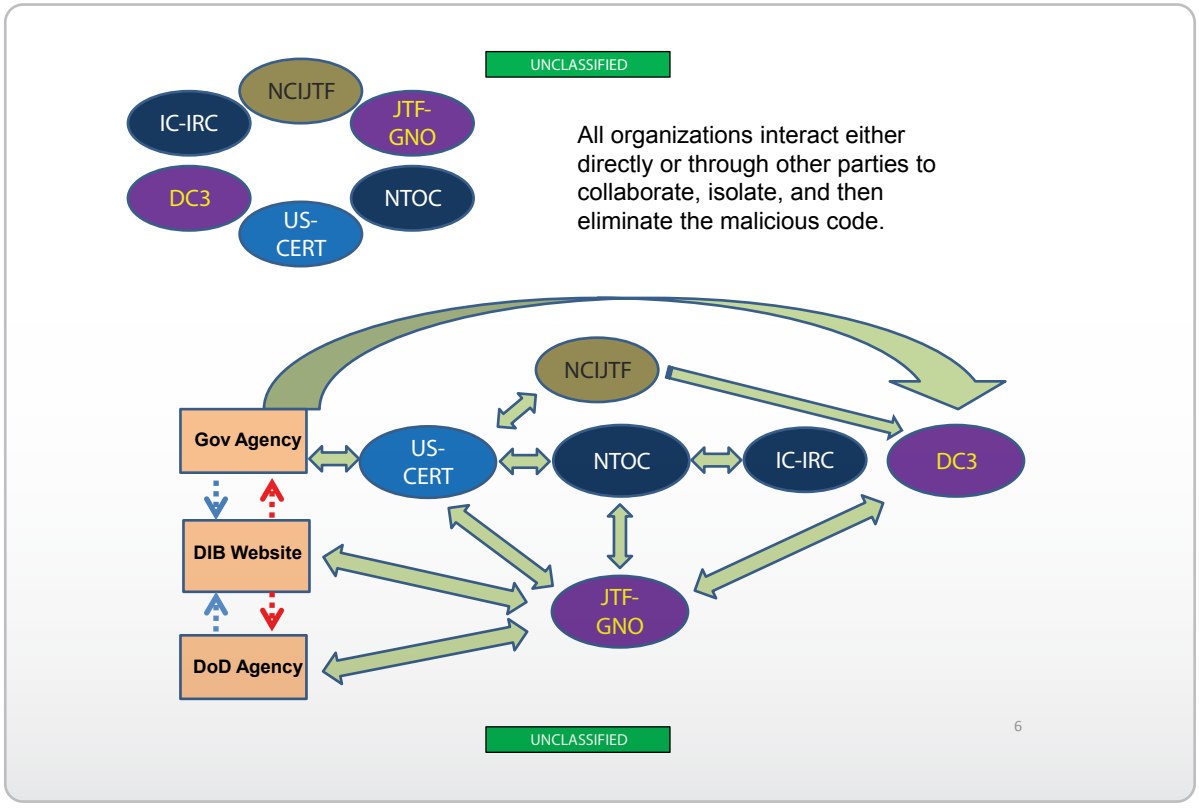
Okay. If we could move to what I think is nearing the end of segment, scenario here.

Basically we have all organizations interacting through the various mechanisms in order to collaborate on this one particular fictitious incident that we've got to isolate and then eliminate the code. And at this point I would open it up to our panel to talk in general terms about challenges that you've had in just general terms of shared situational awareness and maybe even some successes that we haven't brought out yet that you would like to mention. And then when we're finished with that, I would like to have a few more questions that came in here that we'll address and then we'll ask for any final questions. And try to end at about 10:30.

So any challenges or successes?

Mr. Shirley: People, money and time—three principal challenges.

Mr. Teyema: I think one of the things I can identify as a success that we've seen since we've been doing this with the six centers is I've seen the breaking down of the silos of excellence and the sharing of information



connecting the centers that really come down to just cross cultural awareness and appreciating what a computer network defender would need or computer network operations. And an example is where I'm going out and I had a commercial operation where there's a virus or intrusion, and grabbing a copy of the drive pursuant to a search warrant and being able to provide a copy of that back to the computer network defense community so they can start leveraging it or taking the key factors. That has been a significant win from my perspective—is closing that gap on information sharing and sensitizing our agents when we're out in the field that we need to get this information back so we can start locking down the fort.

Ms. Kwon: Well, I can't agree with you more. I categorize it as people, processes and technology, and we definitely need to improve in all of those areas.

But I think the success for US-CERT is we've really turned this vessel around and we're moving in the right direction. We're no longer just a reporting agency, but we are a collaborating agency. We're a defending agency and I think we've become a much better information sharing partner and I hope that only improves. I think this is a team sport and I think the only way we're going to get ahead of this curve is to work together—is to move to network speed and to get ahead of that threat and be able to know who we should be most concerned about.

Mr. Hass: I'll be brief like Steve. I see three challenges—organizational boundaries within the IC—authorities of the DNI to be able to be directive across the IC—and having the offense inform the defense. And as far as success, post Buckshot Yankee, I've seen a quantum increase in collaborations and speed and we'll just keep heading down that path.

Ms. Ramsay: I think one of the successes that we've done is recent and we've mentioned it already and that is many of us have [liaisons] in the other organizations to really facilitate that collaboration and specifically NTOC has a [liaison] from JTF-GNO, from US-CERT, from the FBI, as well as JFCC NW and others and I think that's really facilitated the understanding of each other's mission and the speed with which we can share information.

I think one of the challenges in this brave new world of cyberspace, particularly sitting where we do—where NSA does and the intelligence community—and that is very carefully balancing and doing it well, as well as the perception that we can do it—of really protecting the nation versus privacy and civil liberties and I think that's the challenge all of us are going to face as we continue to try to protect and defend our nation's networks.

BG Davis: We've had a lot of discussion about the challenges. I actually think that there is a lot of good news out there in that we've—especially in the past several months—I think at least from a military perspective—we have leaders engaged today like we've never had before in this arena and we need to take advantage of that in the military because with that attention comes the chance to get on the table when it comes to the resources and the training issues that General Chilton talked about, those things that need to be developed.

There's an opportunity here. I think people are beginning to understand the seriousness of this threat—the fact that it has impact on our operational capabilities—that it's not just a convenience anymore—that it is a warfighting platform in the military—and that it does have a significant impact beyond the military—in our financial markets—our economy—in many other critical functions. I think that's a good starting point and look at this symposium—a great place to discover things like this.

I've got a whole bunch of questions but I've got one interesting and I'll open this up for your consideration—very simple question. In this scenario, who is in charge, or is anyone?

Mr. Shirley: That's a good question. The authorities question.

Ms. Kwon: It depends what space you're talking about.

Mr. Shirley: Well if you're talking about the DIB partner, they are in charge of their network. There's no directive FAR [Federal Acquisition Regulation] policy today that says a Defense Industrial Base partner is obliged to make notice of an event on their unclassified corporate network except as they've agreed to do so under the framework agreement that's currently proscribed.

Now there is discussion out downstream a bit about whether the DFAR [Defense Federal Acquisition Regulation] will be amended to make reporting mandatory on events on unclassified corporate networks that hold DoD content, but that's still out a ways.

But today if you're talking about the Defense Industrial Base—an event on their network—it's their network and it's their risk—and only as it is proscribed in their partnering agreement with us do they make notice of that. So they're in charge of that piece.

Mr. Hass: If you're talking about the IC, here's the standard wording we came up with. "The intelligence community senior information security officer strongly recommends you do X." And to the extent you want to call that in charge, that's about as directive as the DNI gets on fixing the malware.

Ms. Kwon: As far as the .gov space—the state and local space—the industry space is concerned, I would say that US-CERT would lead the effort in collaboration and coordination and that each of those individual entities own their own networks in the .gov space. Each .gov agency or department or agency owns their own network and of course the state and locals own theirs, as do industry.

BG Davis: Well, from the military perspective, with my boss sitting here and his—the boss that he reports under operational control is showing up later today, and all of their bosses sitting at the table—I'll say that within the military, we certainly know who's in charge. The question of command and control is an important issue in the military for all the reasons that General Chilton laid out clearly in his initial discussion about centralized command and control and decentralized execution.

But this is my perspective. In the larger picture, what it reminds me of is my experience in the Special Operations community. And over time we realized that in the problem of finding people in the world—bad people in the world who can hide easily among civilian populations—we found that it takes a network to defeat a network, and that you needed the cooperation—you needed to build the relationships at the lowest possible level among a variety of governmental and non-governmental and indigenous capabilities to find people effectively in the world and arrest or capture or kill them.

Well, in the network world—it seems to me beyond the DoD problem when we look at all of this—we're all connected. We all have recognized an environment where we share risk, and we share vulnerabilities, and it's not a question of who is in charge. It's a question of developing those relationships needed—it takes a network to operate and defend a network in my opinion. So I think that beyond our internal military command and control structures, that's good and that's necessary. But there is more required on a much larger basis and partnerships—networks are what it takes to be effective in that. And I've also found the farther down you go, the more it seems to work just fine. The higher up you go into the organizational architecture, the higher those boundaries become and you begin to argue about authorities and roles.

But anyway, we need to take advantage of what's being built in these partnerships from the ground up and try to facilitate them as best we can because we're all needed in this fight.

Okay. We'll tackle another question. It says please discuss when and how a decision is made to run a counter operation when an exploit is discovered. Given the borderless nature of cyberspace, how are jurisdictional issues addressed? And since we used the word jurisdictional, Trent, I think I'm going to give you the first shot at that.

Mr. Teyema: The decision to do a counter operation—actually that's where I would think on the investigative side—that's where our role would come primarily. So we would leverage the information from the different partners and then immediately what we're going to try to figure out is identify who the person is or people behind that and then try and run a counter operation against that. Either set up an undercover operation—try and set up monitoring—set up whatever we can to find out—give us that further information what we need to trace it back to point of origin.

The one thing about the NCI JTF—let me go back to an investigative point. It's not about cyber investigations, it's actually about people. So the end goal at the end of the day—we're trying to identify direct attribution to the person—to the heartbeat that is launching the attack—and then take it up into his command and control. So, you know, if it's a foreign power, we want to identify which military or intelligence community it is. If it's an organized crime group, we want to identify who those individuals are and be able to leverage against those because that's how you start the pain from our perspective.

And then what it is—it is balance and cooperation—kind of the teamwork depending what AOR you're going into. If it's domestic, you leverage existing civilian and legal authorities. If it's outside the United States, then we're working with our partners—the intelligence community and the DoD—so that we're hopefully perfectly latched up with each other to go after the particular person—persons of interest. And

really that's the idea of what we're trying to do at the NCI JTF—is to take that next step so we can do counter operations—so we can project more force back at them to cause a little pain.

BG Davis: I have a question here and I'll focus this on our friends representing the intelligence community. Why is there not a global warehouse repository of threat actor information—sources, e-mail addresses, identification of threat actor tactics techniques and procedures, and CND computer network defense actionable preventive measures to counter this threat?

Mr. Hass: I'll take first crack. There's another initiative called CI7—increase the security on classified networks. Without going into details in this environment, many of the things mentioned in that question are being looked at by CI7 and there are actions under way to mitigate some of the challenges that are posed in that question. I'll be happy to chat in a secure environment if we can find one afterwards.

Ms. Ramsay: Given that NTOC's job is really to characterize and assess threat information, I'll say we actually do have repositories that have that kind of information in there. However, we can't make those globally available because the information that went in there was often derived from signals intelligence and so there are laws that prohibits us from sharing arbitrarily that information.

We actually have formal reporting vehicles under which we share that information. So there are a number of those. We do threat assessments [that] actually go out to a fairly broad audience including all of my friends on the stage here. We do reports called CIPE reports, C-I-P-E reports, cyber Intel preparation of the environment, which often describes an adversary's network structure. We do formalized SIGINT reporting which goes out to a whole range of SIGINT clients—which actually NTOC's role in that is really foreign threats to U.S. national security systems.

We also do a report called cyber persona profiles. All of that goes out *via* formal reporting mechanisms. One of the purposes behind having the [liaisons] in our organizations are that as [liaisons], they actually—under the specific memorandum agreement that have been approved by our general council's office—they actually can have access to the same information that we do at NSA.

The same is true with the information assurance data. We collect information—threat information—through our information assurance sensors. Those are also stored but also really disseminated under appropriate legal authority. So we're working really hard to make sure the people that need information get it—but certainly within the bounds of the law.

Mr. Shirley: One of the things that we do in building these cyber threat products for industry, as I alluded to, is develop technical signatures from NTOC, GNO, FBI and others and then before we publish those, we submit those back through a deconfliction cycle with each of those contributors to access the Intel gain/loss equation. And it is fair to say that that should always be a dynamic tension. But I will tell you, it's also fair to say we've had some pretty spirited discussions about that in terms of what do we publish to the partners to better defend their network versus what do we retain to exploit from an Intel standpoint. Fair statement? And so I think it should always remain a spirited discussion in that regard. So it's a pretty tough thing. If you had the perfect knowledge about all of those threat vectors and all of that information and threw a blanket over it that would a great thing for one agency to know. But the real power of it is how do you share that with others who need to know that as well—to better defend their networks—and that's where I think the tough discussion will always be.

Mr. Teyema: I think the main way that we share the information that we collect on threat actors and signatures is primarily we push it through the NCI JTF, up at DC3. Also, if it's unclassified information, the primary vehicle we'll push it out through is US-CERT to get it out to the community because they actually have the network in place to get it out to who needs it quickly. We also have outreach programs like InfraGard and our domain program by which we try to share that. But from the FBI's point of view, we're actually going to get it out to the centers that that's their responsibility so they can get it out through their mechanism and provide them that intelligence and investigative information so they can leverage that.

BG Davis: Okay. Obviously we've run out of time. I would just like to thank the panel members for participating today and kind of sharing with the audience some of our challenges and some of our successes. So Sherri, Steve, Trent, Mischel, Jim, thank you very much for being here and sharing today and at this point we'll try to give everybody back about five minutes of their time. So thank you.

End.

Chapter 3

Speaker—Mr. Scott Charney, VP Trustworthy Computing, Microsoft

Industry Perspective

Speaker
Mr. Scott Charney, VP
Trustworthy Computing, Microsoft

Objective
Present industry's cutting edge view of cyberspace challenges and the opportunities to overcome them.

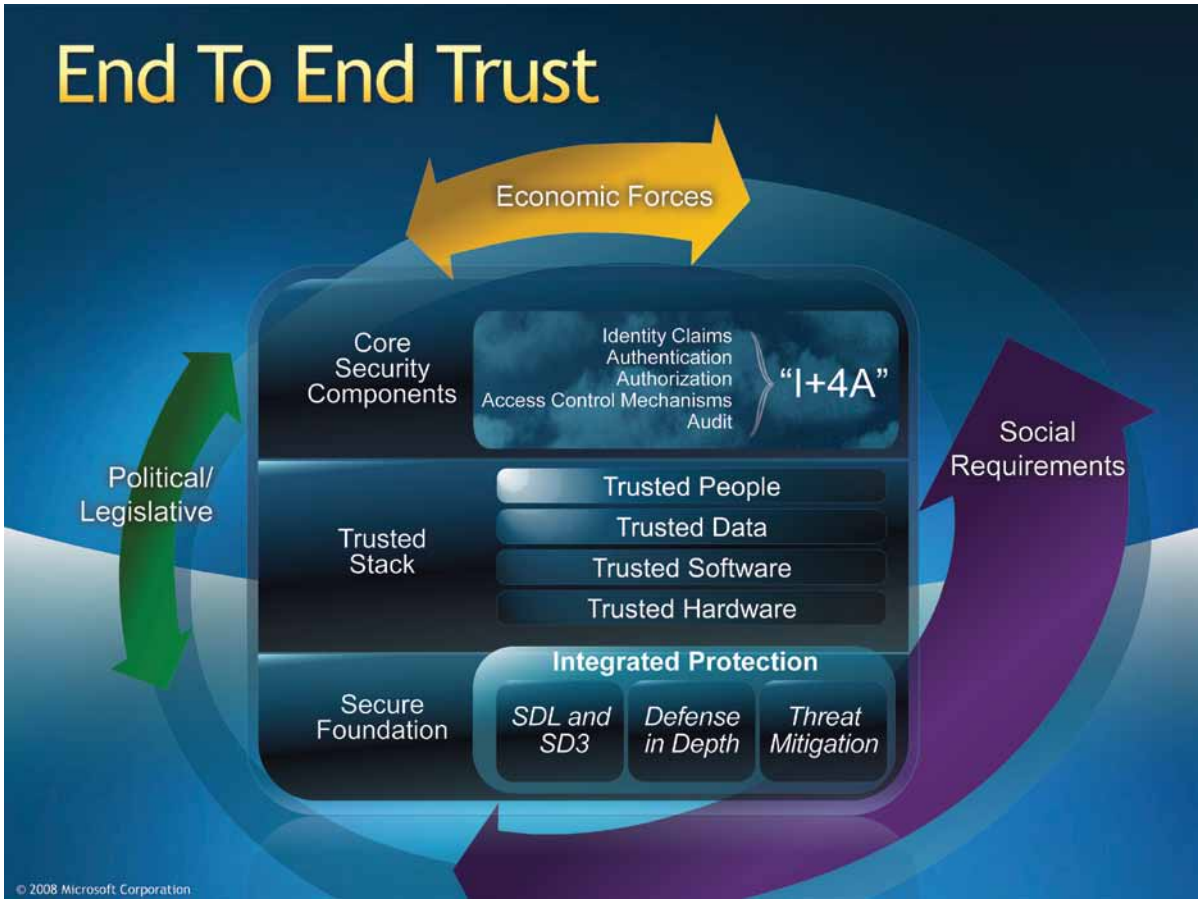
Key Takeaways
- We will always have persistent, dedicated adversaries, to include insider and supply chain integrity threats
- Core principles of trusted systems are trusted hardware, software, data and people
- Long Term Vision to address threat
  - Claims-based identity infrastructure
  - Reliance on Trusted Platform Modules
  - Progress on trusted booting, applications signing, and code injection

Speaker Discussions
Mr Scott Charney: I should tell you very quickly how I ended up on this stage. I spent nine years as the Chief of Computer Crime in Intellectual Property Section of the Department of Justice. And how I got that job is a little bit humorous. I was actually an English and History major. I don't have a technology degree. And like all good English and History majors, when I graduated from college, I figured out that I would never get a job as an English and History major.

So I went to Law School, and after Law School I went to the Bronx County District Attorney's office in Bronx County, New York, where I prosecuted murders, robberies, burglaries and the like. If you know the South Bronx, after five years I was promoted to Deputy Chief of the Investigations Bureau responsible for arson, which was kind of humorous because most of the South Bronx had burned already…and after seven years there I got a call from a former assistant who was with the Organized Crime and Racketeering Section at the Justice Department and she said "How would you like to join the feds?" I said that would be a step up. She was in San Francisco and she said it's not here, it's in our field office in Honolulu, Hawaii. I called home and I told my wife about the offer. By the time I got home, the house was packed. I go out to Hawaii for three years and then I come back and I'm sitting in front of my workstation at main Justice and we had a proprietary operating system made by the Eagle Corporation, Tisoft—no longer around. They had a menu option—D-go to DOS. So I hit D to create some sub-directories—I have a home PC. My boss, Jim Reynolds walks in—hasn't seen a greater-than sign since 4th grade and says—what are you doing? So I said I'm creating sub-directories in DOS. He said, please don't break anything. I said no, I won't.

Now at that time, in 1990, computer crime was handled by the Fraud Section of the Justice Department because the statute was the Computer Fraud and Abuse Act. It was more concerned with people stealing stuff than hacking, and they had one lawyer working cyber crimes. The fraud section had over 140 lawyers, but they had big mega programs—telemarketing fraud—healthcare fraud—defense procurement fraud. And every time they got more lawyers, they put them on one of those mega programs. At that time, the head of the Criminal Division for the Justice Department was Bob Mueller, currently the FBI director. He knew cyber crimes was going to be big and he knew every time he put more resources in the Fraud Section, they would divert those resources to their mega programs. So he called up Jim Reynolds, my boss, and he said you have no mega programs. "Do you think you can do cyber crimes?" He said of course I can. I have a computer expert right down the hall.

So that's how I became the cybercrime guy. Unbeknownst to Jim and Bob, they actually picked the right guy. My father, after coming back from World War II, went to MIT—was a civil engineer—but saw computers as the next big thing, and he became a computer engineer. He worked for Univac in the vacuum tube days. And when I was eight, he had me writing in COBOL [Common Business-Oriented Language] and doing punch cards. And when I went to Microsoft in 2002, people laughed–basically said you're going to Microsoft to do security? How can you use those two words in the same sentence—Microsoft and security. Can we go to the next slide because I'm going to explain what we did.



So what happened was—this was my vision for the future—but I'm going to tell you about the bottom and work our way up to the top, because when I got to Microsoft, we realized we had to take security seriously. The question was, "What does that mean?"

And so the first thing we realized is we had to do the fundamentals right and we developed the SDL and SD3. SDL is the security development lifecycle. Product groups were required to document threat models at design time and code and test to mitigate the threats. We built tools like prefix and prefast to get past the buffer overruns. We put security milestones at every step of the development process. And at the end, when a product group is ready to ship, they have to pass an FSR, final security review. That review is designed to answer a single question. From a security perspective—"Is the product ready to ship?" If the answer is no, we issue a no ship order. What do we mean—a product is ready to ship? It means it has no vulnerabilities, if we have to patch, it would be critical or important. I will say the first couple of times we issued a no ship order, it was like a deer in the headlights. What do you mean we can't ship? We have customers. We have our marketing plan. We have partners ready. We have pent up demand. We have competition. The answer is you can't ship.

And once we laid that line in the sand, product groups started understanding they had to do the security aspect right or they wouldn't be allowed to ship. SDL was a key part of SD3—security by design—secure and deployment—secure and default—secure and deployment. SDL architected for security and improved the coding practices and put security milestones and gates along the way.

Secure by default changed the way we ship products. We used to ship products with every feature turned on so everything you wanted to do just worked. But most people don't use every feature and process, and turning things on broadens your attack surface. So we started turning things off by default. And secure and deployment is about how we kept people

secure even after they deployed the product—configuration guidance—new patching tools—and the like. This was all very productive if you've been watching our products. Generation after generation, the number of vulnerabilities in our product continue to go down.

For those of you paying attention to conficker, for example—if you were running Vista, it wasn't an effective platform because of some of the fundamental work we did; particularly, in defense-in-depth. Recognizing that there's no silver bullet, we started working harder and harder at building protective layers of security. One of the things we developed in Vista was ASLR, address space layer randomization. If you load software in a way that moves it around and when people write malware and they direct their pointers to a memory space, the pointer misses. That's why Vista is not affected by conficker.

But we did a lot of defense-in-depth work. Classic examples are things like—turn on the firewall by default—put in antivirus—put in anti-spyware. And then because we know that users will click okay on any question, no matter what we tell them… we run the malicious software removal tool. When people come to automatic update to get their patches—we actually clean their machines of their infections because we know that not-with-standing the firewall, AV and anti-spyware, they will get infected and we need to clean them.

And then we did specific threat mitigations. Things pop-up like phishing attacks—so we work on a sender ID framework so that bulk mailers have to sign their mail from their source so we can tell when mail is spam. We build better phishing filters and all of that.

From about 2002 when I got there until 2007 or 2008, we were really focused on this bottom secure foundation. It was important work. It was great work. Our vulnerability counts have come down. Our stuff is easier to manage. We talk to customers all of the time.

But preparatory to RSA, the big security conference last year, I started working on what I call end-to-end trust, which is the picture you see in front of me.

How did I end up in this place? Well, we were doing the secure foundation work, but the reality was for all the good work we were doing and the industry was doing, the fact remained the Internet was as dangerous as ever, if not more so. And there were certain very specific reasons for that.

First of all, you have to understand that the Internet is a great place to commit crime. When I was in the Justice Department, I coined the Charney theorem. Here's the theory—I made it up—I named it after myself. Get out your pens—here's the Charney theorem. "There's always a percentage of the population up to no good." That's the entire theory. Okay?

The reason that theory is important here is because, as the Internet went mainstream, you have to assume the criminal population is going to follow. And that's true. But more importantly, the Internet is a great place to commit crime. It is globally connected. It's anonymous—we can argue about how anonymous. It is untraceable, both technically sometimes, and politically because hackers weave through countries and you can't get assistance. And there are a lot of rich targets on the Internet.

If our belief about the Internet is right, global connectivity will continue to grow. There are a billion people online—five billion more to come, right? And more and more people will do more and more things online, which means more rich targets. So if global connectivity and rich targets continue to grow, the only way to solve this crime problem is by focusing on anonymity and lack of traceability. We need a different type of infrastructure.

The fact is most people today do not know what is running on their machines. They don't know where the connections are coming from. They can't tell malware from good software. There are a lot of hard problems. And when I started thinking about that, I said, the secure foundational work is great, but it's just not enough. Look, secure development is wonderful, but we're never going to get vulnerability to zero. Defense in-depth is great, but we know the bad guys will get through the defense in-depth model. Specific threat mitigation is great but it's reactive and the reality is the threat model is changed in some very dramatic ways. It's gone from the early 90s—late 80s—of young hackers exploring network to much more dedicated nation-state and organized attacks.

The attacks are moving up the stack, which poses huge problems compared to the operating system

level. If a few organizations do it right—Microsoft, the community for Linux—if we do it right, all boats in the water rise. But at the application layer, it's not about four or five organizations doing better security. There are millions of ISs, most of whom know nothing about secure coding.

So when you think about the fact that the Internet is going to grow—there will be more rich targets—criminals will gravitate there—there will be vulnerabilities to exploit and mis-configurations to exploit—sophisticated social engineering—you start realizing that secure foundations are just not enough.

And so I started thinking about what next—and what next became the trusted stack, and the components on top. The trusted stack needs to be defined a little bit. Let me explain what I mean by trust. Trust is not binary. You can never completely trust things in the context of looking at this slide and you may not be absolutely safe. Just think about the physical world. Trust is never absolute. There are people I trust a little. There are people who I trust a lot. There are people I used to trust, but I don't trust them anymore.

There are machines that I might trust because they are patched, but after patch Tuesday, if they haven't deployed those patches, I don't trust them anymore. It may be about my risk. I will trust the merchant I do not know with my credit card because if the product is no good I can get my money back. Since I have very low risk, I'm willing to take big chances.

When I talk about a trusted stack, I mean that it's reasonably trustworthy for the purposes for which you're using it. So for people sending mail, they have a certain level of trust. For a classified system, you have a different level of required assurance. Within that context, here are some of the core principles.

One is we have to start rooting trust in the hardware. Software is just too malleable. With TPMs [Trusted Platform Modules], this becomes possible. And, of course, in some of our newer products, we have things like Bitlocker that do full volume encryption, reliant upon the TPM. Ultimately we need to think about more TPM-like functions to root trust in the hardware.

The second thing you need is trusted software. You need to know that the software you're running is genuine and not tainted, and you need to know the source of the software. This is actually quite challenging.

In my view, we need to get to a place where all code is signed and where you can also block unsigned code from running through code injection, which is a hard technical problem.

But even assuming all code is signed, code will live in three buckets—signed by someone you trust—an Abode—an Oracle–for your kid's Disney—whatever. It will be signed by someone you do not trust—known spyware—which you will block. And in some cases it will be signed by Joe's software and who is Joe?

In that area, we need reputational platforms, which are very challenging in this space. Although eBay does a great job with reputations of buyers and sellers, security reputation is much more problematic. Very often I go to a site, and it says, 2 million people have downloaded this gadget. That's popularity, not a security evaluation.

That popularity is in a way a proxy for reliability. If that gadget blue-screened machines, word will get around—people would stop downloading. But it might work really well and have a key stroke logger and there's no evidence in the reputational space that anyone has reviewed it for security.

While that's a broad problem, it doesn't disturb me all that much because most consumers, in fact, run software from very known sources. They run commercial products from Apple—Microsoft—whatever. And in the managed environment, most of the companies and organizations know most of their vendors. And if you block everything else by default, you end up in a more secure state.

We need trusted data. By that I mean the source of the data is known, not that you trust the underlying data. The reason for that is some of the more sophisticated attacks we've seen in the last 12 months involve attachments that are infected in very sophisticated ways and the source isn't clear.

And then you need trusted people. You need to know who is connecting to your network. In a perfect world, based on TPM-to-TPM authentication, you know what machines are touching you, and because of trusted people, you'll know what people are touching your network.

Now, I'm going to talk more about trusted people because if you note the top of the stack, "I + 4A" is all about identity and people.

The reason is the minute you start talking about trusted people, you start talking about identity. And once you start talking about identity, you start talking about national identifiers—privacy implications—chilling free speech—and the like.

So I want to spend a moment talking about how I think about identity now, because I've morphed a lot in the last two years in a lot of conversations with security experts, privacy experts, and civil libertarians.

I want to tell you a personal story that made clear to me that all identity, at its root, is based on social custom and derivative identity.

First, let's look at the Internet today. Here's the way we do identity on the Internet. You go to a site. The site says, "Prove who you are." Give us your name, social security number, date of birth and mother's maiden name. These are shared secrets.

Of course they are not secret at all, but let's pretend for a minute that they are. So you enter that data. The other side verifies it with a third party—a credit bureau—and says okay, you had this secret data—you must be who you claim to be. Here is that certificate and now you are authenticated. Because that secret—those secrets aren't secret at all, the model is hopelessly flawed. So I started thinking about how we do identity in the physical world. Social custom plus derivative.

Here's what happened three and a half years ago. My wife and I had a son. Now, to be clear, at the time we didn't know it was going to be a son. We didn't know what sex it was going to be. And so we picked out a name for the boy and a name for a girl. And my wife told me we have one name for each but when the baby comes out, I might look at it and say no, that name is wrong and I'll rename it on the spot.

She did most of the work. I was okay with this.

So out comes the baby, and it's a boy. And I look at my wife and she goes, name's good. So the doctor says "what's the name?"—I say Dylan—they put this on a birth certificate.

Our social custom is to name the child right away. That's not true everywhere but we named Dylan and gave him a birth certificate. When we took him to pre-school, they said who is this boy? We said he's Dylan. How do you know? We're his parents and here's his birth certificate.

At some point he's going to go to the DMV…over my dead body…and ask to drive. At that point, the DMV is going to say, who is this boy? He's gonna say I'm Dylan and I want to drive and they'll say where's your birth certificate? He'll give them the birth certificate and they will give him a driver's license. Some day he'll want to go overseas. He'll go to the post office to get a passport. They're much more rigorous—they require two forms of ID—birth certificate and driver's license—which, by the way, is based on the birth certificate which was given at the hospital when we attested to who he was.

At some point, knock on wood, he gets a job. His employer says we are going to give you an employer ID. Where are you going to get that ID? You're going to go to this building and show them your driver's license. He'll hopefully make money and go to a bank. They'll say we want you to have a bank card. It'll have your picture on the back. But we can't give it to you unless we see your birth certificate and your driver's license.

All identity is derivative from social custom. But we don't do that on the Internet. And that's actually what we have to do.

And what happens is we replace shared secrets with real secrets—digital certificates. Based on in-person proofing and the issuance, probably by a government, because government IDs have more weight than private IDs. I have tried to fly with my Microsoft ID. They don't let me on the plane. They insist on seeing a government ID, and then they let me on the plane.

Now, why is this model so important? If you think about the way we do identity on the Internet, a lot changes when you go on in-person proofing followed by a real secret. In fact, over time, you can eliminate identity theft by devaluing PII [Personal Identifiable Information].

Let's face it. Today we are an information economy. You're asked for your social security number and all of those things.

We have a two prong strategy for dealing with identity theft in America. I love this strategy. One—educate consumers never to give out their PII, personally identifiable information…educate

consumers never to give PII out when they shouldn't. What are the odds of that working? No, no…don't worry. We have a second part of the strategy.

Everyone who possesses PII should never lose it.

Right? In fact, the UK government lost the data on 50 percent of its citizens in one day.

So yes, you can educate consumers. I'm all for it. And some will be cautious about giving out PII. And if you do the right things in securing—look, Microsoft has a lot of PII on its customers. Hopefully we'll do security right. We will not lose it and have to do a breach disclosure and all of that. It's not that education is pointless or some people won't do it right—they will. But the idea that we all do it right is a non-starter to me. And if you had this model where you went into DMV and you got your license and it had a certificate on it—signed by the state in which you live—then suddenly things become very different. Why? I go to a bank to open a line of credit—I enter my SSN—date of birth—name—mother's maiden name—and they say okay, we're ready to give you a line of credit. Please stick your government ID in the machine. The bad guy can't.

And because the bad guy doesn't have access to that certificate on that driver's license, I've devalued my PII. I can go to you and say here's my SSN—date of birth—mother's maiden name—knock yourself out, because you can't do anything with it. Yes, the threat model will change. People will bribe someone at DMV to issue a certificate, but we know how to deal with those problems. We've been dealing with them forever.

The important thing from the privacy perspective is twofold. One is people will have many forms of ID. You'll have a federal government ID. You'll have a state ID. You'll have a bank ID. You'll have a corporation or business ID or agency ID.

And the point is that if you have multiple IDs, and you can pass different IDs at different times, you eliminate the risk of profiling, or at least reduce the risk of profiling. If for financial transactions, I can use my bank card—for state transaction, I use my DMV card—for federal transactions like filing taxes, I use my passport. It becomes harder to correlate that data.

The second important thing is to stop thinking about identity as a binary. I either know everything about you or nothing about you. We have to move to a claims-based system.

In many circumstances, all someone wants to know about you is a claim, an attribute. For example, are you over 21 or not? For state tax purposes, do you live in this state and do you have an ID from this state or not?

Let me give you a classic example of a government ID being used by the private sector for a secondary use, for which it was not intended.

When I was much, much younger, I occasionally got proofed at bars. It doesn't happen anymore. But when I did, they would say to me, you can't drink unless you show us your driver's license. What did they look at on the license? They looked at two things. They looked at the picture. They wanted to make sure it was my license. And they looked at the date of birth to make sure I was over age to drink.

They didn't care what my name was, my hair color, my eye color. You could say well, the eye color would show up on your license. They never cared that they looked at the picture and the date of the birth. Imagine the digital ID where I could simply say to someone, I am over 21. That's all you really need to know.

If you think about passing claims instead of passing full identity, you can protect people's identity but still allow them to engage in transactions.

Now, on top of that, there's a third thing that the government can do which is, it can create a regulatory and social regime that really fosters both better identity and protects privacy and anonymity.

A classic example—the government could pass a law that says if you are claiming federal benefits—you want us to send you taxpayer money—you must authenticate yourself online with a government issued ID. It could be a driver's license. It could be a passport. But, it has to be government issued.

However, that same law could say, if you are going to a website—a government website—to obtain publicly-available information, the government may not require you to produce an identification.

So if you think about the CDC [Centers for Disease Control and Prevention], which might have information on HIV [Human Immunodeficiency Virus], if they require people to authenticate themselves to get that data, they won't go get it. They won't.

And as much as the government might be interested in knowing who has HIV for treatment and other purposes, they are actually more interested in having people get the data so they can make intelligent choices about their life so they don't spread the disease and they can treat their disease. It is in the government's interest to make this data as widely available as possible, and the way to do that is to preserve people's anonymity when they come to seek the data, and they can require that.

So in all of those contexts, if we think about ID the right way, suddenly you can create an authenticated infrastructure that doesn't raise the worst fears about what happens to our privacy—free speech—and other democratic values.

The last thing I want to talk about is alignment. Political, social and economic forces along with the IT in the middle.

One of the things that I believe is true is that very often, good ideas fail because of a misalignment between the forces at work: Political, social, economic, and IT.

There are some obvious examples. Congress passes a law—the Communications Decency Act—to protect children online. Everyone says that's a good thing to do. But that requires knowing who is a child, and who isn't. There is no good age-verification mechanism today online. And the Supreme Court strikes down the law as unconstitutional and unworkable.

Of course, if kids could go to the DMV—because people who don't drive do go to the DMV to get identity cards—if people were getting ID cards by schools, driver's license bureau or at the post office for the in-person proofing part, suddenly there would be a way to do IDs online that were meaningful. The state has verified that the person with this card is a certain age—yes, you can give your card to someone else—just like people lend their credit cards out—or even their driver's license so their friends can go drinking. But we know how to manage that problem and at least manage the risk.

But let me give you an obvious example about breakdown of the alignment of forces.

Many years ago I was sitting with a hardware vendor and they had a keyboard and the keyboard had a magnetic stripe slot so the consumers could just swipe their credit cards. You can think about why this is a good thing. Users would have to stop punching in all of those numbers and you would actually have to have the card to engage in a transaction. So I said to the hardware vendor, why don't you give these keyboards out with every machine you sell? And they said, well these keyboards are a little bit more expensive and consumers won't pay for it. Not only are they price point sensitive, but even if you bought this keyboard, and you were willing to swipe your credit card, which most consumers are used to because of point of sale terminals, no one on the web accepts that interface. So the consumer will have the keyboard but nowhere to use it.

So I went to the banks. I said, you have a lot of credit card fraud and identity theft. Leaving aside the security of magnetic stripes for a minute, wouldn't this be a cool thing, because then consumers could swipe their cards instead of just entering the cards on the screen. Of course the problem with entering the card numbers on the screen—it's a secret that's not secret at all. Every waiter I've ever given my credit card to knows the credit number, the expiration date and the security code on the back. So the banks said nope, not really interested.

Why? Economic misalignment. There are two types of credit card transactions, card present—card not present. Card present is when you go into a store and you buy something and you swipe the card and you show it to the merchant. Card not present is when you buy on the Internet or over the telephone. The merchant can't see the card.

In a card present transaction, the merchant takes your money and gives you the goods. If it turns out that was a fraudulent use of the card, because the card was present, the bank pays the merchant. The merchant gets their money, the bank takes the loss.

When you buy over the Internet or buy over the phone, the merchant can't see the card and verify you're the cardholder. And as a result, the merchant takes the loss, the bank doesn't pay.

So what the bank said to me—so you want to take card not present transactions, where the merchant takes the loss and we don't pay, and make them card present transactions, where we have to pay the merchant. Why would we want this? They have a point.

So I go talk to some of the big merchants. And I say, look, you're eating all of the fraud on this card not present transaction. Wouldn't this be good? And they said, you know, it takes a lot of money to build the back end infrastructure—interfaces—secure the whole thing. Yeah, but look at all of the fraud. We won't save any fraud. We'll build all this infrastructure but none of the consumers have the keyboard. And they won't pay for it.

And we're not going to buy it for them because they may not even be shopping with us. So you've got a chicken and egg problem. So I went to the Office of the Comptroller of the Currency. I said you have invoked regulations that require banks to do two-factor stuff. And therefore they are all doing their different stuff. Some banks are showing you penguins and some are mailing you USBs. Consumers are hopelessly confused. Why don't you do this? And they said that would be interference in the market. So what you have is a classic chicken and egg misalignment of these four forces.

And so one of the things we have to figure out as a society is if we want to drive this trusted stack in this meta-system of identity. We have to figure out smart ways of aligning these forces in ways that work.

And so in my last two minutes I'm going to give you a practical example of something I'm going to announce in two weeks, on the theory you're not going to run out and talk about it now, because in two weeks is the next RSA conference. And I'm going to be talking about what we've done in the last year to achieve parts of the stack. So, for example, we've had Bitlocker which is this TPM and trusted hardware. But there will also be in Windows 7 something called Applocker which means by group policy you can prevent anyone in your organization from running unsigned code. And in various places in the SDL and fundamentals, we've made a threat modeling tool publicly available so those millions of ISPs can start doing threat modeling.

But I want to talk about identity. We have a school district in Washington State that is in-proofing their kids. So all schools, to be clear—I talked about in-person proofing and how often it happens in your life—for my older kids, they are in-person proofed five days a week. It's called taking attendance in school. And as part of the process of student enrollment in school, this school district is going to issue kids digital certificates based on claims. And then school applications and partner applications are going to accept those claims. So for example, the school can set up a website for Ms. Jones' class and for the 5th grade and for the entire school. And to access that site, you will pass a claim that says I'm a member of Ms. Jones' class, or the 5th grade, or a member of the school. And the claim is issued by the school.

And then people can just sign on and do the things they want to do. How does this change the current model?

If my daughter gets—is online in her electronic playground and someone today says—hey, I'm going to send this girl a nasty message—maybe sexually provocative. If my daughter came to me and said look what this message is. I would say today, well, you're in the social networking site in the school. It could be anyone on planet earth who got access to the site. That's all we know. But in the certificate-based model, it would have to be someone with access to the certificate, which is based on in-person proofing. So if the certificate name comes back and it's my daughter's classmate Sarah, well, the reality is it's probably not Sarah, but it's got to be someone with access to Sarah's certificate. That means it has to be either her—her parents—her brother—someone who is visiting the house and has access to her computer. Law enforcement knows how to do those cases. And if Sarah ultimately said you know what, I left my computer on the city bus and I didn't have it password protected, we still have two options. We can leave the path open—sandbox it and investigate it—or we can revoke the certificate and throw the guy out of the playground.

The reason I'm doing this with the schools is because to get alignment, you need to align—one of the things I learned in government is if you want to get something done, find a train that's moving—jump on the train. There is so much political concern about child safety that this train is moving—the state agencies are driving it—and I want to be on the train and use it. But this works in the enterprises, too. At the end of the day, you may be in a place where you stop issuing IDs and companies just rely on the IDs of governments—accept their certificates for corporate log on and when the employee leaves the company—you just revoke the certificate. Because at the root, there will always be in-person proofing and a true secret.

So you will see as the years go on—this is a long term vision—but you will see many elements of this in our products that are coming to market. You will see claims-based identity infrastructure. You will see more reliance on the TPM. You'll start seeing us work on the very hard problems of trusted boot and enforcing application signing and addressing code injection.

It is a long path. But I actually believe as the threat model continues to get more sophisticated, we need to really drive the easier attacks out of the network. You will always have an insider threat—you may always have supply-chain integrity threats—you will always have dedicated, persistent adversaries, who are very creative.

Commercial software development will not, in my view, ever rise to the level of a national security protection because the markets aren't designed to do public safety and national security. You cannot make a market case for the Cold War. But what we can do is through smart engineering and the right philosophical approach, eliminate many, many, many threats to your network infrastructure, and that allows you to take the resources that you expend on all of these threats and re-purpose them on the threats that are the most intractable, and the hardest to deal with from a commercial perspective.

So that's where we're headed, and I'll be around afterwards if anyone has any questions. Thank you very much for your time. Enjoy the rest of your conference.

Chapter 4

Left to right—RDML Janice Hamby, VADM Robert Harward, VADM Nancy Brown, VADM Ann Rondeau and VADM Carl Mauney

COCOM Perspective

Moderator
VADM Carl V. Mauney, Deputy Commander, USSTRATCOM

Panelists
1. VADM Robert Harward, Deputy Commander, USJFCOM
2. VADM Ann Rondeau, Deputy Commander, USTRANSCOM
3. VADM Nancy Brown, Joint Staff J6
4. RDML Janice Hamby, USNORTHCOM J6

Objective
Discuss challenges, solutions and opportunities to enhance freedom of operations in the cyberspace domain.

Key Takeaways
- Focus on info/data (payload) security vice infrastructure (platform) security
- NORAD Northcom (N-NC) needs to be able to quickly set-up extended networks for civil emergencies, without endangering the GIG
- Great promise in identity management
- Need to support synchronizing NETOPS/ acquisition reform for faster response
- Need to manage/leverage DoD equities openly with the commercial sector, not control the commercial sector
- DoD/National cyber requirements take precedence over individual organizations
- Think of cyber as a domain that can be weaponized rather than admin networks
- Embrace culture of sharing among USG/ Allies/Partners
- Require Forces to show up with what they need to plug in for Joint Ops
- Support JS/J6 GIG 2.0 initiative
- Put the IO range to use and properly exercise cyber
- We must train as we fight
- Exploitation *vs.* Attack—J2 and J3 must collaborate
- Joint task forces should be certified before going into the field
- Work in terms of influence and visibility
- Some critical DoD CO occur almost exclusively on the NIPRNet
- STRATCOM needs to step up and provide DoD cyber policies

Panel Discussions
VADM Mauney: As General Chilton mentioned earlier, cyberspace is one of our three lines of operations. We sometimes call ourselves Cyber Command—that's a joke! No. We're Strategic Command, but certainly cyberspace is our developing line here. I wanted to just briefly mention the Unified Command Plan which proscribes to all the Combatant Commanders their missions—assigned by the President—an updated version was issued in December of 2008.

And in terms of cyberspace, for General Chilton tasks STRATCOM to operate and defend the Global Information Grid; plan against designated threats; coordinate with other combatant commanders for cyber threats; advocate for cyber capabilities; integrate cyber theater security cooperation activities; plan, direct and synchronize operational preparation of the environment with geographic combatant commanders; and execute cyber operations, as directed.

I don't have to tell this group in the 21st Century what cyber means to us. It is a domain, but it's a man-made domain that exists because it was invented, and it was invented as a way to conduct many things. In addition to [the way] we use it today for military operations, it's arguably the economic distribution system for data that powers our economy, and many other critical elements of our society.

But it could be removed. And so I think we've talked about that in some degree this morning. We could lose cyber capability or cyber access. And so what we're about here in the military is maintaining that freedom of access for the nation.

And I don't have to—I was going to mention General Chilton's 3Cs—conduct, capabilities and culture—but I think he covered that pretty well.

Our first panelist is Vice Admiral Nancy Brown, the Joint Staff J6—principal adviser to the Chairman on all command, control, communications and computers matters.

I'll introduce each panelist and then ask them to give a few minutes of their thoughts and remarks on the joint view and the combatant review in cyberspace. So Nancy.

VADM Nancy Brown: Great, thank you very much, Van. I want to thank STRATCOM and AFCEA very much for providing me a short respite out of the beltway. Anybody who's ever been there knows that any minute outside of it is better than any second inside of it. And so I'm pleased to be here for that reason as well as to be part of this joint panel.

And I did say that this was historic, but, you know, it really is because when I was—my first time on the joint staff was in early 2002. I would go to joint meetings, and there would not be one other Navy person there. So this really is remarkable to have COCOM deputy commanders here at the table being Navy. So I'm pleased to be a part of that.

What I thought I'd do this morning is just give a brief overview of some of the things that J6 is doing to try and support STRATCOM's efforts, as we figure out how we're going to operate in this new cyber domain. You know, one of our real challenges is really to figure out how do we maintain freedom of access in this domain and how do we maintain freedom of navigation.

We have to figure out how to fight and defend in a domain where we know we're facing very sophisticated adversaries. And it's going to take a real dramatic shift in how we think about our networks in order for us to be successful.

We have to design a security framework that promotes freedom of access and freedom of movement and enhances our ability to reach out and embrace new capabilities rather than restricting us from using those things.

We have to change the way we think about our networks from administrative things to lethal weapon systems. It's a system that can be used against us if we're not vigilant.

We have to address the entire DOTMLPF [Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities] spectrum and one of the hardest things I think we have to address is one of the General Chilton's Cs, and that is culture.

And joint is not good enough anymore, but we have to figure out how do we dynamically include our NGOs [non-governmental organizations], inter-agency coalition, and first responder partners. Whomever it is we need to share information [with] on the battlefield, whether that's humanitarian assistance or whether it's fighting a terrorist. How do we provide them the access to the information that we're both going to need in order to be successful?

So why is this so hard for us? Well, our networks evolved as service systems, as service Intranets, not as a Global Information Grid. And so when we stand up JTF, all of the components show up, and each component brings a different network. Each component brings their own information. Each component brings their own processes, procedures, policies. They are all different.

And so the JTF commander ends up being a systems integrator. And that's one thing you don't need the JTF commander worrying about is how to integrate the technology that's there to help him or her prosecute their mission.

So we need to figure out how do we solve those issues so that when a JTF stands up, people come and they plug in. And they have available to them all of the information they need. They don't have to bring their servers from home station. They don't have to establish a new domain. They don't have to get new passwords or user names. They arrive, they plug in, and they are ready to go.

And that's what the warfighters deserve, and that's what we should be figuring out how to give them.

I like to use, and I don't want to steal Ann's thunder, but I like to use TRANSCOM as an example because an AO in TRANSCOM that wants to complete one function of putting together a mission package, has to log on to 17 different systems—that's 17 different logons—just to do one function. They use three different CAC cards to do that.

Now, if you think that makes that person agile and effective, then we've got a place for you in the Pentagon. But if you think there's something wrong with that, then I'd like for you to join my team.

I recently had the opportunity to hear Lieutenant General Kearney, the Deputy SOCOM Commander speak. And he said some very unkind things in a very kind way, about the information technology

industry and the folks that provide him things. And at the end, he summarized his remarks by saying—you know, I want five things. If you could just give me these five things—then I would be happy.

He said—I want access to data. I must be able to discover and understand it. I want global access. I want one network with a common infrastructure. Four, I want common policies and standards. And, five, I want to be able to use Web 2.0 new tools.

So I was heartened hearing that because one of the initiatives we have in J6 is a framework that we're using to describe our vision for where we want to take the department. And we call it GIG 2.0 and it has five characteristics. And unbeknownst to me they are really the same five things that the general said that he needed.

Our five characteristics are global authentication access control and directory services—that means I can go anywhere in the world and I can access the network the same way I would regardless if I'm on an Air Force paid for end implement or I'm on somewhere where I have a Navy paid for desktop. I have access to all of my information because it recognizes who I am and what my mission requirements are at that time. And so when I deploy or I'm at home station, it's no different. Look-feel is the same.

Information services from the edge. When we design capabilities, we need to design them with that edge warfighter in mind—the person that's disconnected—the person that has limited bandwidth. How do we get them those capabilities? It's not important to get capabilities to people that sit in the Pentagon. It's important to get capabilities to the warfighter. But, yet, if you look at our program of records—the big ones—none of them takes those capabilities to the warfighter. They are based on requirements and bandwidth that don't exist at the edge. And so we have to change the way we define our requirements so that the first person we consider is the warfighter.

We need joint infrastructure. So we've got to figure out how to seamlessly put together this infrastructure. We have to be able to incorporate wire and wireless. And it needs to be operated so that the folks that are doing the defense—the folks that are doing the operation—the folks that are doing the attack—are able to see end-to-end and understand what's going on in that entire network so we have situational awareness.

We need common policies and standards. You know, if I certify a piece of software, that should be good enough for anybody else in DoD. We need reciprocity. Another example I like to use is TRANSCOM. If TRANSCOM has one software upgrade made to one software program, it may take one week to write that upgrade. It takes them 18 months to put it on their network to use because there are so many different accreditation authorities that have to test and certify it before they use it. So it's outdated before they can put it on their network.

And the fifth one is unity of command. We have to figure out how we define a command and control structure that supports the operation of a global network that needs to operate at network speeds. And you can't do that when you have service components, COCOMs, and every other cat and dog out there being a DAA [Designated Approving Authority] and taking control and trying to implement different policies and procedures on their networks. And deciding what they are going to allow and what they are not going to allow across their network. You're never going to get into the enterprise approach that we need to.

So I like to say that, you know, we've entered a new world. And the new world we're in is one of blogs—wikies—social networking—those web 2.0-like tools that we need to be embracing. We need to figure out how we incorporate those. We learned we couldn't fight a counter-insurgency from garrison. We need to appreciate the fact that our network will never be effective or allow us to be as effective as we can if we seal it off and make it a garrison.

We need to be out there. We need to be operating and taking advantage of the tools that are available to us today. And that's why our security architecture is so critical to us, because that's what's going to be key to allowing us to do that.

And so I think that if we fail to take advantage of that, we are going to be irrelevant in today's world. And so it's a real challenge and it's one that we're working with STRATCOM and all of the other partners—NSA, and DISA, JTF-GNO, JFCC-Net Warfare—to try and address. And thank you very much again for the time today and I look forward to questions.

VADM Mauney: Our second panelist, Vice Admiral Ann Rondeau.

VADM Rondeau: First of all, I want to also thank STRATCOM and AFCEA and to tell you that all of the folks up here are friends, but also smarter than I am at this stuff. So I'm learning from them everyday. And Van, thank you very much.

My world as a Deputy Commander at USTRANSCOM is an interesting world. There used to be a thing called Wayne's World. Well, in TRANSCOM—70 percent of my asset management is commercial—30 percent is organic military.

In my mission, I touch railroads, trucks, trains, air, and ships at sea.

I am a COCOM by mandate—by UCP—and by direction from DoD—the manager and the influencer of the entire distribution process within the Department of Defense.

So my world is 70 percent commercial. We have—along with SOCOM—we're the only COCOM with acquisition authority. And so much of my interfacing is not within DoD. It is on the NIPRNET and it is with commercial industry.

There is no way that I would even possibly hope, even with the largest ego that anybody would have, that I would ever have C2 over my domain. And so what we do is that we're not ones who look at command and control of the distribution process. We do not seek to understand that we're going to ever have C2 over the entire logistics network of DoD. We do work on a principle of influence and visibility.

Now, it's interesting what that does for us is that both the words trust and visibility have two connotations for us. One, and the one that drives us principally, is the trust of the warfighter. And what he or she asks for is exquisite visibility as to what comes to him or her at the point of effect—whether it be food—or it be ordnance—or it be bullets—or it be radios.

We also have, though, the trust of what our networks do to make that happen. Visibility. It means for us that every warfighter who is in our system has visibility to where his or her stuff is because, frankly, we're in the world of Amazon.com. And they want to know now where their stuff is and, frankly, that also is a responsibility of ours so that people are not hoarding and ordering more than they need to and getting more inventory than is even manageable.

So visibility for us is part of the trust, but as it is our strength in terms of delivering to the warfighter, the operator, it is our—it is potentially our weakness—because we track everything. We track everything.

When you track everything, and you do it through satellite RFID [Radio Frequency Identification] or ITV [in-transit visibility] or asset visibility, not only are you able to track that, but so can everybody else in some manner, because as we've heard today and as we will hear forever, there are very few things that are very secret when it comes to anything you are doing on the Internet.

So if I look at trust and visibility, I've got to look at it from both sides. And what we do is that we also maintain the Internet—and how I manage the NIPRNET where I live—mostly where I live—we do it by visibility.

So I do not even pretend that all of my commercial vendors and partners—that they all are going to have everything that I need for protection of my network as I use it. But what we do is that we use the contract mechanisms that when we put out the RFPs [Requests for Proposals] or any other kinds of contract tools and mechanisms, that we ask industry and our commercial partners who are so important to us that they meet certain standards—that their people are trained to certain kinds of requirements, and that, frankly, we have an obligation to also train those partners, because it helps us.

So rather than a lot of money and time and assets put towards trying to—and I love Nancy's phrase—trying to put us in a garrison mentality—we [need to have] frankly, an open mentality.

We believe that we are pushing against impossibilities if we try to just hunker down and lock everything down because we will be challenged in courts. By who we disadvantage—of various kinds of vendors and commercial partners—so we have adapted to our environment.

Rather than trying to make the environment completely come under some sort of a C2 environment, we have said we are in this environment—we are in this milieu—how do we protect ourselves?

So in summary, I will tell you that the answer to the question is in General Chilton's comments. It is about

culture. It is about us training our people and making sure that we are accountable to that. It's about, also, the culture of how we organize—how we operate—and how we behave.

It is about conduct and behavior and to make sure that people are not only within our areas—across also. So how we organize within the COCOM is important. And it is about capability. It's about making sure everybody who comes into us meets a certain standard, and we can do that by contracts and we do that and we keep people out who will not comply with that process. So we are about behavior because we know that our customer base is, first of all, the warfighter. We must succeed when it comes to supporting him or her, but our providers are outside of us in terms of DoD. With that, I'll stop and I'll look forward to your questions.

VADM Mauney: Our third panelist—Vice Admiral Bob Harward, Deputy Commander, USJFCOM.

VADM Harward: Thanks, Van. I think what Van was trying to tell you, and I'll acknowledge, I'm probably the least qualified person in this room to talk to you about cyberspace. And why that's important, when you get to hard questions, please ask my shipmates and my other panel members at the end.

But I want to talk to you about my background and what we do at Joint Forces Command because it's all about the fight. And I want to make comparisons about this fight and another fight. The fight we have going on with Al Qaeda. I was at a meeting last week with Dr. Bruce Hoffman from Georgetown, one of the preeminent experts on terrorism and he was saying we were at the 20th year anniversary of Al Qaeda. I went back a little further actually. I went to the bombing of the marine barracks in Beirut where we lost 243 marines and our embassies there. And then you can trace it through Khobar Towers—Yemen—the attack on USS COLE—the attack on our embassies up to 9/11—when we really realized we were at war with these guys and we got serious.

But I want to make that analogy to this war—this conflict we have on cyberspace. I can't tell you where we are in it right now. Have we seen a Khobar Towers? Is that what Buckshot Yankee was? Is 9/11 the equivalent tomorrow? Is the enemy trying to bleed us out of resources—kind of a philosophy we used against the Russians in the Cold War? We don't know and that's why we're challenged. So when we prioritize our efforts in what we do in this realm—we base it and everyone does—on DoD efforts—how does this sit-up against the other things we are doing in the fight right now. I had an opportunity to spend a day with General Chilton and his staff here a couple months ago. And I went home and I was in awe at what I saw—Ops Center. And I went home and really started doing my homework—reading his testimonies on the Hill—reading stuff they were saying in their speech—and I was struck by the three no-fail strategic missions they have. The deterrence—the nuke; the space; and then the cyber. And the complexity on how difficult that job is and why it takes an astronaut or rocket scientist to run this command.

But that's one of the issues. It's hard to go and tell Congress and all how serious this fight is and how we prioritize these assets. And I'm amazed the boss can pull away from his entities and spend the day here with us doing this. I just wish we could really assess how much damage has been done and where we're at and make sure each one of our soldiers, sailors, seamen and airmen understand that, because that's the challenge we have day in and day out.

I can tell you at Joint Forces Command, we are very much a supporting entity to STRATCOM and all of the other components in this. And we have that full—I call it cradle-to-grave capabilities and efforts we do for the joint force—be it joint concept development and experimentation—integration into the force—force provider and global force management—augmentation—lessons learned—training. And so in all of those efforts, we're tied in with STRATCOM and working in those efforts, and we have different degrees of success in all of them. And it's a challenge day in and day out.

But I wanted to hit a couple just to give you a sense of—down in the trenches—what we're battling through and what's going on.

The boss talked about accountability—setting standards and holding people accountable—but how difficult it is to make them…After Buckshot Yankee, we knew we had to do certain things so we came up on the VTC—told everyone—we put it on our NIPRNET—you can't do this—you've got to do this—and yet a week later, we had two more violations. Well, I was on leave, or this woman was at the hospital. Okay. Now we need this accountability. So I've told my guys, I want to be able to tell—tell me when I have 100 percent

accountability on the net. I made it mandatory for everybody at JFCOM to log on to the portal once a day and I wanted a ticker to tell me that they've all done that so I had that accountability. I can only get about 60 percent right now because I can't find—it's hard for me to make sure who is on the system—who is logging in—and we battle that—and it's different between a guy in uniform, a woman GS, or someone else in our contracting force.

And when I find a contracting force who hadn't applied to that standard, I can't do the same thing I need to do with that person. I can go back to the contracting agency and say, hey, this individual is no longer allowed on our systems or allowed to our access. You've got to keep him out of our command. And they are working with us. But how we're going to do this accountability and the standards is going to be a challenge, and we're wrestling with that day in and day out.

We're very focused on making sure we train as we fight. And that's got to start at day one when that soldier—that sailor—that airman—that marine show up and know here's what you can do or what you can't do on your NIPRNET system. And, oh, it probably applies at your home, too. And that's at the service level, Title 10.

I've got a responsibility in that joint world of making sure those JTFs [Joint Task Forces], before they go off to Iraq, Afghanistan, or HOA [Horn of Africa] have those standards. And I'm fortunate because I own entities like the Joint Command Support Element—JCSE—who is out supporting all of these JTFs—we can get the standards to them. And so if an event happens, we can quickly get it inculcated into the processes forward with the warfighters. But I still can't get that accountability. It's a tough part of the equation.

Games and exercises. I can't tell you how important it is for people to be able to go out and exercise and do this and yet you can't do it on our systems. So we've established an IO-net. A whole separate entity we can go out and exercise and train on to bring people up to standards and stress them on that system. Now, that system was bought three years ago for a whole different purpose, and we were only funded to certain levels—it's grown by tenfold—and it's tough for me to get the assets now to make sure that training expands accordingly—but it's another area we're working in.

This whole issue in being a guy at the tippy end of the spear was frustrating—this exploitation versus attack capability is going to be a persistent—and both have very valid arguments. And it goes back to this—what's your J3, your J6 and J2 doing? Boy you've got to bring them all together and they've got to live together so you know when you need to exploit and when you need to attack. And oh, by the way, we need to really start building up experience and corporate knowledge on how we do this attack function. If we can't work through the ROEs [Rules of Engagement] and stuff to do that now, when we really are going to need it, we won't have that experience.

And last, back to this issue of certifying JTFs—how we're going to get these standards—how will I get the warfighters forward to embrace and understand and bring this under their auspices—is another part of the equation we wrestle with each day. So I just wanted to give another perspective from the warfighter and how we support STRATCOM and the COCOMs in this effort. Thank you.

VADM Mauney: Thanks, Bob. Our final panelist, Rear Admiral Janice Hamby, Director of NORTHCOM J6.

RDML Hamby: Thank you, sir.

Because I'm the one star on the group, I felt I needed to have a slide to back me up because I didn't have those extra two stripes. I'm kind of hoping by being on this panel with such a distinct and august group of folks, maybe I can get a battlefield promotion out of this. We'll see how that goes.

If you take a look at the slide that I've brought today, I want you to have an appreciation for the spectrum of operations that are addressed by NORAD and NORTHCOM. If you follow that arc that starts out in the lower left with Defense Support of Civil Authorities and it moves on up into Homeland Defense, that covers the ground in terms of what our mission set addresses. Some of the things we do are planned—National Special Security Events—the Super Bowl—things like the Democratic and Republican National Conventions—and so forth. We're able to plan for those.

Other things are surprises. Hurricanes that come in, we can anticipate over a three or four, maybe a week's period—three or four days or maybe a week's period. But other things like earthquakes—wild fires—mudslides—those are things we can't anticipate quite as directly and we have to respond to very quickly.

This is where a lot of my challenge as the J6 lies. If you look in the upper left quadrant of that slide, you will see a mere representation of the symbols of the different agencies, organizations and groups that we work with on daily basis.

We have a routine and continuing relationship with over 60 Inter-Agency partners. And this means we have over 60 sets of protocols to deal with. And we have to come to some kind of an agreement—establish the protocols and parameters by which we are going to share information—so that we can develop a common situational awareness and be ready to act when the nation needs us in the event of those emerging events, or in a more coordinated fashion for those planned events.

Now, those 60-plus Inter-Agency partners are not the only people with whom we do business. When an incident takes place to which we need to respond, we also now have a new set of partners [composed] of the local first responders—so that police force—that fire department—perhaps that tribe—or the county government—we need to be able to inter-operate and share information with them so that we can all direct our level of effort to the most urgent needs, and so we aren't being redundant and overlooking other critical needs within that little area of response.

In order to do this I need to have a very, very agile network. I need to be able to flow my network forward very quickly, which I do with mobile communication suites. I also need to be able to tie in other folks' networks into that suite. Now, some of that is done through some of the great equipment that has been developed to support us. If you're not familiar with the ACU1000—that is my saving grace—it allows me to tie local first responder networks into my networks so we can communicate even by e-mail or by radio frequency—by hand sets—so we can coordinate a response.

We also work with commercial providers so we can roll in mobile cell towers and bring cellular service for the first responders—for the governmental response—into an area that has been wiped out—that does not have use of the mobile services that we've all come to rely on today.

So this challenge is a very real one. I need to be able to react very, very quickly. So how are we able to do that in an environment where we're trying to lock down the network? This is kind of a repetitive or it's a redundant theme here. Those of us who are out there working to accomplish the day-to-day operational mission are asking for more freedom of maneuver.

Now, as I asked for that, I also do not want to put the global network at risk. And with my background, I definitely recognize that by creating a vulnerability in one area of the network, I'm exposing the entire network to that vulnerability. So I want the ability to have this agility within protocols that also bring me a reasonable level of risk avoidance—of assurance that this information is going to be protected.

I believe that a great deal of promise lies in the field of identity management and the ability to work with folks in advance so we can establish some kind of credentialing system or token system so that we would be able to recognize them when we need them. So that's one area. We were asked to identify areas where STRATCOM might be able to assist us. If STRATCOM is able to help advocate for the resources and a common approach for how we go about identity management, I think that would be a great thing.

Now, other areas where I would love to work with STRATCOM to advance the cause is on that whole synchronizing piece of the UCP. And I do not envy them this task. The responsibility of synchronizing cyber operations is an incredible, incredible task that they have got.

We took 30 years to get to the point where we are today with somewhat fragmented network—different sets of protocols—different ways of doing business. And sir, I think it's going to take you a while to get backed out from where we are to a more rational approach. We applaud all the efforts of your team to try to drive us in that direction. It's a huge, huge initiative and one that we all need to support as deliberately and as actively as we possibly can.

Another area where I could use support is in the advocacy for acquisition reform, because many times our ability to respond to direction from STRATCOM is limited by how quickly we can bring on board the appropriate hardware or software or services in order to do just that. And the way our hands are tied within the contracting system right now, it sometimes makes that response far, far, far less than agile. So advocacy in the area of acquisition reform would be very valuable.

Now, for our mission set, the real center of gravity is actually not the networks themselves. It is the information on the networks. So I would also urge the entire community to take a hard look at our strategy of trying to harden and defend-in-depth the network and see if we can't shift that focus just a little bit to a focus on the information itself. I'm reminded of the story of the thieves who stole the ATM and were ultimately unable to break into it so they abandoned it. If we can provide a structure whereby our information is protected in a hardened fashion, even if it's exfiltrated, maybe we won't have to be as concerned. So a focus, a strategy focusing on the protection of the information itself would allow us to perhaps, be a little more open in our view of how we allow access to the network.

I think we'll probably get questions on command and control of the networks so I'll avoid that for right now. But I would say that we have a need to react quickly at a local level. All activities are, in fact, local. So whatever command and control structure we do work through, it needs to be very responsive right down to that local piece. And the local elements need to be responsible backup to that authority and be held accountable to them. The discipline and the accountability of our individual users is going to be key. It's going to be the critical success factor to our ultimate success in this entire network world.

And then the last thing I would offer to you is a quote by Admiral Grace Hopper that I love, and I think applies directly to our challenge ahead of us and that is—"A ship in port is safe, but that is not where ships are meant to be." And if we are to close down our networks and make them entirely hard to those folks who are not DoD and may need to do business with us, then we are, in effect, putting our ship in port. And we need to be out there. We need to be out there in the world reacting to, and dealing with new partners everyday and we need to figure out a safe way to do that. Sir.

VADM Mauney: I've already got some questions but what I would like to do is take just a couple of minutes and orient those of you who are not in the military, maybe some of you who are new to the military, into some structure in the "as-is" mode.

In cyber, we talk of really three bins of organizations—combatant commanders, services, and agencies—and that's within DoD. These are the participants, as it were, in the Global Information Grid, and these are the groups that STRATCOM and our components who are assigned the cyber mission deal with on a day-to-day basis.

Combatant commanders are like the production department in a major corporation. We produce things. I don't want to get across the breakers here, but we use the word effects all of the way from non-kinetic to—we can blow things up, too.

Contrast that with the services and their role is organize, training, and equip. They are the human resource department, the training department, and the procurement departments. And so the services have pretty much procured the cyber networks and put them in place as they are today.

And then agencies in the department provide various services and support either the services or the combatant commanders, or both, across a wide range of activities.

In the case of Strategic Command—how we're organized to do cyber—we have the headquarters staff which is focused on integrating across our mission areas—principally the three lines of operation—and then the joint enablers are also worked by elements of the staff and the subordinate organizations who work in those areas.

In terms of cyber, we have two components that are primarily focused on cyber. First, Lieutenant General Keith Alexander at the Joint Functional Component Command—Network Warfare—and I know Keith is going to follow me so I'm not going to talk about his role other than to say he's got the lead for operate—defend—attack—and exploit, blending the various authorities under his hats.

Lieutenant General Carroll Pollett, JTF Global Network Operations is the commander responsible for operating and defending the networks. And so both Keith and Carroll bring in their organizations over which they are dual-hatted. In Keith's case, it's the National Security Agency and in Carroll's case, it's the Defense Information Systems Agency and those elements of the cyber piece cannot be understated.

The last thing I'll mention, and this is one of the areas that we are working on and we are working to sort out—put in place concepts of operations—is how to prioritize, and I think all of the panelists have mentioned that in one way or another. Prioritization between mission assignments and between allocation of resources is a never-ending endeavor, and we need a process that will allow to us do that for cyber.

And then the last point I'll make is we think of cyber in a similar way that we think of space. Space is an area where there are very limited and precious resources. The space assets of the nation that belong to the department are assigned to Strategic Command, and yet we can use those resources in any region and support any combatant commander and we do that every day. And so through an organization at each combatant commander, the Director of Space Forces, we provide those effects. We support their operations, be it in the middle of Baghdad, or out in the Pacific Ocean. So that's a model that is one of several that we're taking a look at to get to some of the issues that the panelists have mentioned.

What I would like to do now is I'll just dive right into the questions. And the first one is STRATCOM Centralized Command and Control Model seems to conflict with the unified action at the theater level. Is it STRATCOM's position that all networks—services—agencies—combatant commanders—will be operationally controlled by STRATCOM and/or what is the COCOM role in C2 of all domains in their warfighting theater?

I'm going to answer this one from the STRATCOM perspective and then I'll ask the panelists for their views and I think Jan has indicated that that's a question.

As General Chilton mentioned, this is our least mature area and how to satisfy the requirements and, indeed the needs of the various regional commanders, is one we're only beginning to fully meet. I would say that the effects that you want from cyberspace—freedom of action—the ability to support military operations—fall into two categories. One is those who are confined to a theater, and in other words, there are some things that the Northern Command commander can do or needs to expect from the cyber capabilities of the nation. And that applies to Pacific Command and indeed all of the other regional commanders.

But—and this is my opinion—most of those activities cover more than one region simultaneously. And indeed our experience is—and you know this—but you can be on your computer in your home state and the server you're looking at is in a foreign country and you're not sure of that. You don't know where it is because of the transparency and, indeed, the global nature of the Internet.

So the ability to respond at net speed, be it in a region or be it global, is one of the challenges that

we just have got to conquer here in cyberspace and I think we're making good progress.

But what that indicates is a demand for the command and control that's like space. It's the ability to deliver things, either pinpoint in a region, or more broadly—and I'll use the case of operate and defend the network—more broadly in the event of a cyber—I don't use the word attack, but I'll just mention, you know, the conficker worm problem is a global problem. And so you've got to be able to simultaneously deal with the pinpoint effect as well as the broad problem. So I'll open it up to the other panelists.

RDML Hamby: I don't think there's a person in this room who does not understand the construct of this being a global issue, and that when events take place in a local spot on the network, they really are a global event when you back up and see the possible implications that the incident could have for the entire network.

I would suggest that because we have gotten to where we are over the course of three decades plus, that to try and correct that situation and put in place a very centralized control immediately would meet with great resistance from many of the players who are out there. Rightfully or wrongfully, doesn't matter. I think the fact of the matter is that there would be a great deal of pushback.

I think that pushback could be minimized—could be driven down—and even transformed into acceptance and even an embrace of the construct—if we worked on some of those issues that Admiral Rondeau actually spoke about in other comments, and those revolve around the issue of reliability—influence—and visibility.

If we can work the construct where through a common understanding of what it is to say that our network is ready—if you tell that to any commander they understand what you mean—what the elements are that go into your network-readiness picture. And if you can consistently deliver on your piece of the network, then I think the transference of that control over the COCOM or the organizational network would be much, much more readily greeted.

So I think the first piece of it, it's almost a phased approach to how do we get our hands around this problem, and I think the first piece is building on the visibility of what is going on in the network so people have a better understanding of the current situation in which we find ourselves.

Then the influence piece—the synchronizing piece of providing authoritative direction on how configuration must be managed—on how the things that we have done, for instance, through the establishment of the "new normal"—if you'll forgive my use of that phrase—providing those parameters within which the COCOMs—the services—the agencies have some freedom of maneuver for their own networks. That helps build that trust between the organizations, and I think eventually that control piece then can transition into a more joint network, into a STRATCOM view.

I really think it does circulate around visibility and understanding what readiness is. We have done some work across the COCOMs for the Joint Staff to develop a network-readiness model. We at NORTHCOM are referring to it as the Horigon readiness model in honor of the 03 who spent his life working on it and coordinating and collaborating with the other COCOMs. And we'd be happy to share that with anyone—and I think that's a big step in terms of developing the sense of trust—that we're all talking about the same thing—and that we can be relied upon when we say that this is the status of our networks. We owe that to you, and if you're able to provide that to us about the other networks within our COCOM regions, then I think you'll see those fingers starting to unclasp and release some of that control up to you.

VADM Brown: Well, I don't think we'll ever be in a situation where something as complex and as large as the Global Information Grid is really going to be able to be controlled—centrally operated—and maintained centrally. The network is going to have to be operated from a strategic to a tactical level. And every point in between is going to have a role and a responsibility—authority and accountability—in ensuring the proper operation of that. And I think it's almost, right now, almost too hard of a question for us to put our arms around if we look at the status quo.

I think we have to do a lot of things in different areas in order to achieve the situational awareness—the definition of what the network is—the definition of what control really is—in this environment. And I don't think the old terms of OPCON and TACON will apply. I think we have to come up with new definitions of how we actually

command and control something as immense—and as Ann brought up—an excellent point—is that this is not just a government-owned thing. I mean, there are a lot of tentacles off this network that affect our readiness as Ann pointed out. And without having a complete picture of all of that, you can't really maintain or attain situational awareness to be able to understand what needs to happen. And what the second and third order effects are of something being done in one area to several other areas in different COCOM's responsibilities areas.

So, we're going to have to really do some hard work. There's going to be a lot of rice bowls that are going to have to be broken, and this is probably, I think, the biggest challenge that we have as we move forward is the culture and the trust—the ability to get over having to own and control things ourselves—to be able to really resolve how best to organize and delegate responsibility—to operate and maintain a Global Information Grid.

VADM Mauney: Okay. Let me move on to the next question. There seems to be great emphasis on taking the enterprise-view in providing enterprise-wide capability for our networks. To what extent are the combatant commanders directing the service to participate in joint enterprise architecture development to enhance each component's ability to provide the capabilities that will be integrated from the start? Nancy, you may want to take a stab at that one.

VADM Brown: You know, I think it's a complicated question. I'm not sure that the COCOMs can direct the services. Each COCOM has a service that's an Executive Agent and, of course, they have their components, so they can direct things to their components. But the issue of enterprise services is one that—I really believe it's the best way forward for the department because you're going to save money—you're going to save resources—and if you can buy something once and we all use it, it's a lot more effective. And that's really the theory behind enterprise services—is that we all don't have to have a Microsoft license for e-mail—that if we have an enterprise license, we can consolidate the servers and we can provide e-mail capabilities from an enterprise, it's going to save us dollars—it's going to save us personnel—it's going to save us boxes in our spaces which saves air conditioning—power—on and on and on and on. So if you look at it from a delivering a capability in a cost effective means, enterprise services is the best way to approach that.

Now, we have a lot to learn in how to do that effectively and how to do that so we continue to meet mission requirements because it has to be able to be timely. It has to meet the requirements of the individual command. But I do believe that that is the best way for the department to move forward. And if we can get a Microsoft to provide that service for us, as a managed service, we shouldn't be doing it ourselves. And I think that the COCOMs would agree that if they don't have to dedicate resources to supporting an e-mail server, and they can put those resources on to something that's more directly related to mission requirements, then that's the best use of their resources and helps them in the end, and is a benefit to all of us.

So I'm not sure if that really answered that question, but I think enterprise services is the wave of the future and I really believe that it's going to be a great benefit to all of us.

VADM Rondeau: So how do you control or direct an enterprise? I would submit that the term "direct" is kind of interesting because I'm not quite sure that the word direct really complements the optimization of the enterprise. However, I do believe that leadership matters. So what USTRANSCOM does with our components is, first of all, every Wednesday we have an Ops Update that brings in our components and, frankly, one of our other partners, DLA. And we go over the entire world of what we're doing. But the very second thing that happens after the first J2 pre-brief, is that we get a cybersecurity briefing. So all of the components see—right there at real time—what is going on. So the enterprise does not direct behavior as much as it seeks to inform leaders.

Secondly, when we have a component that has had a cybersecurity behavior problem, we feature it. We bring AMC [Air Mobility Command], MSC [Military Sealift Command], or SDDC [Military Surface Deployment and Distribution Command] in on those Wednesday Ops Updates and we allow conversation—because what is happening to AMC is happening to SDDC—what's happening to MSC is happening to AMC—and so our components get to see each others issues—behavior errors and mistakes—and remarkably, with a four star there, behavior improves.

Third thing is that when you make a component or anybody accountable, it is abusive if you don't give them the tools. So in the year of 2008,

USTRANSCOM asked the components what is it that you need to come up to the standard that we expect? And indeed we bought for the—Army—SDDC—our component—we bought for MSC—the Navy component—and we bought AMC—our Air component—firewall protections. We bought them training. And we bought them other things that would meet up to $1.5 million—not much money—$1.5 million to bring them up to what we thought was a standard by which we could hold them accountable. We did not direct, but we shared and we collaborated on information and common knowledge. And that then brought coherence to the behavior. Because we can not direct a Title 10.

But leaders matter. So if we inform the leaders and bring them to the table—and have the conversation—and maintain the standard—and help to enhance that standard—and we walk the talk not only as just the COCOM, but as the COCOM that cares about their component succeeding, because success for us equals success of the warfighter up on the point of effect—then we believe that we have exercised enterprise leadership and management.

VADM Mauney: Let me just add in a more practical way what the COCOMs do to provide that kind of information to the services. What is it that combatant commanders need. Joint Forces Command, Transportation Command, and STRATCOM periodically host what's called a Senior Warfighter Forum [SWarF], which is a forum where all of the Deputy Commanders of all of the combatant commanders come together, following roughly two to three months of staff work by our staffs to prepare for an issue. And back in February, we did one of these—focused on a number of things—but cyberspace was one of them. In that forum, we looked at the capabilities that each combatant commander determined for his particular mission set was needed and we prioritized those and we provided those as input to the Vice Chairman of the Joint Chiefs. And he, in turn, fed those into the budgeting process in the Pentagon. So that goes into the Services. It goes into the other forums that are on the leading edge of building programs for cyberspace. And so that is one way that we get our voice heard.

The second way—General Chilton mentioned this morning—that's one of conduct. And that's setting the standards and JTF-GNO and JFCC-NW are in the process every day of setting those standards and getting that word out and providing the baseline standards. We're not nearly where we need to be in terms of standards and—something that's already been mentioned—visibility and transparency of the network— but it's a known to-do—it's on our work list. And it's one of those things that's going to evolve over time as we learn more about our network, and we're able to, through the commanders, get those standards A—implemented, and B—followed.

VADM Rondeau: Can I also add to that, and I—thank you, Van. The role of JTF-GNO is critical because they help us to think across not only our enterprise…and it helps us across the COCOM so that components and services are not whiplashed all of the time. And so it does help us through JTF-GNO to have some coherence about those standards. So thanks, Van.

VADM Mauney: The next question, what is the acquisition authority impact of capability portfolios, including Joint Forces Command—the command and control portfolio—and STRATCOM's battle-space awareness and net-centricity? Do Services continue to have ultimate Title 10 authority or is there a shift to JROC [Joint Requirements Oversight Council]—OSD increased acquisition authority. These are related questions, and I'll ask Bob to lead off since they do the C2 portfolio and perhaps you can talk about that.

VADM Harward: You know, it's interesting. I sat at a defense writers group the first week I was in the job in November, and they asked me that same question so I could plead ignorance at that point. But my impression had been at that point through the capabilities portfolio manager—JROC—all of those, even the SWarF—that it was very open—very collaborative—and we were getting what we want.

Now that I've been in the job six months, I'm not quite as happy. There are some areas where we've had long collaboration on projects—I'm not going to be specific—where we had worked with all of the Services—moving down the road—over three years—commitments made, and now in the final stages of those commitments where we had commitments—Services have pulled out of those—large sums of money out of some of those commitments. Our only stage at this point is go back through OSD—identify those—work through the SECDEF—to make sure they are aware that some of these Services—or this Service in this one case—had taken a different course.

So ultimately there is still some tension. I think the process is good. I think it's valid. I think we're going to see as we go through this QDR [Quadrennial Defense Review] and this budget crunch, further validation of the program, one way or the other. I don't know how it's going to shake out. But it's tough, also, as the Services have some big demands on the money now. And the money is going to get tight. It's going to make this process much more combative—I may say—and less cooperative so I'm not as optimistic or naïve as I was six months ago, but I'm also not completely tainted yet. The process hasn't worked out. We'll see how SECDEF and everything weighs out, but it's a very dynamic environment. It's also—the processes haven't been around that long. We're still evolving—trying to get this right. I think there's been a lot of interest by the current team at OSD to making this work. And so I think we'll continue to evolve in the very near future through this QDR process as well as some of these other issues we discussed—see where the QDR may take us.

VADM Brown: Well, what I would say from my perspective—and I've been in the Pentagon too long—so I was there before capability portfolio management was thought of and watched it evolve and I believe that it's one of the most effective processes that we've put in place. The problem is we didn't do away with any processes. We added another one. And the intent of portfolio managers was that they would do the analysis across a portfolio of programs and look at gaps, and look at the IPLs [Integrated Priority Lists] that the COCOMs had submitted, and try to focus their portfolios to fill the gaps. And eliminate duplication. Unfortunately, we haven't. You know, as Bob said, this is a new process. It is still evolving and taking shape and we only have four portfolio managers. The plan was to have nine, and we really haven't figured out how to do cross-portfolio exchanges.

So I think there are still things to be worked out, and we need to figure out what processes this replaces. Because, you know, we just continue to build process upon process upon process, and you can't expect to deliver a capability in any timeframe that is useful unless you're building a ship. I mean, it works for ships, because it takes ten years to build a ship. But it doesn't work for an IT system. And so we need to make it more flexible and we need to try to structure it so it produces something that we can use in a short period of time rather than just being another process that we've added on in the Pentagon. But I do think in theory, portfolio management really is the best thing we've come up with in a long time and could do away with a lot of the other things that we waste time on.

RDML Hamby: If I could offer just from a COCOM perspective, we really like the idea of the portfolio management but we'd like to see it be faster. We would like to see it have teeth so it can be a more authoritative and effective about how we go about acquisition. We would like to see an acquisition landscape that allows it to be more agile and adaptive. And we would like to be able to know that when we go into the fight, we're going to have service systems that are all based off of that portfolio. We would rather have fewer systems than more, and we think this is a good way ahead.

VADM Mauney: Here's an interesting question. What's your vision for how we will conduct cyberspace operations in and through cyberspace 20 years from now, and what investments are most critical to getting us there?

VADM Brown: Well, I think addressing our command and control structure—how we define roles and responsibilities. I wish I did have a crystal ball, but we really have to address how do we bring the stove-piped Internets together and make it a Global Information Grid that we can understand?—that we understand the situational awareness of—so that we can make it an effective weapon and that we can defend it and that we can use it as a weapon in cyberspace. So I think we have to address those basic issues that each one of us mentioned earlier and lay the foundation, so that 20 years from now, they're still not wrestling with the same issues. One of my favorite sayings in the Pentagon is "There is no cat too flat to run back over again."

You know, if we could come up with an answer and stick to it, then 20 years from now we'll be well-positioned, I think, to operate in cyberspace. Otherwise, we're still going to be sitting here talking about the same things.

VADM Rondeau: So let me be somewhat provocative in that we sit up here as COCOMs, and as purveyors of the UCP and good order and discipline and all those kinds of things and we live in a hierarchical organization in a flat world. We're going to hear Rod Beckstrom tomorrow. At least in the context of this conference, I don't know. I come to you as a non-IT expert. I do come to you—as we all do—as people who have been around people and who lead and manage people. And I don't know if conceptually and philosophically we can talk about the empowerment of the individuals through

IT—and that means individual expert and his or her computer—and not talk about the awareness that we should give that person about their effect.

We at TRANSCOM have remarkable ability for self-awareness as an organization. Every hour, every minute, we are learning. We are a learning organization. And I don't know that in ten years, we would not be able to also transfer that to the learning individual and having utter, exquisite awareness by the organization and the individual as to how they effect or don't affect the entire GIG. And then it's all about belief and culture and behavior. We go back to General Chilton's two human factor pieces here and maybe three if you talk about capability.

So I think in ten years, we have organizations that are self-aware—self-learning—minute-by-minute—second-by-second—through automation and through people. And if you take in people, then you must have an ability to also make them learning and aware—minute-by-minute—second-by-second—act-by-act.

RDML Hamby: Sir, I think the question would be a great one to ask someone who was about 20 years younger than any of us on the panel. Where did that eighth grader go? We look at this from the world in which we grew up in, but we have got folks flowing into the military and into the departments and the agencies today that multi-task and think about information flow in a wholly different way than we do. And they will be the ones that are designing and directing and controlling our networks in the future.

I do think we'll reach a point where we're normalized to a degree. We are in a big period of transition today. We've gone through a number of years where we did look at the networks as administrative tools. Then we went through a few years—maybe a decade or so—where people were trying to sound the alarm for the need for investments in infrastructure basics as well as in information security. We've reached a point where there is critical mass of understanding and awareness of the importance of the networks, and I think we're ready to make a big investment into the networks to make them far more capable. And those networks are going to be shaped by these young people coming in today. I don't think I can really envision what that will look like, but I do imagine it will be far more fluid exchange of information—a far more focus on the information itself—and the networks will be looked [at] more as a highway system as opposed [to] the vehicles moving through them. And I think it's a very exciting time and I'm gratified to see folks like the three who were up here being recognized for their scholarships who are so talented and so incredibly imaginative on how they might make these networks work in the future. That perhaps we should diminish our level of anguish just a little bit. We're going to get there.

VADM Brown: Sounds like a two star talking to me.

RDML Hamby: Just one more to go.

VADM Mauney: I wrote down three numbers. The first is 2029. That's 20 years from now. I would submit that what we're buying in the Pentagon today will be around in 2029. And that's what our successors at that time will be using with the exception of information technology and our constructs for moving information in the information domain.

The second number is 1989, which is 20 years in the past. And then I wrote down—actually, the third number is 1969. So the difference between 1969 and '89—and then '89 to today—I think they are pretty different in terms of where we've come. So I, too, agree that the prediction for 2029 needs to be one our youngsters are thinking about and will drive us there.

But my impressions from visits around various regions in the last ten years is that we—America continues to produce absolutely eye-watering young people and they are doing some great work out there for our nation.

I would like to conclude the panel. Thank the members. I appreciate you coming today and also the time and energy you put into preparing for this discussion. I would like to thank the people who submitted questions. Again, [I wish] we had more time, although Keith I've got one I'll save for you. But it's more in your AOR there.

Anyway, again, thanks for your attention. I think we've got about five minutes before the next session.

Chapter 5

Left to right—Air Commodore Bob Judson, Brig Gen John Turnbull, Air Commodore Andrew Dowse, Mr. Mark Hall

International Perspectives

Moderator
Mr. Mark Hall, OSD/NII, DoD-CIO Chair, Director, Information Assurance Policy & Strategy

Panelists
1. Air Commodore Andrew Dowse, Australia, Director General, Integrated Capabilities Development
2. Air Commodore Bob Judson, United Kingdom, Director, Targeting and Information Operations
3. Brig Gen John Turnbull, Canada, Chief, Military Signals Intelligence (SIGINT)

Objective
Explore U.S. and Allied common interests in the cyberspace domain. These common interests range from the sharing of information on common threats to the freedom of action in cyberspace to an agreed upon set of norms and standards to operate in cyberspace.

Key Takeaways
- Information sharing is greatest challenge across the international boundaries.
- Building partnerships at all levels pivotal to cooperation/operation in this "global domain." We cannot "stove pipe" on an international scale.
- International standards key—much of our allies' information ends up on our networks and vice versa. We need to protect this system of systems to ensure our "global" network is protected.
- Networking is vital. USSTRATCOM presently has LNO's from the UK, AUS, DEN, and will add CAN in fall '09. Now is the time to encourage an influx of international participation. We need to get the experience to the younger generation of future leaders.
- The retention of cyber individuals is poor and needs improving. This industry is willing to pay "cyber" experts high salaries/benefits. It's hard in today's economy to ask someone to work for much less.
- In support of information sharing, combined exercises and training across the services and with other nations a must.
- We need reliable contacts and bilateral exchanges to ensure that not only is information flowing between the militaries, but also across civilian/national organizations and leadership.
- All panelists agreed with the idea of a "central" authority for analyzing cyber events.
- In order for a central clearing house to work, we need an internationally agreed upon set of rules and norms for operating on the Internet, GIG and other network systems.
- Ensure resources budgeted to build capable personnel, trained to use our latest hardware/software as our "cyber" force.

Panel Discussions
A complete transcript of the discussions is unavailable. A brief summary is provided below.

Mr. Hall opened the panel discussions providing a little perspective from OSD in what they're doing and where they're headed. He used the ongoing cyber training and exercise events hosted by the University of Nebraska at Omaha as a great example of bringing together 20+ nations to deal with the evolving cyber challenges.

Mr. Hall mentioned how ongoing activities to build partner capacity and developing international standards and norms is critical to our cyber efforts here in the U.S. Mr. Hall states that we don't fight alone any longer and if we're going to connect our networks together—give our international partners access to our networks—share battlefield information and strategic information with them, then we need to address how we do that. He also mentioned that challenge of trust. He mentioned the multiple tethers that exist between our countries in the cyber area (*e.g.,* the intelligence

community tether, the military tether, the law enforcement tether). Mr. Hall lamented the challenge we face with information sharing. He opined that we have to write-to-release.

Air Commodore Dowse opened his comments discussing the nature of the defense environment within Australia, briefly discussed how Australia's CND efforts are structured, and closed his comments by highlighting some of the future challenges for Australia in the cyber area.

Brig Gen Turnbull opened his comments by highlighting how Canada is organized at the government level to deal with cyber. He mentioned that Canada's network itself is similar to Australia's and highlighted that their network has a single operational authority and a single technical authority. Brig Gen Turnbull stated that Canada has a totally integrated power and telecommunications grid so they are very conscious of being seen to be a trustworthy partner on the continent and in keeping our own IT infrastructure secure. He also highlighted that the Canadian government is also very concerned about the privacy of its citizens.

Air Commodore Judson opened his comments by discussing the organizations in the UK who deal with cyber and the way they coordinate cyber activities. He followed this some thoughts on how the UK looks at the cyber problem and closed with some thoughts and challenges from a UK perspective.

After opening comments by each panel member, questions were submitted by the audience and answered by the panel.

Chapter 6

Speaker—LTG Keith Alexander, Director, National Security Agency.

Integration and Synchronization of DoD-IC Cyberspace Operations

Speaker: *LTG Keith Alexander, Director, National Security Agency*

General Chilton, ladies and gentlemen, it's a privilege and honor to be here today.

First, there's a few things that I do want to go over. What I want to talk about a little bit, I'm going to go back in the history, and I know you don't want to hear history from an engineer. But I'm going to give you my version of history, and there will be formula in it.

First, let's talk a little bit about what happened in World War II and how we got to where we are today because I think our predecessors, the greatest generation, have helped us set up the United States where it is today, and that's a good thing. And if you think back on it, the predecessors that set up NSA did a few things. They broke the Japanese codes, red and purple, and that helped us win the war in the Pacific. And they worked with the Brits and the Poles, and they broke the German ENIGMA code, and it's interesting. We have a copy of that downstairs, I understand, a working copy, or will have—we have one in our museum. And if you look at it, the combinations that you would get on that are 3×10^{114}. I'm not a real good mathematician, but I understand that's a big number. And we broke it. And the reason I bring up those two things, we broke those two codes and had great success.

On the other side, we had SIGABA and SIGSALY, the ones that would defend our networks. Think of it as the GNO portion of this. The Germans didn't break that nor did the Japanese and that gave us an incredible leverage in the war, huge. And so when you think about that, the mission that we have today hasn't really changed. The environment we are in has changed significantly.

So what's STRATCOM's role in cyberspace and bringing all of those mission elements together in DoD and then partnering with the intelligence community and partnering with DHS and potentially the commercial industry, is a huge change. Because our military operations back in World War II were point to point. These were pretty easy. When you think about it, our world was pretty straightforward. Defend this circuit, defend this here. Think about what's happening on the network today. All of these devices—it's really kind of interesting. I had—I have four daughters, and one of the people said, you know, you have to help repopulate, regenerate. I'm doing my part. (laughter) Because they have—I have ten grandchildren and now—oh, cross that out. 11. We had one last night. Oh, I didn't have anything to do with it. We're still proud of them. Actually it was kind of nice. They named him—you know, I have four daughters. Our first grandchildren were all granddaughters. And everybody said aren't you going to get any grandsons. Well, the next four were grandsons, and they've named this one after the two grandfathers, and I thought that was huge.

When you think about it, these kids, and they go from one to seven, they have their little iPods. They are digitally connected. They talk on the phone all of the time. They send text messages; we were

getting text messages about two every minute last night. I think I might have a larger family than I thought. (laughter) They were sending pictures. We're connected. It's huge.

America's business is done on that network. Our Armed Forces fight on that network. Our government fights on that network. Great capabilities, tremendous for warfighters. And today, we haven't been challenged on that network. We haven't been challenged in a warfighting zone on that network, I'll correct that, because I think as General Chilton brought out this morning, we are being exploited on those networks. So one of the great things I think we bring together is a mountain of partnerships we have with GNO and NW, under STRAT.

STRAT with all of the pieces brought to it, it's huge. It takes a team to fight on that network. And that's some of the stuff I would like to talk about, how are we going to form that team, where do we support that team, how do we support John and Carol in defending our network. What's the way to do that? Because if you jump back in the old days, you had the guys who broke the code, they get really good at it. And they were hugely successful. And the guys who make the code, what we found is when they partner together, the defense gets a heck of a lot better.

So how do we help our defense and continue that great offensive capability that we have? There are a number of things that we've got to think about. Let me just hit some of the threat things. I think people have talked today about Latvia, Lithuania, Georgia, some of U.S. Banks that have been exploited or attacked, all in the span of a couple years, shows that people are starting to use network tools that can do distributed denial of service attacks and more into our networks. It's huge.

If you go on to the commercial side, Heartland Payment Services, many of you have heard of that, were exploited back in October/November time period. They lost 100 million plus personal credit cards, our stuff, names, credit cards, and all of that. Huge. Millions of dollars worth of stuff!

Not only did they lose, then they got fined, and then Visa decertified them. And then their stock dropped from 15 to 5. That's a definition of a bad day, isn't it? (laughter) That had nothing to do with the Wall Street picture that you're going through today. That was separate. So when you think about it that's where industry is at and they are getting hammered on their networks.

If you think where GNO is and where we're trying to defend our networks, we have this problem, and then we have these exploit capabilities, and we're not organized. The conduct, the culture, the capabilities that General Chilton talked about are the things that we've really got to look at.

What's that mean for us? And I think Sherri and some of the folks on John's panel this morning talked briefly about real-time situational awareness. You see, we're thinking about this as Information Assurance over here and defending our networks, and we're thinking about exploit over here and attacking theirs. And what we need to be thinking about is the team, that's us, working together for the good of everyone. And we've got to do it at network speed. And we don't operate on our networks at network speed. We don't have the visibility, too many firewalls. You can't see them all. And as a consequence, John's job is incredibly more difficult.

And if you can't see it, you can't defend it. A big gap, an exploitation gap, because if he can't see it to defend it, an adversary can get in there and exploit it and he won't know about it for a while, similar to the Heartland Payment problem. Our problem. And in the future, these things happen at network speed.

So what we've got to do and what we're in the process of doing is first you've got to be able to see this stuff at network speed. You have to have real time situational awareness. This is like missile defense. If you think about it, we would never have the guys who are shooting missiles over here and the radars over here disconnected for missile intercept. You'd say, "They have got to be together because they have got to work together." Our network defense, our network exploit, our network attack all work on that same network that's converged. One network. It's not three, it's one. We all operate on that network.

And I think some of the biggest coups that we've had in the last four or five months is because of that great partnership that we have working together. Things—unfortunately we can't go into them here in an unclassified level, but what we can say is the ability to tip and queue, between the defense, the exploit, is huge.

How are you going to do real time attribution? How are you going to do real time litigation? How are you going to tip and queue that? And the answer is first you've got to see it, you've got to have the rule sets made, and you've got to have your team forward.

For the military, the Defense Department, the STRATCOM group that's working this, that means that what we've got to do is get really good about seamlessly working these networks and operating them at network speeds. That means that our defense has to be able to say, "Help." Something hit me here. Tell me what it is, and can you turn it off.

That gets to that question, "When does a network exploit become a network attack?" I think that was the real question that Van had. And so these are going to be issues that we're going to have to wrestle with a defensive measure, called CND-RA, response actions, which allow us to stop somebody from attacking us.

Now, you can play this scenario out and say, "What if it's a distributed denial of service attack, and we take one of those new bot-nets and we throw that against the Defense Department?" Is it a network attack if we climb in there and stop it? And the answer is difficult. Beats me. That's one of the ones we would like to know.

No, actually when you get to it these are the kinds of questions that you face because as you see, there is not a legal framework that somebody has thought up for this new environment. Of course, you have the right for self-defense. You say, "Well, actually, this guy is going through 15 hops to get to John." You say, "Well, yes, you do" and you can turn off parts of it and as long as you don't break his equipment, that's probably okay and the lawyers will walk two parts of it. Okay, we can justify A, B, and C, that's where you go from real time to less than real time, legal opinion will be rendered at this point.

We've got to have those rule sets set up, because when you think about it, that distributed denial-of-service attack cannot be stopped at John and Carol's front door. It's on the network, the global network. We have to see that global network, and that brings up a whole host of opportunities for us.

You know, we've talked a little bit about the military, but the military and industry, DoD, DHS is going to have to work together on this. And the reason is that we don't have all of the smart folks, we need to partner. And in this area that's going to be huge.

The other part of that partnership is going to be with our allies. For NSA, we have the 5-eyes, that's the Brits, the Canadians, the Australians and the New Zealanders. I know they are throwing a party tonight. Where is the party going to be? Well, we'll go to that later, okay? (laughter)

A huge capability that sprung on to that story was ENIGMA because they are the ones that partnered with us and they still partner with us today. Why is that important to us, though, and to not only our military because we're going to fight with them, ENIGMA, but also our Nation. And the answer is it gives us defense and depth. It gives us a defense and depth. And by that I mean if you think about the global grid and instead of trying to just position your sensors at your front gate and say I need to seamlessly see the stuff that may be of an interest to you and you see stuff that may be an interest to them. Our partnerships on the network are going to be key to our success. Absolutely key.

And so what we have, you know, the real good part about network operations and where we are and where we are going, is all about teamwork. How do we create the team? The STRATCOM team that does the defend, the exploit, the attack in support of DoD, the DNI team that does our network collection. And those two teams are going to have to help DHS in their mission.

And I'd just—just a paid political announcement. I know there was some press a few weeks ago before NSA wanting to take over the world. Some of you know I really am lazy and some of you are really good friends of mine saying, "Yeah, we know that." DSS has a tough job running the rest of the .gov networks. That's going to be really hard, really hard. We don't want to work that hard. We want them—and well, technically.

And I believe they are the right ones to partner with industry. The front end port. Yes, we're going to have relationships with industry. The military is going to have relationships with industry, but the front end, especially for critical infrastructure, that's a DHS mission. That's not a NSA nor is it yet a STRATCOM mission, nor will I think it will be. So I just put that on the table because somebody said you hadn't said that emphatically from your NSA perspective. So I just want to make that clear. DHS doesn't have the technical capability to do it. It's just standing up. And so I think the STRATCOM team, the Intel community team is a team they can lean on for that expertise. And that's our role. I think that's our appropriate role. Now, that's my opinion on it. And I'm putting that out there because I do think there's an awful lot that we have to do.

So let me review a few things here and then I'll open it up for questions. Is that what I'm supposed to do? (laughter) First, you know, we have had a lot of operational time over the last, well, since October roughly 24th at 1630, to work together on real world events. And I'll tell you, it's a privilege and honor to be the Director of NSA. We've got great people. It's also a great privilege to work with GNO, DISA, and STRATCOM in helping to work on our networks, it really has, because I think the operations that we've had have allowed us to take leaps that we could never have done before.

And so at the moment, the operational necessities have driven us to do things that we have never done before. That team has really come together, and it's a great team making great strides. I had an opportunity to sit in as a number of these players from GNO, from NTOC, from ANO, Advanced Network Operations, and from our Signals Intelligence Directorate and a couple of other groups. We were talking about "conficker", not "cottonpicker", that's what I thought. (laughter) No, "conficker", that's that new virus. And they had some really huge solutions, some great capabilities, that go way beyond what people are thinking about that would really improve the security of our government, military, IC networks, and something—and the types of things that we ought to be working together on. It was huge. So we have a great team that's formed and it's a privilege and honor for me to work with them.

The second part I can mention—what DoD is doing, STRATCOM leadership here in the cyber community is huge. We've moved up. The Intel community is helping out on that. I think now with Dr. Lute on board, you'll see DHS start to make moves. You'll see a partnership there and I think it's essentially the teamwork that we talked about.

And then finally, industry. We have to have partnership with industry. How do we do antivirus software and signatures faster than we've done before? How do we do that threat sharing? That's going to be huge for all of us because there's a lot that the government has. It's classified that we can't share with industry today. We've got to figure out our way through that.

How do we get on the networks and do tipping and queuing and, what's the government's responsibility to tip and queue DHS and critical infrastructure that they are going to be attacked, and what's the government's responsibility to defend it? Those are things that we're going to have to work our way through.

And finally, I would just say our allies. We already have a great working relationship with the Brits, the Canadians, and Australians, New Zealand, and much of the architecture I've talked about they are helping us put together so we have a global capability that we can leverage for our common defense and I think that's a huge step forward.

So with that, let me open it up to questions.

Question: As we likely stand up a sub-unified command to focus on cyber, what roles does a commander retain and what gets subordinated to the subcommand?

We have to do better than the USFK model, General Chilton. No, I'm just kidding. Well, that solves that one. (laughter) Yes, the answer is yes. Of course. It's actually from Tom Gregory, Deputy J86 USSTRATCOM. Was I not supposed to read that? (laughter)

You know I used to watch with my kids, Annie, 132 times. (laughter)

Okay. We're working our way through that right now. General Chilton is giving us guidance on that. Some of the stuff we're working on what is the right command control relationships, how do we keep moving it. We understand we're going to have to keep doing that together, and I think that's proceeding along pretty good and you hit it pretty close so I'll drive on to that's next.

Question: Do you have these young people on your 20 year, 10 year, 15, 100 year plans, are you national leaders working together to do this well?

I don't know which young people you're referring to. I have some of the young people on our plan. I don't know if they've signed up for the hundred year plan.

But really I really don't know that. I'll have to go back and ask them because this new generation signs up for five years and after that we will see.

Let me give you a serious part about that. We have a great recruitment capability at NSA. I can tell you that right now. We have something called the Director's Summer Program. What you may not know is we have the world center of gravity for crypt-mathematicians at NSA. That's why they made me memorize that formula. (laughter) You've got to get all of these things down and we have Mukasey

come in there; he was the 81st attorney general. So all of this stuff. You've got to get it down or you're not going to stay long. We do have a great recruitment program with that Director's Summer Program. We get the top mathematicians in our country from Harvard, Yale, Princeton, and Berkeley. The best universities, the best math.

We get—they come in for the summer programs and get their clearance. We hire 75 percent of them, and they stay with us. They like the job. We're doing well and retention, we're doing really good on retaining. I think some of our people are on the hundred year plan. Although I don't know that anyone is a hundred years old and we're not allowed to ask that. (laughter)

Next question: Is being DIR a case of the fox guarding the hen house regarding Intel gain/loss?

It depends on your perspective. The biggest proponent for NW in the Intel gain/loss for the attack has been NSA. And the reason is, is that I don't buy the paradigm about Intel gain/loss, I would say if it has an operational perspective and it will help the warfighters, we're going to do it and we'll figure out how to get the Intel back. Now, there are some times I'm sure where that doesn't make sense, and so we'll work our way through that.

There is always going to be an Intel gain/loss equation. I think more importantly what you really need for NW is if we're going to do an attack is what are the equities and, who knows those equities and who can explain it.

Having NW at NSA we were talking to, General Vautrinot is around here, she had to—She'll tell you and her folks will tell you that one of the great things is they can go to the groups. What we call offices of primary interest, like our China shop or others to see what "WII's" are on the networks, what we're collecting and talk to them so if you talk to the people in the NW J2 shop that he will say we go down into that office of primary interest, see where we're going, work it together. We have not yet had a disagreement with that, in the three years that I've been there. Not once.

Now, we have had disagreements with other agencies, but NSA and NW have always been on board, in-sync and the objective was always going after it. So I think that was huge.

Question: Do we need a cyber czar?

I think that's more European or Russian. How about cyber prince? (laughter) You know, or Exec. Because cyber is—you know, it's got a 'Z' in it or sometimes an 'S'. I think, well, I don't know. Here's my thoughts. I for sure don't want to be the cyber czar. I think the nation needs somebody in the White House who's going to do policy on cyberspace that hits on many of the issues we've talked about.

I think our role is to operate in cyberspace. We need a cyber czar down there who can help us get the policies, the funding, the infrastructure and things we need. We need somebody good at that. I have some great ideas. None of those people would launch forward to that. I guess they can't pay them as much as they were used to. Might be an industry thing. (laughter)

I think where we should be, what we the military and the Intel needs, is great operational capability. I think those two must be separate. I think the nation does need somebody in the White House working at some level that can talk in cyberspace that understands it.

One of the really tough issues in this area is technically really difficult. It's not something that you just walk in and say, "Hey, we were talking about pico jules per bit op". And I can remember one of my friends—we were briefing this to one. Guys and he said I can't believe you folks were using that. They were serious; we were actually worried about power.

We need people that understand cyberspace, that can help us build the policy, and that person I think needs to be in the White House and I think needs to be at a level appropriate enough to pull their weight. I don't have any other fixed opinion on that.

Question: Where do you see America with respect to cyber security ten years from now?

I think the U.S. and our allies are going to do an awful lot in security. And our adversaries are going to do a lot and exploit. And we're going to do a lot and exploit. It's not going to change. We'll get better on the defense. We'll get better on the offense. They will get better on the defense, and they'll get better on the offense. And what we want to make sure that we stay ahead in that

equation. That's where I think we're really going. I don't think there's a silver bullet that you can fire today that would change everything.

There are some things that we can really fix right now that kind of get back to the culture, the conduct, the capability.

You know, we talk about some things, about best practices on the network and ensuring we operate our networks like that. Protect, defend, hunt on your network, a gold standard on your networks, and some way of tipping back and forth between the exploit. That will jump us up to the next level. And once we get to that level, it's going to be like where we were in World War II. We'll have a strategic advantage, but it will dissipate if we are not taking the next step and the next step. And that's where I think we need to go.

The other part is if you think we can forecast out ten years in the IT area, I'm in a different area. We do spins—it's kind of humorous, and I know the folks at NSA have a different view of our spins. We're on spin 15. We do a spin every quarter, a technical change in our capabilities in an upgrade. It's a huge way of spinning your infrastructure and your capabilities very quickly, very difficult. It's a leadership technique built upon the premise that it's not hard if you don't have to do it. That's my—I thought that was good. That was a joke, I'm sorry. (laughter)

So when you think about that, this is a fast-moving area. If we thought three years ago we could build a cloud infrastructure that could handle the speed and velocity that we're in today, everybody at NSA would have said no way. And we've passed our expectations already. I'm sure our adversaries are doing the same thing.

So in the IT area, it is moving at a rapid pace. It really is. I think we can see clearly out three to five years. Beyond that, things like a quantum computer start to bump up there. Is it coming in five years or is it in 25 years? And when that hits, that's a game changer. So things like that are there that we're going to have to look at.

Let me just summarize with a few things.

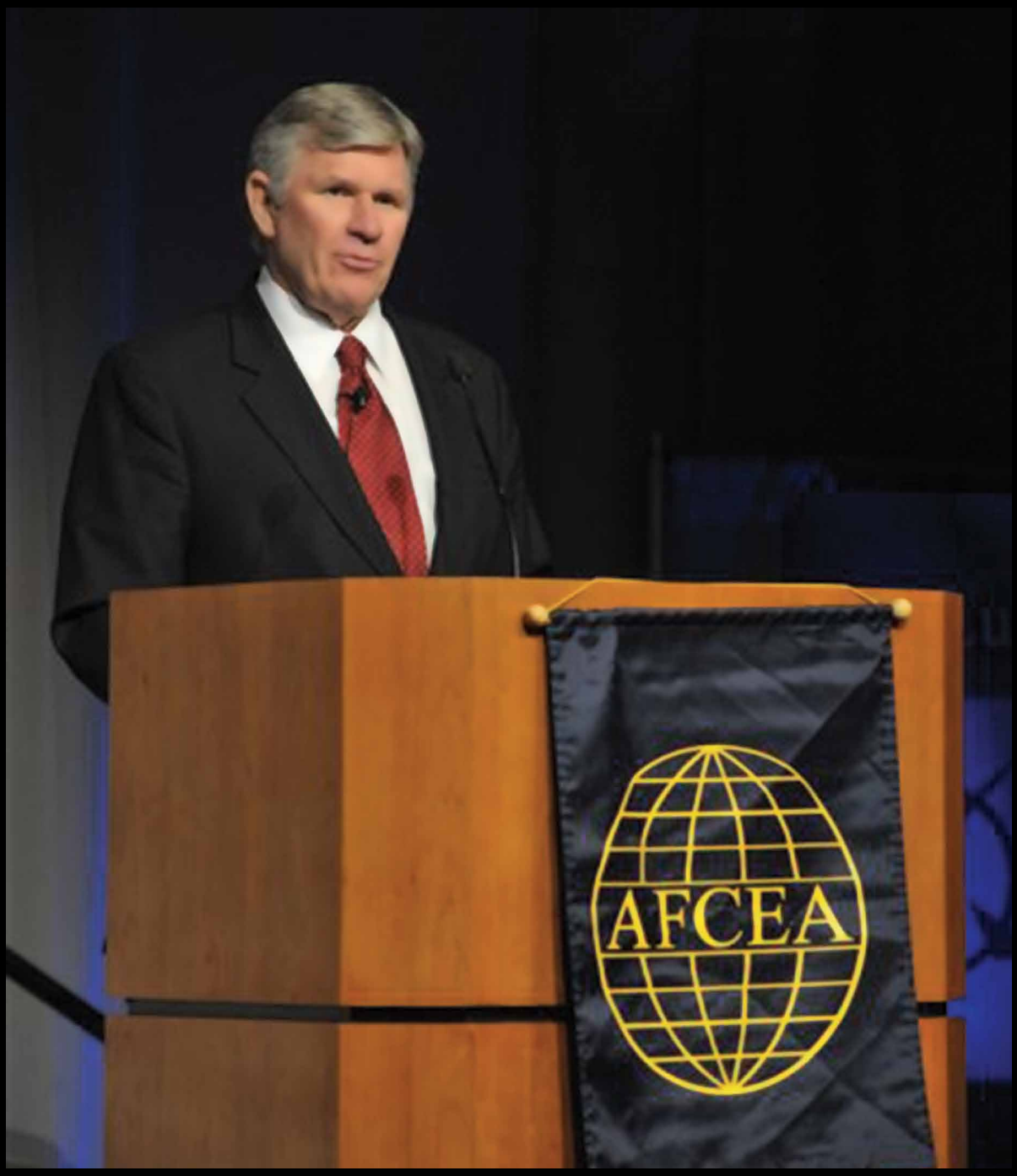
You know, working in cyberspace is a lot of fun. You know, one of the things, and I said Sherri and the folks down in NW and GNO and I get to go down there and other places, it is a lot of fun to work in cyberspace; it really is because we get to do really neat stuff. And unfortunately we can't talk about it in non-classified forum.

But we do get to do neat things. We have great people. Our military and civilians are absolutely superb. We have a growing, great team. And I think what DoD and the Intel community has is a team that DHS can lean on as they get started running down that same road.

The other key thing is it's a great team for our allies. And for me, it has been a great privilege and honor to be part of that team and to get to work with some great people that we have. And I see the Sergeant Major over there he would kick my butt if I didn't bring that up. (laughter)

So it is, it's a lot of fun. It's going fast. I think we as warfighters, we need to think now about how are we going to leverage this for the good of our nation; what's that mean for us. We do—I know STRATCOM gets all of the Capstone courses and we get them, and talking to them about what could be, what should be, is huge. And that's how we've got to think in this area. So with that, thank you, thank you very much folks. (applause)

Chapter 7



Speaker—Lt Gen (ret) Harry Raduege, Deloitte Center for Network Innovation

Securing Cyberspace for the 44th Presidency

Speaker
Lt Gen (ret) Harry Raduege,
Deloitte Center for Network Innovation

Objective
Provide the audience background information on the Center for Strategic and International Studies (CSIS) Commission and their recommendations to the 44th Presidency for securing cyberspace.

Key Takeaways
- The effort to improve Cybersecurity offers the opportunity to rethink how government & industry operate and to build collaboration across organizational boundaries
- The goal should not be the best defense, but government & industry that can:
  - Securely take full advantage of Cyberspace
  - Enable and assure essential services in Cyberspace
  - Create opportunities for collaboration, growth, & national advantage

Speaker Discussions
You know, many in this room saw this event coming over the years. However, they didn't know exactly how it was going to evolve or how this cyberspace mission area was going to be worked. And I think it's very, very interesting. The fact that it has now become a national priority—and it's even being worked by the President of the United States—which just shows the tremendous significance in national importance of this key mission area.

I want to thank General Chilton, U.S. Strategic Command and AFCEA for putting together this first in a series of cyberspace symposia. The fact that there are 1500 people that come to an initial event of this magnitude speaks a lot about the national significance of this topic and the passion that many of you have been looking for in this area for quite some time.

Now, I want to say something about Admiral Steve Oswald. We worked together when he was with the JTF for computer network defense—which then moved into computer network operations. And so he goes back to the days of what we used to call the "Great Get Along" in this business. Because there were no command lines in the Department of Defense—and I know this really strikes General Chilton because the Great Get Along—those days have to be long gone—because this is all about working together—about relationships that really work and addressing this issue of cyberspace. So Admiral Oswald was there with me, with us in the early days.

Yesterday I think I heard one of the most stirring speeches I have ever heard and it was by General Chilton. And I think it is a speech that we really need to read and re-read, and I commend you to do that because it certainly captures a great leader's perspective—a commander's perspective on the fact that this cyberspace is the commander's domain and needs to be addressed like that.

General Chilton also noted yesterday that the computer that gets the space shuttle in and out of orbit is still working on 256K of memory. And you know, I knew General Chilton and Admiral Oswald were great leaders, magnificent individuals and patriots, but I had no idea that getting in and out of orbit, they were doing so much brilliant work, working those rudder pedals and that stick, getting that shuttle to go in and out, but with 256K. They must have had a big part in steering that shuttle in and out of orbit.

Today's subject—and I appreciate the opportunity to speak with you—sort of takes this area of cyberspace and what we've been talking about in cybersecurity to a different level. And so I hope that this presentation will stretch our minds a little bit into where we are going with this important area as far as a national priority.

Yesterday, General Chilton talked about the historical perspective of his involvement, and he talked about Second Lieutenant Chilton back in 1893 and what he would have witnessed at the military academy and the kind of things he would have been taught. I can't go back quite to 1893 with this, but I would like to go back to 1997, '98 timeframe when General Dick Meyers, who was the Commander of United States Space Command, went to his first Combatant Commander Conference at the Pentagon. And the Deputy Secretary of Defense at that time was Dr. John Hamry. He sent General Meyers back with a task of putting

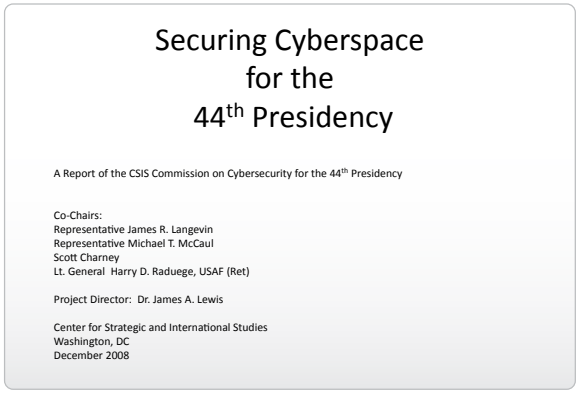
together a computer network defense program for the Department of Defense, and also started to talk about a computer network attack capability because the Deputy Secretary of Defense had been thinking about how important this mission area was and he wanted to have a Combatant Commander in charge of developing this capability for our nation.

So General Meyers came back and we went to work. First with the computer network defense areas of responsibilities, and soon in 1998, we stood up the Joint Task Force for Computer Network Defense (CND). Later Admiral Oswald came to work with the CND and actually took it to the computer network operations, which included the attack and defense missions.

And then since that time, we have developed the JTF for Global Network Operations, which many people talked about yesterday and the Commander, Lieutenant General Pollett, is here with us today and is dual-hatted as the DISA Director.

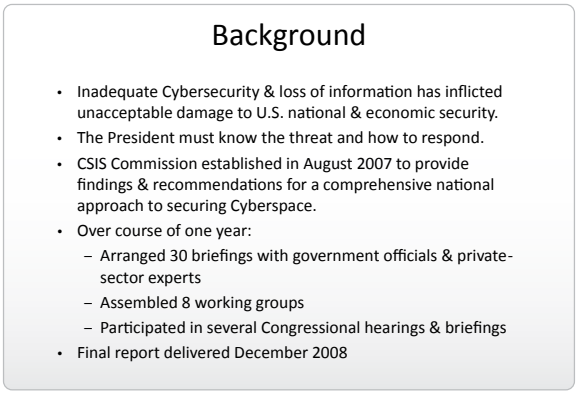
In 2004, when we stood up that JTF for Global Network Operations, I had the privilege of bringing Dr. Hamry back to the JTF-GNO and showing him what his vision from seven years prior had developed. And if you've been at the JTF-GNO, you see how the Department of Defense is in good hands with the Global Information Grid being managed, operated and defended, and network controlled from that very important position.

In 2007, Dr. Hamry, still believing in the importance of cyberspace, computer network defense, computer network operations, attack and those type mission areas, went to the Congress because the two individuals here that I've listed on the front of this chart—Representative Jim Langevin and Representative Michael McCaul—were subcommittee chairmen of the Cybersecurity



Subcommittee in the Congress. And Dr. Hamry talked with them because they had initiated the idea of putting together a special commission to study this all important mission area.

I note on this first chart that we have several co-chairs, one of which talked with you here yesterday at the luncheon presentation—Scott Charney.



Now, here's the brief background of what this commission was all about. We started from the perspective that we are taking a lot of damage in our nation today. We've got inadequate cybersecurity, and we're having unacceptable damage from the U.S. national perspective and from our economic security perspectives. We realized that the President was going to have to be engaged with this important area—was going to have to realize the threat and how to respond. And of course we targeted this for the 44th Presidency not knowing, when we started this study, who the President was going to be or what their background was going to be. But we felt like this was important enough that we needed to make our presence known through this commission.

This commission was established in late 2007, and we established it with the goal of developing findings and recommendations and presenting—putting together a very comprehensive national approach to securing cyberspace.

So over the course of the entire year of 2008, we arranged for a number of briefings—we broke into a number of working groups—and we participated in several Congressional hearings and presentations.

We were told to be bold. In the past there had been a number of commissions and reports that were coordinated with a number of outside activities prior to being published and they seem to get watered

down. But we were told to publish our report—to be bold in our findings—and to get into specifics.

So here's the four co-chairs. I was privileged to serve as I mentioned with the two congressional members and also Scott Charney from Microsoft, who presented yesterday. And I would just like to thank also Deloitte for allowing me to participate for a whole year on this commission, and also I'm sure Scott Charney believes the same way with the involvement and support he got from Microsoft, especially with him traveling all of the way across the United States to attend most of our meetings.

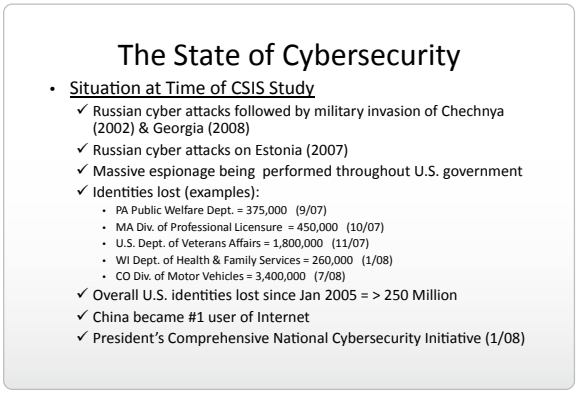
We had a great project director in Dr. James Lewis from CSIS. We had 33 or so experts. We called a lot of other people in. And as you review the names of the individuals we had on this commission, you will see the kind of healthy debate, just from the knowledge of these people—where they have worked—what they have stood for in their public and private lives. We had lots of diverse opinions, exactly what General Chilton is looking for from this type of a setting here today, and the topics that we got into with this number of commission members, as you might imagine, were trivia to some, and they were critical to other people. So we had a whole diversified approach to our study.

Now, I wanted to just put into perspective, for posterity's stake, the situation at the time of this CSIS study that we put together. The Russians had cyber attacks followed by military invasion of Chechnya, and into Georgia. The Russian cyber attacks that were conducted in Estonia had already been in the books and we had learned from that. Massive espionage was being conducted throughout the United States Government by others outside our borders. And just to put this into perspective from the national involvement, I just listed a few things that I picked up from the news back in those days—of the identities that have been lost—and take a look at this whole series of identities in these—this multitude of areas. You know—in our states—in our departments—across all functional areas that are very, very critically important to the economic stability and prosperity of our nation—I think this really underlines the fact that this is a federal, state, and local problem. It's a problem that stretches across industry. It's a problem that stretches all of the way into our personal lives and is very real for all of us.

Overall, U.S. identities lost—over 250 million—which is staggering. And I think this is an interesting fact—the fact that China has now taken over as the number one user of the Internet. Now it's estimated that there are 220 plus million users in China, and that's out of a population of 1.3 billion people. The United States has about 216 million users out of a population of about 300 million.

Now when you think about that, and that China has now taken over as the number one user of the Internet, they've done that with about 17 percent of their population, and we're a little over 70 percent of our population with those kinds of numbers. So those give you the kind of ideas of projections and what we're looking at for the future.

And, of course, President Bush had kicked off the comprehensive national cybersecurity initiative in January 2008—right about the time that we were starting to really gear up strong with our commission—and we took that into full consideration during our commission study of the entire year.



Now here are the major findings. As I said, our commission was going to have findings and recommendations broken into these three areas.

Major Findings

- Cybersecurity – now a major national security problem for the U.S.
- Decisions & actions must respect privacy & civil liberties.
- Only a comprehensive national security strategy that embraces both the domestic & international aspects of Cybersecurity will make us more secure.

Cybersecurity now being recognized as a national security problem for the United States.

The second point is one we really wanted to make sure was up front in our report because we have to protect, defend, and comply with the U.S. Constitution in protecting and respecting privacy and civil liberties of our nation's population. We wanted to make that one of our findings so it was in print and not just understood.

And then the last finding being—only a comprehensive national security strategy that actually reaches into the domestic and outside the international aspects of cybersecurity will make us truly secure.

Now, here's the summary of the recommendations. And what I've done—where you see an actual checkmark is pretty much the recommendation—but I've grouped the recommendations for brevity here today in the time we have remaining into categories.

Summary of Recommendations

- Create a Comprehensive National Security Strategy for Cyberspace
  - ✓ President to state that Cyberspace is a vital national asset
  - ✓ President to direct NSC to create comprehensive national security strategy for Cyberspace
  - ✓ U.S. to open broad national community discussion on how best to secure Cyberspace
- Organize for Cybersecurity
  - ✓ President to appoint an Assistant for Cyberspace
  - ✓ Establish a new National Office of Cyberspace (NOC)
  - ✓ Create 3 new advisory groups

So the first category I've described here as creating this comprehensive national security strategy for cyberspace, and the President really stating that cyberspace is a vital national asset. And I think President Obama has already done that, not only as a candidate but also has done so in office.

And so what this means, then, with the President establishing that state is that the U.S. will protect our networks using all the instruments of national power.

And that gets to the second bullet here, and the President is directing the National Security Council to create this comprehensive national security strategy for cyberspace and use all the tools of U.S. power, and that gets into international engagement and diplomacy, military planning and doctrine, economic policy and the intelligence and law enforcement communities.

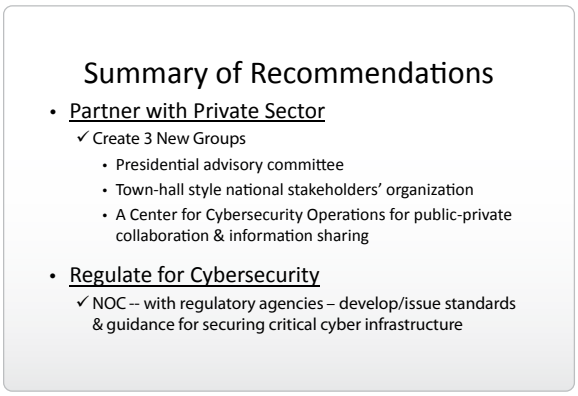
And in this area with the National Security Council, we could see that we need to be at the level of policy development—oversight of the overall program throughout the United States—and also to have a balanced program across all entities that are contributing—because I talked to someone who had worked at very high levels in our government before and had to bring together a lot of national assets and national capabilities, and one of the biggest problems he had as far as providing oversight was the fact that we got out of balance with the different places. So somebody would put a lot of emphasis—other people wouldn't—but it needs to be a balanced program for our overall nation's survival.

Another sub-category was to organize for cybersecurity. And there we recommended that the President appoint an assistant for cyberspace. In fact, President Obama has been talking about that now for some time. And I think after a special report, an assessment, I think we may be seeing something along those lines, an announcement from the White House.

We also recommended to put the teeth into this and so that you just don't have one individual working by him or herself, that we establish some sort of an office that would—we called it, for lack of anything else—a National Office of Cyberspace, a NOC. And it could be named anything, but there had to be some sort of organization of people who could support this assistant for cyberspace and to provide the policy oversight and the balance program.

And we also recommended putting together three new advisory groups.

The next area of our recommendations was to partner with the private sector. And this is really a step forward, I think. Some of the people who were talking yesterday talked about, what do you do in establishing a better public-private partnership? And we said we could do three things with these three groups.



A presidential advisory committee—and this would be created really as we envisioned, under the Federal Advisory Committee Act with key representatives from key cyber infrastructures across the nation.

Town-hall style stake holders meetings—and this would be a platform really for education and awareness across the board and across our nation.

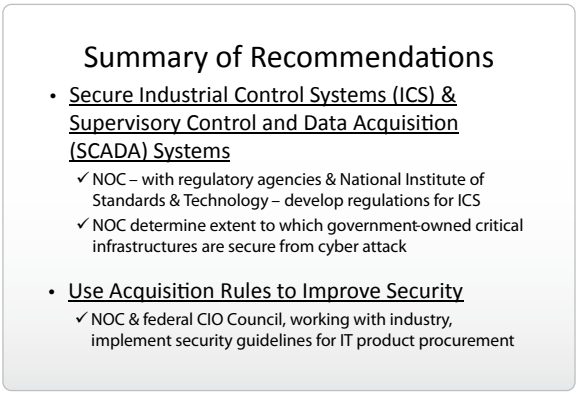
Also a Center for Cybersecurity Operations—and we envisioned this as being the actual place where the public-private collaboration and information sharing could take place. This would be an organization that we saw that could become something that would build trust and really would establish more trusted collaboration within the public-private domain.

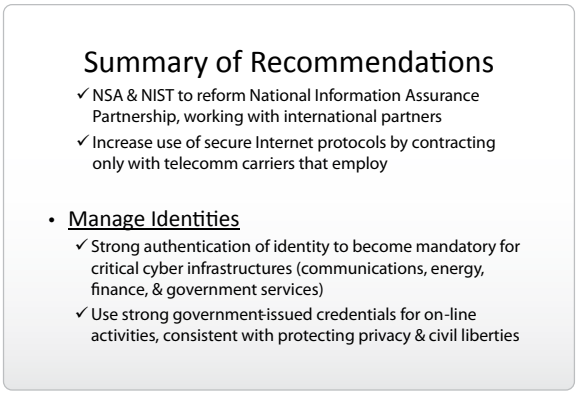
We also in our report recommended regulating for cybersecurity. And there we really pointed to the model of Y2K where we blended voluntary action along with regulation. As you recall, our government mandated SEC regulations for publicly-traded companies to actually report steps taken to secure their networks from disruption. And this was something that worked very, very well and it was a prefect blend, I think—for those of us who recall that involvement with Y2K—a blending of voluntary action with actual government regulation and requirements.

We also recommended in our report securing our industrial control systems and SCADA systems. And this would be done through this operations center for cybersecurity with regulatory agencies, and the National Institute of Standards and Technology, and developing these regulations. And we saw there an opportunity to include standard certification matrix and standard and enforceable standards.

The NOC would also determine the extent to which government-owned critical infrastructure are secure from cyber attack and would work with the appropriate agencies to secure them.

Yesterday folks talked on the panel about acquisition rules to improve security and, in fact, our commission also addressed that fact—of working with the federal CIO council on industry and implementing security guidelines. We see there an opportunity to develop and incorporate standard security guidelines, settings, specifications, into a government-wide contracting strategies. And we see implementing guidelines and standards through appropriate policy and standards of organizations taking place.





Also we noted that the NSA and the NIST could reform the National Information Assurance Partnership. And there, the NIAP-common criteria is time consuming and focuses on individual security features instead of the overall product. And we saw that we could reform common criteria that would improve cybersecurity globally in this regard. And also to increase the use of secure Internet protocols by contracting only with telecom carriers that employ these things. And of course, this would be federal acquisition that could actually drive cybersecurity, using this acquisition process to our advantage.

We made recommendations about managing identities. We felt like strong authentication was needed—it was mandatory for what we referred to as critical cyber infrastructures. We have talked in this nation, and have used the commission report from a number of years ago about critical infrastructure protection. Well, here we're talking about critical cyber infrastructures—defining those—what are those for our nation? And we established the fact that communications, energy, finance, and government services fall into that critical cyber infrastructure area.

Summary of Recommendations

- ✓ FTC to implement regulations to protect consumers by requiring businesses to adopt a risk-based approach to credentialing
- ✓ By 2010, all agencies should report how many employees, contractors, & grantees are using credentials that comply with HSPD-12

- Modernize Authorities
  - ✓ DOJ to reexamine statutes governing criminal investigations of on-line crime
  - ✓ Attorney General issue guidelines for circumstances & requirements for law enforcement, military, or intelligence authorities in Cyber incidents

We also endorsed the use of strong government-issued credentials for online activities. And yesterday Scott Charney gave a magnificent luncheon presentation on this. And his underlying fact is that all identity is derivative and it's based on social customs. And I think there's something great we can learn from and work on in that particular area of the identity. The FTC to implement regulations to protect consumers using a risk-based approach to credentialing. And, you know, the risk-based approach really needs to be applied in the business areas because people in our networks, you have to manage the risk. And by 2010 we also recommended that all agencies should report how many individuals in their employment and who support them comply with HSPD-12 which is the policy for common identification standard for federal employees and contractors. And the way you could control this—to really have a hammer, if you will—is to restrict bonuses and awards for non-compliance.

Modernizing authorities was another area and we had two recommendations under that—Department of Justice examining the statutes governing the criminal investigations for online crime—and recommending that our Attorney General issue the guidelines for the requirements in law enforcement.

You know, this is an area where we need to have increased clarity—speed up the investigations—and better protect our privacy. We're using a lot of law enforcement standards today that are really industrial-age type activities. Wrapping yellow tape around a crime scene in cyber just doesn't get it. It's not fast enough. So I think you can understand that we really have to issue new kind of guidelines—new type of processes—new procedures that address the speed of the network.

Revising the FISMA is something that has been worked. FISMA1 is in works right now, but we really need to work a FISMA2 that uses performance-based measurements and go from a compliance paperwork-type drill—an exercise—to one that really gets to the real requirements and real assessment of operational security on our networks today.

We need to end the division between civil and national security systems by eliminating legal distinctions between these areas and adopt this risk-based approach for federal computer security.

We need to assume that we have intrusions—they are there—and we need to learn to deal with them and manage that risk.

A couple of the last areas of our recommendations—conduct training. We heard a lot about that yesterday from people on the stage here in our panels—for cyber education and workforce development. We think this is something that ought to be taken on in a national criteria—creating training programs and career paths for federal cyber workforce and developing a national education program. We really think of increasing the supply of skilled cyber workers is very important, and I'm happy to report that Secretary Gates yesterday announced a three-fold increase in the output of cyber skilled workers in the Department of Defense—one of his criteria now.

Summary of Recommendations

- Revised Federal Information Security Management Act (FISMA)
  - ✓ Congress to rewrite FISMA to use performance-based measurements
- End Division Between Civilian & National Security Systems
  - ✓ Eliminate legal distinctions between technical standards for national security systems & civilian agency systems and adopt a risk-based approach for federal computer security

Summary of Recommendations

- Conduct Training for Cyber Education & Workforce Development
  - ✓ NOC – with relevant agencies & OPM – create training programs & career paths for federal cyber workforce and – with National Science Foundation – develop national education programs
- Conduct Research & Development for Cybersecurity
  - ✓ NOC – with Office of Science & Technology Policy – coordinate Cybersecurity R&D

And then finally, the last recommendation is really in the research and development area of for cybersecurity. And working with the Office of Science and Technology Policy—coordinating this cybersecurity R&D across the nation—we see and recommend that the U.S. should increase—longer term—R&D investment in the areas of telecommunications, power, and those other critical cyber infrastructure areas.

We talk about—also—re-architecting the Internet. You know, today we are still using 1970s and 1980s core protocols in our Internet. And by golly, we built it—we invented it—so we ought to be able to make changes to it. But we have to do that with a national-type effort and involvement.

Now, those are the findings—three—and the 25 recommendations, briefly noted. And you can find the report. It goes through a lot more detail, and I wanted to hit on a number of these things. I think you can see, as General Chilton talks about the full spectrum of cyberspace, that we are trying to address at the national level as General Chilton is addressing this across the Department of Defense. It's a big area of involvement.

Now, I talked earlier about what the situation was at the beginning of our study in January of 2008, and so I just went through a few newspaper clippings and took a look at what's been going on since our report was released just several months ago in December of '08.

Take a look at some of these statistics of where we're going—$1 trillion worth of data stolen globally is the estimate. You talk about an economic stimulus package globally—$2 trillion—and I think it's going up exponentially.

Cybercrime up 53 percent and the kind of numbers that are associated with the financial institutions are staggering.

Cyber attacks continue against Kyrgyzstan—with taking out two out of four of their ISPs—which eliminated their connectivity by 85 percent with the West. Somebody knows really what's going on there and they are mapping the terrain and using cyber to their advantage.

Reported cyber attacks against the computer networks climbing, you know, in great numbers here.

Sensitive records of FAA workers breached.

Stolen design secrets being announced by Michelle Van Cleave who was in the press—that's why I put her name there—as far as design secrets of all U.S. nuclear weapons being stolen. Nuclear weapons lab missing 69 computers just in February of this month.

And repairing the average 2008 data breach is estimated to be on the average of $6.6 million. You talk about economic crisis in your own organization—that's what it costs you to fix the average data breach in your organization.

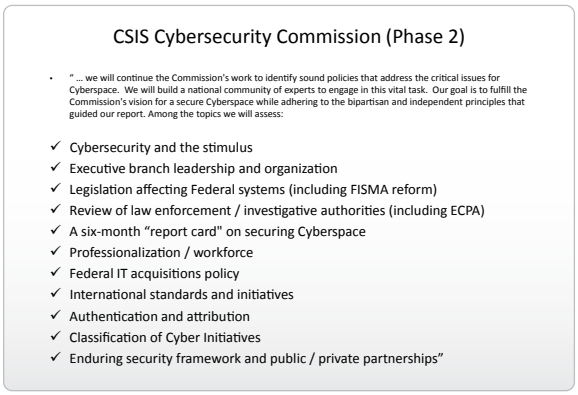
The State of Cybersecurity

- Situation After CSIS Study (post Dec 2008)
  - ✓ Estimated $1 Trillion worth of data stolen (2008)
  - ✓ Cybercrime up 53% in 2008
    - Topped $20 Billion at financial institutions
  - ✓ Cyber attack against Kyrgyzstan's ISPs (Directed Denial of Service, 18-31 Jan 09)
  - ✓ Reported cyber attacks on U.S. government computer networks climbed 40% last year
  - ✓ Sensitive records of 45,000 FAA workers breached (Feb 09)
  - ✓ Chinese stole design secrets of all U.S. nuclear weapons (Michelle Van Cleave)
  - ✓ U.S. nuclear weapons lab is missing 69 computers (Feb 09)
  - ✓ Cost to repair average 2008 data breach = $6.6 Million
  - ✓ U.S. moved from #4 to #17 in broadband connectivity

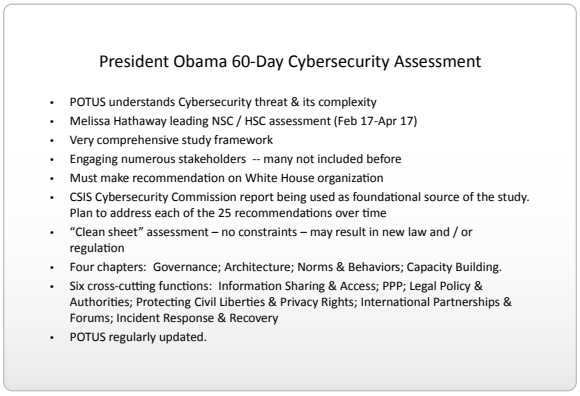
And I noticed in the newspaper also today that Secretary Gates just announced that he spent a $100 million over the last six months to fix damage of cyber attacks. So it's real—that's the kind of costs that we're faced with today.

The U.S. also moved—and I think this is an interesting wave of the future and something we really need to be concerned about because the United States has moved from number 4 to number 17 or higher in broadband connectivity around the world. I think that shows where the rest of the world is going.

Now the cybersecurity commission report was published. We thought that was going to be the end for us and we were going to be able to go back to our normal day jobs—maybe just respond to an occasional question. However, we've launched into Phase 2 of the cybersecurity commission. We're keeping the commission together and we're going to build a national community of experts to engage in a whole new series of questions that are coming up. And I list here some of the areas we see our commission on cybersecurity continuing in the future.



Now, you've heard an awful lot about President Obama's 60-day cybersecurity assessment, and I want to put a few facts out there because the President really does understand the cybersecurity threat and its complexity.



Melissa Hathaway is the one that is leading this assessment and Melissa has been given these 60 days—and I think today is Day 51 of 60—and she has been meeting regularly with a number of individuals—and she has also been reaching out with a very comprehensive study framework. Every time she updates the commission on the individuals and organizations that she is meeting with, it absolutely is staggering—the amount of input that she's getting.

And of course, that goes back to one of our recommendations in our report about reaching out nationwide and really spreading and getting input from multiple organizations—many that had not had a voice in the past.

The one requirement that this assessment has to provide is a recommendation for the White House organization. And I covered that at the early parts of my presentation about how we would recommend organizing nationally at the White House to run cybersecurity as a national security critical element.

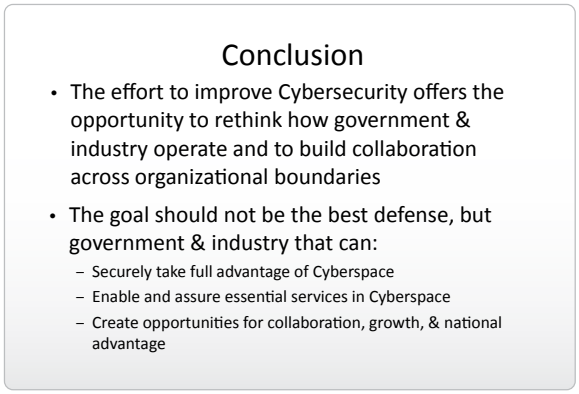
This Cybersecurity Commission Report, I'm proud to say, is being used not only in this study, but also in other areas as a foundational source for individual assessments and studies that are ongoing and will continue.

Melissa was also given a clean-sheet opportunity for an assessment. She has no constraints, and it may even result in new laws and regulations that could come out. And I think that's why it's of critical nature for us to realize and keep an eye on what the assessment is really going to provide for us.

She's divided this report into four chapters which are listed on this chart—and also six cross-cutting functions—to try and address all of the different areas that we have identified and that she has been asked to assess. And I can say that the President is being updated regularly. The National Security Adviser is very much involved in this and with the report coming to conclusion here next Friday—on the 17th of April—Melissa Hathaway is scheduled now to brief the President on her conclusions.

So, in conclusion, this effort that we've got to improve cybersecurity and cyberspace offers us great opportunity to rethink how our government and our industry are going to operate together and build collaboration—and really trusted collaboration is the way I would put it. I don't think it can always be secure collaboration, but it certainly needs to be trusted collaboration. And I think Scott Charney yesterday talked an awful lot about the benefit of trust. And when you think about it, it's like that old Johnny Carson show, you know, who do you trust? On this—in this area, you've got to know who you can trust. And that whole panel we had up here of the group that worked together on a daily basis—you know—fighting the networks—operating the networks—collaborating—they trust each other because they know each other. And so I think trusted collaboration is really key for the future and something we have to build upon.

And then the last area here I think in conclusion is the goal. It doesn't need to be just the best defense but how government and industry really can best use cyberspace in these areas here of taking advantage of it—of enabling essential services to be performed for our nation's security and our economic and financial stability—and creating opportunities for collaboration, growth and national advantage.



And General Chilton and the people of U.S. Strategic Command and the AFCEA participation, I want to thank you. I would say that one of the challenges I would issue to you all is the fact that the Department of Defense has been ahead in many of these areas for a long time. A lot because of the great vision of an initiative of Dr. Hamry back in 1998 of challenging us to take this on. So we really moved out and the Department of Defense put an awful lot of resource and emphasis on developing this area. So Dr. Hamry really put us on the right track on this, and I think the United States—the national level—can use the inputs that you have—the experience you've gained—and your great ideas as we stand up this national-level effort of putting cybersecurity and cyberspace as a national priority. So you can contribute to that, and I think we all would be better off knowing your efforts and having the great benefit of U.S. Strategic Command and the great minds that are helping you in this trusted collaborative effort into the future of cyberspace.

Thank you very much, everyone for your kind attention. And by the way, if you want a copy of the report—which has the actual words in more detail—it's at www.csis.org and you can download the whole report. It's about 90 pages. You can see who we interviewed—who was part of the briefing—and also who was part of the assessments. So thank you very much for your kind attention.

Chapter 8

Speaker—Mr Rod Beckstrom, Independent Cybersecurity Advisor

Cyberspace–The Long View

Speaker
Mr. Rod Beckstrom,
Independent Cybersecurity Advisor

Objective
Present a view of the future of the cyberspace world from the perspective of a Cyber experts and author.

Key Takeaways
- Decentralized networks improve survivability of the GIG
- Networks are more vulnerable due to lack of collaboration and international boundaries that prevent or limit information-sharing (win-win *vs* win-lose)
- Need to understand the net present value of your networks (*e.g.,* what is the value? how much should I spend?)
- Need to re-architect the Internet protocols (*e.g.,* IPv6, SMTP, BGP-SEC, *etc.*)

Speaker Discussions
Transcripts of Mr Beckstrom's presentation are not available for public release. Notes taken from his presentation are provided below.

Immediately following 9/11, Mr. Beckstrom dedicated three-and-a-half years to development of a network of CEOs who he thought could help the U.S. deal with the global threat represented by terrorism. He focused his initial efforts on track-two diplomacy. He said first there were two of them, then four, then seven. A month later there were 20, two months later there were 50. In the course of 2 years, 4000 CEOs from around the world registered to join his network.

Mr. Beckstrom said the CEO network decided to model themselves after Al Qaeda because Al Qaeda's network was extremely effective with limited resources and in order to counteract their activities, they'd need to understand Al Qaeda's network and how better to do that than to model themselves after it? As it turned out, they could find no research that reflected that anyone modeled Al Qaeda. Much was done to analyze personalities but no one had actually studied a structural model of Al Qaeda.

Mr. Beckstrom said they wrote a book capturing what they learned about decentralized networks entitled "The Starfish and The Spider." This book and subsequent presentations at various forums led to invites by the Intelligence Community to come and brainstorm on USG efforts in cyberspace. These efforts eventually led to Mr. Beckstrom being selected to serve as the Director of the National Cybersecurity Center. His tenure there brought him into contact with senior leadership at JTF-GNO and DISA.

Mr. Beckstrom went on to discuss decentralization as a theory and concept. He presented the Internet as the world's biggest decentralized network. He highlighted that while the Internet is decentralized physically, it is centralized logically. It hangs together with a very small set of protocols that are vulnerable to attack.

Mr. Beckstrom presented the concept of organizational models based on the extremes of either a spider or a starfish or some combination. He discussed how a spider represents a centralized network or organization. If you cut off a spider's leg, it impacts the entire network. However, if we look at a starfish, if you cut off one of its arms, it grows a new arm and in some cases, the arm may actually grow back into a new starfish. Why? Because it's decentralized. A starfish doesn't have a centralized brain—it has a decentralized neural network. That is why they felt it represented Al Qaeda. He also proposed that it represents the hacker communities.

Mr. Beckstrom provided an analogy in military terms, focusing on General Patreus' challenges in Iraq. He highlighted the need to deal with the challenges in Iraq by going tribe by tribe, region by region, city by city in a decentralized fashion to stabilize the country.

Mr. Beckstrom briefly discussed a couple of concepts like the "prisoner's dilemma" developed by Rand Corporation. He then shifted to the critical importance of collaboration and information sharing, at the national and international levels.

From this discussion, he shifted to the topic of the economics of cyberspace. How do we assess the value of our networks? We spend hundreds of billions of dollars protecting our networks, yet have difficulty evaluating what they are worth. He discussed a model they used at DHS to look at the transactions that occur on a network. He went on to provide some mathematical formulas for determining the net present value of a network. He also provided some thoughts on the economics of security for those networks and how our investment must weigh trade-offs in how much we invest versus the losses we experience.

Mr. Beckstrom briefly discussed re-architecting the Internet, highlighting that a number of the key protocols today are extremely vulnerable. He opined that we've got to diversify our networks and diversify our protocols to have the resilience we need.

Mr. Beckstrom closed out his presentation by talking about cybersecurity and democracy.

Chapter 9

Track 1—Cyberspace Operations

Track 1—Cyberspace Operations

Track Lead
Brig Gen Michael Carey, USSTRATCOM DJ3

Guest
Maj Gen Tom Deppe, Vice Commander, AFSPC

Track Speaker
Mr. Sami Saydjari, President, Cyber Defense Agency

Breakout 1: Joint Command and Control
Breakout 2: Joint Battlespace Awareness
Breakout 3: Joint Net-Centric Operations

Objective
Draw on the diverse experience of symposium participants to collect unique insights on key Tier 1 Joint Capability Areas (JCAs) critical to cyberspace operations.

Key Takeaways
- Lack of DoD guidance/decision making
- Lack of CO strategic priorities
- Need for centralized strategic leadership
- Lack of national/international oversight/regulations
- Lack of CO resources and domain knowledge at the tactical/operational level

Recommendations/Action Items
- Create CO "brain trust" of industry/academic/gov experts to advise STRATCOM
- Mandate best practices as the standard and rework DoD processes to meet them
- Require routine analysis of decision maker info requirements and info pathways for critical DoD decision maker tasks (C2, *etc.*)
- Field a scalable Common Operating Picture (COP) for both CO platform (network) and payload (data)—must include placeholders for unknowns (legacy networks, black holes, areas lacking metrics)
- Field secure non-IP/non-cyber based comms for critical C2
- Standardized and automate security requirements/response actions
- Create processes/measures for all source cyber BDA/effects
- Create a list of STRATCOM CO priorities and push DoD/industry/gov to solve
- Create a single DoD/gov/industry CO risk/hazard assessment org outside of operations similar to safety model to conduct assessments of decision, information, infrastructure failures leading to operational capability loss
- Create a portal for cyber lessons learned emphasizing max access/minimal editing
- Develop and propagate DoD/STRATCOM strategic goals and objectives for CO (NNWC has excellent model tied to tasks)
- Develop, implement, and publish unclass CO ROE for clarity/deterrence effect
- Create a joint DoD/ODNI IA control for info quality based on info quality criteria in JP 3-13 similar to the IA security control issued by NIST for non-DoD/Intel orgs of the Federal government
- Reference and imbed principles of JCS Functional Concept for Battlespace Awareness (2003) into CO policies/strategies/insts/JPs
- Reference and imbed principles of DoD Network Centric Operations Conceptual Framework (2003) into CO policies/strategies/insts/JPs
- Create a policy to separate cyberspace ops Intel products from cyberspace ops collection methods to prevent over-classification of critical Intel sharing essential to working with industry/partners/public
- Reproduce or shift critical CO activities currently managed by the Intel community to DoD/Gov orgs to enhance/maintain public trust (Per annual Ponemon study of gov and industry, NSA ranked last for 2007 and second to last for 2008 in public trust of 74 Federal orgs).
- Create a billet for STRATCOM J3C (cyber) to support J3 similar to J3N
- Create C2 capability for CO at STRATCOM that mirrors nuclear C2
- Set deadlines for the creation of standardized training and qualification criteria for enlisted and officer cyber operators across DoD and civilians in Gov/Industry
- Support development of cyber operator career paths in all Services where specialization/education and consecutive operational tours are not detrimental as cyberspace has fastest rate of operational change of any domain
- Require minimum level of CO in all exercises and measure success by ability to mitigate cross domain risk (loss of SA, loss of C2, loss of Intel, *etc.*), not avoid it
- Create internship program across STRATCOM entities to recruit students (high school/college) and professionals into military or government service in CO

Guest Speaker/Track Discussions

Brig Gen Carey: Good afternoon. I'm Mike Carey. I'm the Deputy Director of Global Operations STRATCOM and I would like to welcome you today to Cyberspace Operations—called Track One.

Because it's the number one issue—no, kidding, from operation. I'm not prejudiced in that regard.

We have the distinct pleasure of being joined together by Major General Tom Deppe, the Vice Commander of Air Force Space Command. He will offer some perspective on Operational Space as well as Mr. Sami Saydjari who is the President of the Cyberspace Defense Agency and founder of that organization. Both of these gentlemen will bring different perspectives to cyberspace operations. One, an Air Force and service perspective and not to steal the bloom from the rose, sir, I will allow you [to inform us] what's the latest and greatest on cyberspace operations in the United States Air Force.

Maj Gen Deppe: Thanks, Mike.

I told Mike I didn't have any prepared remarks, and that introduction may just take longer than my remarks.

But this track called Cyberspace Operations is what I wanted to participate in because we at Air Force Space Command are going to become the operational arm of the U.S. Air Force in cyber dealings and in cyber operations. This is taking, as many of you know, somewhat of an awkward path to get to Space Command. Many of us remember back in 2000 or 1999 when cyber operations were going to be located at Air Force Space Command where we thought it should be as part of Cyberspace Command because of the natural marriage between space capabilities and cyber capabilities. Because eventually it found its home.

We are in the process right now of forming our numbered Air Force, our combat operational numbered Air Force, which is going to be called 24th Air Force, location to be determined. We have done the siting surveys, and we're just waiting for a decision. It could be one of six places, either here at Offutt, which is one of them, or at Lackland or Langley or at Scott or at Peterson.

I hope that was six.

But anyway, when that decision gets made, we will then stand up that numbered Air Force and the headquarters organization. The train and equip leg of that will be with us at Peterson. And at the same time we're doing that, you are probably aware we're losing our intercontinental ballistic mission and that is going to Global Strike Command—going to Barksdale.

The one thing that I found, and Mike mentioned that I've got nearly 42 years on active duty, the one thing that has remained constant in these 42 years is that we're always changing.

We change organizations—we change patches—we change the way we do things. In fact, I gave a speech down at Air Command and Staff on change and I said, "You know, I've seen so much change I said my last car cost more than my first house and my last pair of shoes cost more than my first car."

And this is going to be another change that is going to require a culture shift in our Air Force as we look at cyber from an operational and warfighting standpoint.

There are a lot of people, and there are probably some in this room, that think, okay, Cyber Command or cyber numbered Air Force, is going to be part of Space Command, and all of those people are going to go to the A6. They couldn't be farther from the truth. Cyber operations are going to be intermingled throughout the command just like any other operations. We're going to have people in the 3, the 4, the 5, the 6, the 8. They are going to be responsible for the organize, train, equip of this mission area in this domain, which I think marries very well with space.

So I will look forward to answering any of your questions, but now I'll turn it back over to Mike, and he can introduce our featured speaker. Thanks.

Brig Gen Carey: (Introducing Mr. Saydjari.)

Sami Saydjari: Thank you. What I would like to do is start out being controversial.

I would like to talk about the right thing to do. And so one of the things that I was advised in my early career was that good management is about figuring out how to do the things that you're told to do, how to do those things right. And good leadership is about figuring out the right things to do.

One of my concerns about the conference so far is that we've been really talking about how to do the things we've been told to do right, and not about the right things to do.

One of the background pieces that I've done in the work I've done the last decade is a strategic cyber attack analysis in support of the National Security Council. It was dubbed Dark Angel, which was done fully from open source information.

And the purpose of that analysis was to make the case of how bad, bad can get. The conclusion was that a strategic cyber attack would do trillions of dollars of damage to the U.S. economy, trillions of dollars, and would compromise U.S. sovereignty in the end and would have the effect of about a thousand [Hurricane] Katrinas.

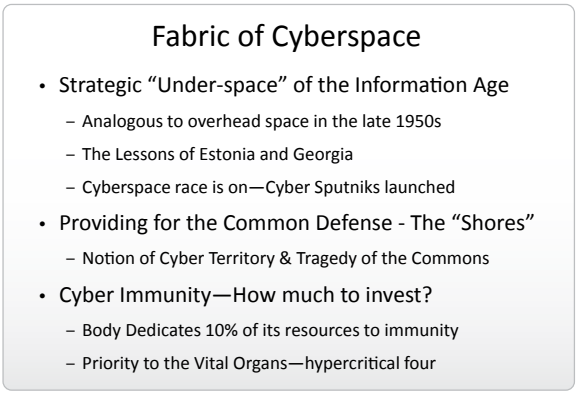
We talk about bringing down the U.S. power grid to the 70 percent level and holding it down for six months. It is a level of attack that is not acceptable.

Now, you may or may not believe that, but uncertainty about how bad bad can get will cause us to do the wrong thing. So in fact, if you don't know the answer to the question about how bad bad can get you can't possibly know the right strategy for dealing with that. So I would like to ask that the group consider very strongly the urgent need to do a national risk assessment about where our risks lie and to look at the gravity of the situation in the same way we did in the Dark Angel and develop strategic cyber attack scenarios against which we measure our actions to see whether or not we reduce the risk from those scenarios.

Now, there was nothing that was said in the last several hours that I disagree with. Certainly the DoD must come to terms with defending their portion of cyberspace. I consider that hygiene. And it's good to have good hygiene. But it's not sufficient. And we cannot spend all of our time and resources talking about good hygiene. We have to talk about defending the United States against strategic damage from a strategic national cyber attack.

All right. So those are the remarks that were sort of engendered by the last couple of hours about what I heard. Let me get on to how I think about this problem.

I view cyberspace as a strategic under-space of the information age, and we should look at it in the same way that we looked at overhead space in the late 1950s. So I agree with the General that it's very appropriate to place [Cyber Command] in Space Command because I think the gravity of the situation, the urgency is very much similar to the late '50s for the space above the earth.



The lessons from Estonia and Georgia tell us the cyberspace race is on. Estonia was an experiment in the wild of a cyberspace attack by Russia. Georgia was an indication that they are going to use attacks on civilian infrastructure as part of general warfare.

These are very important lessons and they are harbingers of what's to come.

So the cyberspace race is on. And it is a space race. Cyber Sputniks have been launched. The Chinese capability is substantial, both in quality and quantity, and probably exceeds our own, and I know that nobody in this room wants to think that way, but I think it's true. And I think we are behind in the information-age space race that we originally [technologically] created, and that is not acceptable.

The second point I would like to make here is about providing for the common defense of our shores. Cyberspace is a part of our territory. There is no question about this. And it is an essential part of our territory.

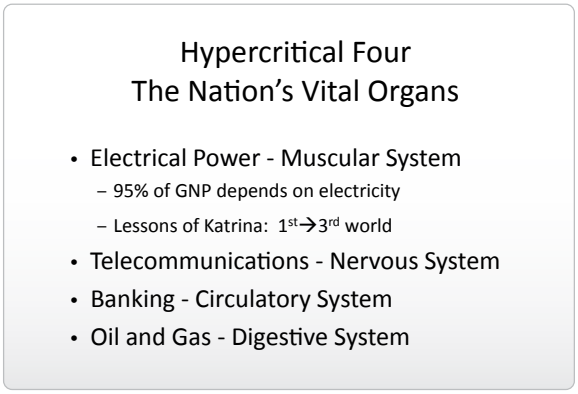
Our critical infrastructure providers are on the shores of that territory. We do not ask people who live on the shores of our physical territory to bear the cost of defending the United States against foreign invasion on the beaches. Similarly, we cannot ask the people who are operating the power grids and the banking systems to bear the cost in the defense of those systems which are critical to our status as a first-world nation.

So we must look back to the Constitution in terms of providing for the common defense. These are costs that we have to bear as a society. We cannot ask those who are on the front line to bear that cost. And it is squarely in the mission of the Defense Department of the United States of America to defend our cyber soil against strategic cyber attack.

And this notion that DoD's business is to defend DoD's network is analogous to the white blood cells of the body giving exclusive priority defending the immunity system at the risk of, and expense of the heart, the brain, and the soul. That is not reasonable. That's not a reasonable position and we must change that.

Which brings me to my third analogy—which those of you who know me understand that I think very much in terms of these analogies, and what they can bring to us. Cyber immunity is a question about what is it that we should invest and how should we invest it. The body dedicates about 10 percent of its resources to the immunity system. Do we dedicate 10 percent of our resources to defending our cyberspace in terms of IT? Not even close. We're off by at least one order of magnitude and probably two. We must make an argument in a business case for the right level for investment. It can't simply be whatever is leftover or whatever that we think that we can sell. We must make the case on first order principles of what's necessary to invest because we have to look at what the risks are. And if the risks are our national sovereignty and they are in the trillions of dollars, we are way under-invested. And if you don't know again what that gravity level is, then we're not doing our job here.

What are the primary vital organs we need to defend? Let me get on to this. This is what I call the hypercritical four.



Electrical power is [the] muscular system of United States of America. Ninety-five percent of our GNP depends on electricity. Our superpower status depends on power. The lessons from Hurricane Katrina, which was a natural disaster, shows us that a portion of our country went from a first-world country to a third-world nation overnight and stayed that way for weeks, and some argue for months. Imagine that effect times a thousand across the United States for a minimum of six months. That is a compromising event to our sovereignty. That is not acceptable.

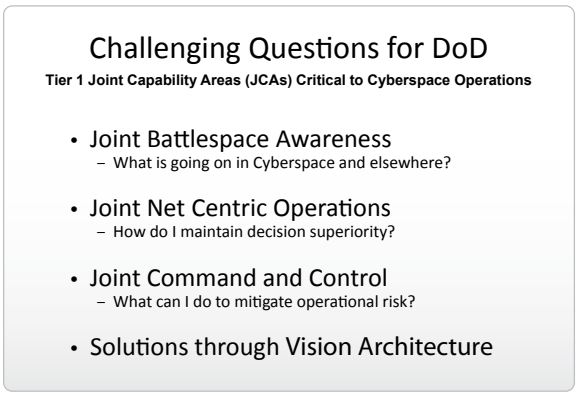
Again, you can say I'm wrong. You can challenge the assertion, although I will tell you that Dark Angel was heavily vetted with infrastructure providers. But if you think I'm wrong, then it is incumbent upon you to find out what level of damage is possible before you decide what the right course of action is, and decide what the right thing to do is. Because even though you have been told to do X, part of your job is to figure out whether X is what you should be doing or something else.

Secondly, telecommunications is the nervous system of our country. Without it, none of the critical infrastructure can operate. Can our telecommunications infrastructure stand a strategic cyber attack by a well-resourced nation willing to spend a billion dollars and three to five years in preparation for attack against our telecom? The answer is no. Ask the telecom providers, they will tell you so. No, that's not okay. We can't live with that answer.

The banking system is our circulatory system. As we've seen in the last 18 months, in particular the last six months, our whole world rests on the integrity of the banking system. The integrity of that system and the ability to defend against a

nation-state adversary is not great. They do very well against organized crime. They won't do so well against nation-states.

And oil and gas is our digestive system. If that is destroyed, we are out of luck.



Now, I'm going to skip this slide—well, let me say a couple of things about this. One is in terms of joint battle space awareness; to a first order approximation, if we look at the stealthiest of the stealth attacks that we know of, we are approximately blind to those attacks. If we look at infrastructure attacks and life cycle attacks, which I know we talk about in another session, for example, we are blind and unable to stop those kinds of attacks. That is not okay. We can't live with that, and we can't wait for the DHS to stand up such capability. We cannot say it is not our job. It is our job as citizens and military.

The other thing about command and control, just to skim down to Bullet 3 here, command and control, it's really, really important in my mind when you have a very, very hard problem like we have here, to have some use cases. And so, again, you know, we need Dark Angel to help the United States and to help the White House understand whether their strategy to defend cyberspace was adequate, so we created a use case or, if you prefer, an abuse case, of strategic cyber attack.

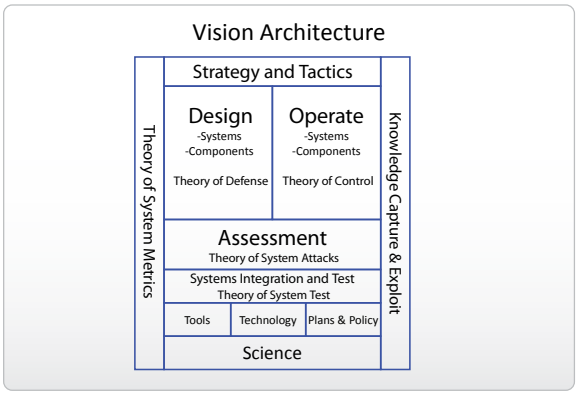
To me I think the way to handle this problem, at least to get going on how to do the right thing as opposed to do what we're doing right, is to develop about a half a dozen to a dozen strategic cyber attack scenarios on the order of Dark Angel that we did for NSC, and compare every action we do to this standard. To ask the question, does this mitigate the risk? Does it reduce the likelihood of these attacks? Does it reduce the damage from these attacks?

And if the answer is no, stop doing that and do something that gives the answer of yes to that particular attack.

And once we have an understanding of the kinds of things we need to do, the kinds of decision the President needs to make on Day 1 of a strategic cyber attack, which I assert we don't have right now, then the command and control infrastructure we need to deploy these decisions—to execute those decisions—will become clear. And then once the decisions that we need to make and the command control we need to support those is clear, then it will become clear what intelligence we need to gain in order to support those decisions. I think when we're reversing the precedence of intelligence and command and control. This is because of historical reasons that we have done cyber computer network exploitation before we've done any of these other things. So now we have to figure out again the strategic scenarios to drive those to figure out what the right thing do is.

Now, so those are my comments that are sort of deep and very philosophical. And I know they are kind of a downer, right? Because nobody wants to hear that we've got a lot of work do and nobody wants to hear that we really need to figure out the right thing to do, but part of my job today is to say things people don't want to hear so I apologize if I offended anybody.

What I want to talk about here are some categories of how to think about this over for our discussion this afternoon. And I'm not going to do the review. I'm going to talk about a few of these because there isn't time to talk about all of them. But these are things that I really think we need to think about and how they work together towards achieving the kinds of plans and playbooks that we need to be able to be working from.



We need strategies and tactics. Above all else we need to understand what we need to do in a strategic cyber attack. Again, I would like for us to focus our attention on the most damaging of attacks because if we focus our attention on all of the tactical stuff that's going on today, we're going to miss the big picture. Yes, we should be doing that stuff—defending our networks—I'm not saying we shouldn't do that. We should also spend time, resources, and brain power at the strategic scenarios because if we don't, we are going to get bitten.

So this is the overall picture, and I'm going to focus on a few of these—strategy and tactics—operations—and a bit about technology and science. And maybe I'll mention a little bit—I'm going to skip over design because there's not a lot of time.

Operate

- Goal
  - Create a Theory of Control in Cyberspace Operations
  - Understand optimal static configurations
  - Understand how to reconfigure with dynamic risk
  - Realize that iterative control with feed-forward (standards) and feedback (effects) loops needed to reached desired state
- Near Term
  - Create and retain Super Operators
  - 10X effectiveness difference between the best and average
  - Knowledge capture of top system operators
  - Encode knowledge in expert systems and make them available
  - Expert systems become advisory to average operator

I think in operations, we don't have a theory of control on cyberspace, meaning what things do—we need to do—will have what effects against what part of the attack space.

The attack space is huge. The countermeasure space is huge. The understanding of how to map the two and to understand how to re-configure a system to optimize your defense against a particular attack is not well understood. Now, I say that in criticism of the R&D community, being a member of that [community], for having failed to develop those concepts. But in fact, we are where we are, and we have to figure out what we do in the face of a conficker attack versus a GhostNet attack versus a DDoS [Distributed Denial-of-Service] attack. We need to understand, and we need to understand it now.

Another point I want to make here, and I should have made it a little bit earlier, is that the front line [in a strategic cyber war] is not in the DoD, that is to say the DoD will certainly be attacked in the next cyber war, but will not be the primary target.

This theory of control has to extend into the private sector. And so we have to look at different kinds of models—about how they operate—and work with them for this kind of control. And I think the notion of the military parachuting into the operations room of electrical power grid plant or into the telecom operations room to try to help—I think—is kind of ridiculous. I don't think it would be reasonable that that would work.

And so we really have to recruit people, I think, in a militia-type fashion, who are on the front lines of these wars—practice with them—engage in the development of the strategic cyber attack scenarios and the defense plans with them—as we develop theories on how to control the most damaging and devastating attacks we can think of.

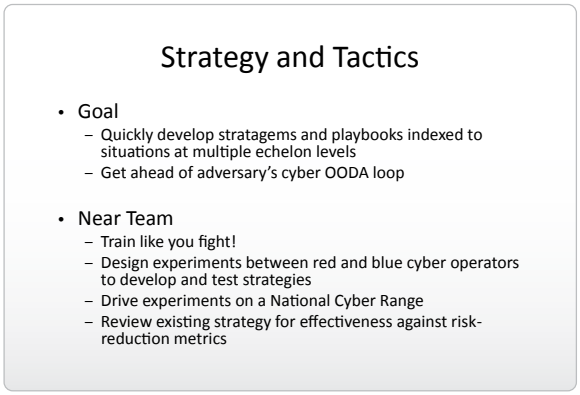
So when you think of Cyber Command—you think about STRATCOM, NORTHCOM—I think you have to think about a different kind of model for the engagement of a defense, including the militia model of people on the front lines of the war who will really be there.

Knowledge Capture and Exploit

- Goal
  - Create frameworks and processes to capture existing knowledge and make it widely available
- Near Term
  - Look for other pockets of key knowledge by targeting cyberspace communities encompassing the old-guard, front line operators, new blood, etc.

The other point I would make in the operations community is that the best of our best operators are at least ten times better than our average operator. There are some very talented operational defenders out there—amazing people—people who found, you know, things that nobody else would have found. We have to find a way of bringing that incredible talent down to the average type of operator who has much less experience and insight and making that visible [to the average operators]. And I think a way to do that, for example, is to capture [in an expert system] his triggers, his cues, and the kinds of things that person looks for—and make that kind of knowledge available to the average person to multiply the kinds of operations that we do in terms of their effectiveness against

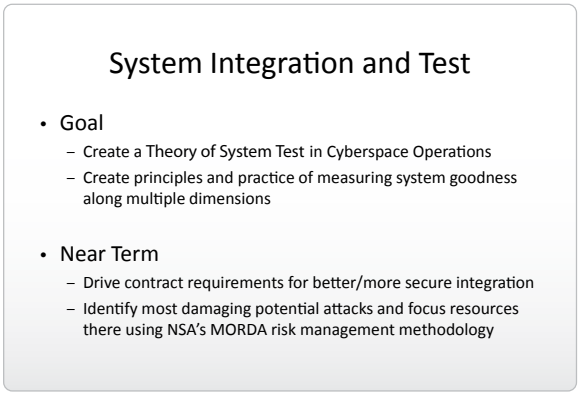
cyber attacks, because really if you're talking about something to better our posture tomorrow, it's not a technology. It's operating differently and capturing the very, very highly talented people who are very creative in defending our networks.



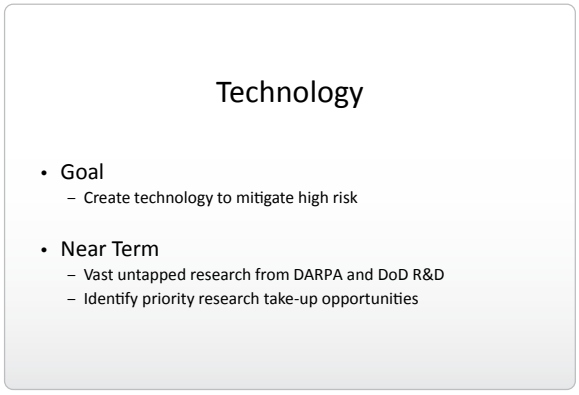
Strategies and tactics. This is one of my many soap boxes, but one of the most important ones. We have developed strategies and tactics, for example, for taking the high ground in a battle through many, many millennia of people not taking the high ground in battle and having it hurt really bad. You lose lots of troops when you're in a battle, and you figure out the low ground is not very helpful. We don't have millennia in cyberspace and the first strategic cyber attack blow will be very, very damaging. We can't wait until we have millennia of experience in order to develop our strategies and tactics. Our only hope here is to design real experiments, and I'm not talking about exercises in the military where you do a little bit of cyber, where you tie cyber attackers' hands behind their back and blindfold them, and let them operate from 12:01 to 12:02 at night so you don't interfere in the operations of the exercise. I'm talking about an honest to goodness experiment where the action and intention is to develop sterling strategies and tactics at the national level, and playbooks about what we're going to do in the context of each of these. What are the actions? What are the possibilities? What are the pros and cons with each possibility? What is the President going to do? What is the Commander of STRATCOM going to do? What is DHS going to do? What is NORTHCOM going to do? And what is the civil sector going to do? We don't have those playbooks. That is urgent. There is no excuse for not having that playbook tomorrow. Somebody can sketch on the back of a napkin this evening, hand it to the President, and we've got the start of a playbook, and we should iterate. There is no excuse for not having that playbook today. And the excuse of that's not my job, that's DHS' job or somebody else's job will not hold muster when we are under fire in a strategic attack against the United States.

We need to drive these experiments, and we need to have our best of the best in the red teams operating against the best of our blue teams, and we have to include the critical infrastructure because they are on the front lines of this war.

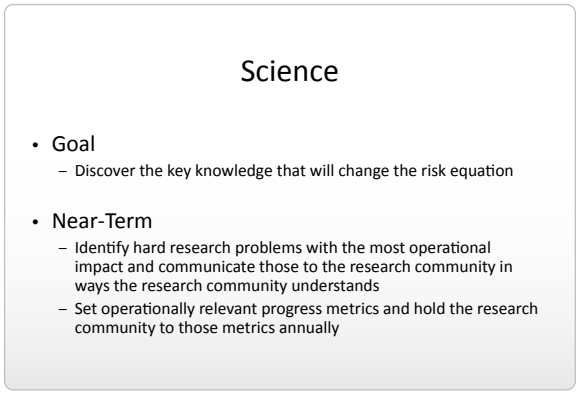
Another point I would like to make is really a metrics point that I'm making on this slide at the bottom. I think we really have to look at risk reduction as the primary matrix of the effectiveness of what we do. Risk reduction particularly in terms of strategic risk reduction is what it's all about. And risk reduction return-on-investment, meaning for each dollar that we spend, how much are we reducing our risk, is really what the investment strategy should be about.



So the kind of methodologies out there, NSA's MORDA [Mission-Oriented Risk and Design Analysis] risk management and related risk management methodologies, are there to help us prioritize our threats and vulnerabilities and attack areas we worry about so we are focused on the right things. Risk management and understanding of the kind of attacks at the strategic level are critical to our planning process—to our technology development process—to our operations—to everything. We must have a metric. Risk reduction is the best metric I've seen in the last quarter century. We must operationalize that. We must hold it out, in everything we do, as the standard by which we measure whether something is the right thing to do next.



On technology, I will say that there is a vast untapped research/resource that has been done by DARPA and other sponsors that we have not deployed. Much of it is useful, some is not. One of the things I have seen is an unfortunate disconnection between operations and R&D that has lasted too long in this field.



We need visionary leadership to pick ten of the top capabilities our nation needs—such as cyber indication and warnings—cyber command and control—cyber playbooks at the national level—and drive the R&D from these capabilities. There needs to be a top-level vision. Somebody has to step up. STRATCOM seems like a good place. Maybe it's Space Command. But somebody must establish the vision from the top level down and drive the R&D and drive the engineers of the United States capability to make sure that we are able to defend against strategic attack.

And technology has a key role here, and we do not have much time to waste. And so the technology has to be driven. And by that I don't mean that we want to wait or even that we want to have 18-month or six-month horizon R&D. We should definitely do near-term research, but we should also have a whole portfolio with the full spectrum of the kinds of things that we want to do.

And the deep science underneath this is broken. I think we have not done enough of that—and this is not the right forum to talk about it here—although I'll say it to stimulate some discussions.

There are some hard problems we are going to have to overcome. The metrics problem for example—we look at it every three years—we pull up the rock, look under it—we say, that's hard, and we put the rock back down. It's time to face some of these deep science problems and have a continued investment.

I think that I'll wrap up here—and I'll say something about the urgency here—the last bullet. We should have started yesterday. There're a lot of things that we can do now—right now—not tomorrow—but now. Particularly in the workshop and when you go home tonight—there are lots of things you can do to reduce our risk posture of strategic cyber vulnerability—which is the metric I have and we need to focus on this.

Brig Gen Carey: I don't know how many times you noted that a poke in the ribs or a prodding along to get energy to organizations that are—many of us represent were just presented. I thought it was really nice. Right in front here is Mr. Pattermann, who is Director of Training Exercises. So when you said exercises, I said to myself how handy that is so whole will be able to take. Here's a couple things I jotted down that you should find pejorative. If not, we'll get more coffee out and then you will think so.

For example, when you think about exercises and who the owners are and who the leaders are in cyber—is it DoD—is it civil—is it commercial—is it private—or is it all of that—and who is to lead—a service—a COCOM—or some other agency that is represented in another capacity?

Resource apportionment is highly contentious. Ten percent of the resources going to cyber defense would come from insurance. It's maybe not a zero sum game, but it's pretty close, so we need to think through that. And it's kind of an interesting issue, especially when you think about accountability and shared defense. When you think about the shores—who lives on the shores—how much investment is it to those who benefit from the enterprises but don't bear the burden of the enterprises?

Risk reduction versus risk management. A lot of what we do in the Department of Defense at-large is about risk management. Understanding the risk is the first and foremost part, which I think was alluded to. Maybe you don't understand the full scope of that risk because we haven't invested enough energy in looking under that rock. You know, every so often, we look, put the rock back down, and keep looking through it. Knowing…throughout the room from time to time find that there is a pocket of individuals here and there who certain thoughts have resonated with. Civil liberties versus principles of security—and the challenge ongoing there. As you get into the cyber world, that's particularly problematic.

We have a number of allies with us here today, and although the principals are the same, the actual rule sets may be different. So how will those play in a coalition environment as we move forward with our partners? And then R&D versus Ops—that's a perpetual challenge in industry and DoD. And again, roles and missions. Who does what to whom and under what authority—with what budgetary authority as well?

So if you didn't have a thought about some of those things, those are the first things that kicked me in the shins, as you were standing next to me here. And I understand there's a question or two already posted and ready to be presented, so please.

Participant At Large: You mentioned playbooks. I'm wondering what the government is doing? Private industry, private companies, Amazon, Google have been attacked—sharing these things—are they sharing the playbooks—building liaisons?

Maj Gen Deppe: They are.

Sami Saydjari: They are starting to try to work together. I think that they are primarily working. To the extent they are working, some of them are working better than others. Banking tends to work well. Telecom works well, primarily because they already had established relationships, even before DHS stepped in. They work well against tactical situations. I don't think they work well against strategic situations because they haven't thought about the really, really bad stuff.

Participant At Large: I think you might be reaching to say the Department of Defense will be responsible for defending private companies, banking or utility companies. The one way we can think of doing that is to secure the network or, B, build a wall around them so they can't get in anyway. Neither one of which the private companies like us to do. How do you get around that?

Sami Saydjari: Basically what he said. The DoD would have difficulty defending the private sector unless they are inside, or they build some wall around the private sector and how do I propose to do that?

My answer is that I think that's why I introduce the notion of a militia because I think you have to recruit the people who are inside of these networks to operate with us, and with DoD support, as part of the DoD's operations. So if you are a CSO [Chief Security Officer], for example, of an electrical power grid—an important part of power grid—you're also colonel so-and-so of the militia for cyberspace defense—and you operate and exercise with the DoD in the face of a strategic attack scenario. So essentially you recruit the officers of this kind of strange militia that's inside of these companies operating critical infrastructure. And by the way, we make our technology available to them as well and do some of our R&D and support their defenses to make their systems more robust.

Participant At Large: Trapper John. I don't have a question, but I got a couple of comments. First off, with the gentleman that talked about building a wall. I was in Peter Kiewit Institute…literally closed in a nuclear power plant, you know—cut it off from the rest of the world. But point being that building a wall doesn't work because down the road a little ways was the water infrastructure that if he had the nuclear power plant and it was as vulnerable to cyber attack as the power plant would have been had it not been for…But with respect to your use of the term militia, I just have a—I had a thought and suggestion. That were the nation to be attacked from a kinetic respect, you know, we have what we refer to as viral police, ambulance drivers and so forth as first responders. And maybe instead of using a term like militia or something especially as it relates to the private industry, maybe we need to think about broadening our term of first responders as it relates to cyberspace.

Sami Saydjari: Okay. Other questions and—okay. Go ahead.

Participant At Large: China, Russia technology challenge as far as them being…If you had to categorize it further, would you say that they are

technologically more advanced or do they exist? The political will to do things that the United States won't do and no matter what architectures we establish we don't establish the political will to retaliate based upon wrapping around an axle with attribution. Do you believe we'll ever be able to respond to what you say we'll be thrown at?

Sami Saydjari: I think the point is that there is a political will and a willingness by China and Russia to do things we won't do. We've had that problem in kinetic space. There're certain things we won't do in kinetic space so it makes our job more challenging. So I don't think we'll ever do some of the lawless things some of our adversaries are doing in cyberspace. Does that hamper us? Yeah. Do we have the political vision, for example, China had ten years ago—we are going to nationally commit to information dominance within 50 years. Do we have that national will? We certainly haven't. Our investment strategy certainly says we haven't. Plan says we have not. Will we develop that visionary leadership? I'm afraid it might have to wait until after we incurred a major attack that will cost us a trillion dollars. I'm afraid that that's—you know—I'm afraid we'll have to wait. That's why I'm here, so we don't have to wait for that, but oftentimes we are a reacting society. So again, part of what I believe leadership is all about is acting before the event, not after the event. And part of what I think we need to step up to is deciding to act now—act before that event happens—and begin to develop the national will—and educate our President—and educate our Congress on the right thing to do.

Participant At Large: Cyber Initiative 12, Project 12, has to do with the private industry—Admiral Brown is heading it up—But how are you tied into that? Are you working with them or on that plan?

Sami Saydjari: No. Well, I don't know exactly how to answer that question. I mean, there are many, many different activities—R&D activities—there's the industry plan. I don't think any of them are oriented towards strategic attack scenarios and how to defend against them. I'm not on Committee 12. From listening to people leading these things, they are not geared toward strategic cyber attack scenarios and how to defend against them. I think they are geared to the sort of political process instead of big picture. I think they are all missing the big picture, and I think we have to reorient ourselves, and that's what I'm trying to encourage us to do.

Brig Gen Carey: (Break into subgroups.)

Chapter 10

Track 2—Mitigating the Threat

Track 2—Mitigating the Threat

Track Lead
CAPT Jeff Canfield, USSTRATCOM J2

Track Speaker
Ms. Priscilla Guthrie, Director, Info Systems & Tech Division, IDA

Breakout 1: IT Supply Chain Hazards to U.S. National Security Interests
Breakout 2: Information Assurance
Breakout 3: Insider Threats to Cyber Security

Objective
Highlight vulnerabilities to the U.S. posed by computers and military hardware components in the supply chain; increased threat of socially engineered e-mails and similar threats to information assurance; threat of espionage by insiders.

Key Takeaways

- There should be a trusted manufacturing capability rather than outsourcing (Supply Chain)
- Need to institutionalize a process of Education, Training, Certification, Enforcement and Inspection…change the current culture (Insider Threat)
- Start following our own procedures; consequences for non-compliance (Information Assurance)
- Procurement cycles and acquisition process lags behind technology improvements; for example, retrofitting systems to meet security requirements
- International Security Standard need (Supply Chain)
- IA security compliance needs to be a bullet on OPRs, EPRs, appraisals—Hold people responsible for IA violations; start firing people (Info Assurance)
- Invest in resources to detect anomalous activity of intentional insider threat…track current activity, analyze and predict future insider activity (Insider Threat)
- Catastrophic events may be required prior to concerted change (Supply Chain)
- Industry fears of hiring or educating people with "attacking skills" (went against corporate interests); however, these people are the most knowledgeable with the threat (Info Assurance)
- An industry expert revealed a 5000-user company is moving to thin client architecture and human-observed kiosk media center. (Insider Threat)
  - Offers possibilities for a static office environment, but may not be suited to a high tempo environment

Recommendations/Action Items
No action items. Recommendations from the Key Takeaways:

- There should be a trusted manufacturing capability rather than outsourcing (Supply Chain)
  - Conduct actual cost/benefit studies in concert with risk mitigation evaluations to determine if a trusted manufacturer is required for key components, whether command and control systems, weapon systems or simple databases that contain sensitive personal information. While admittedly difficult and costly, especially for current systems, knowing the current threat environment and not acting on it is irresponsible when considering future systems on which national security will depend.
- Need to institutionalize a process of Education, Training, Certification, Enforcement and Inspection…change the current culture (Insider Threat)
- Start following our own procedures; consequences for non-compliance (Information Assurance)
- IA security compliance needs to be a bullet on OPRs, EPRs, appraisals—Hold people responsible for IA violations; start firing people (Info Assurance)
  - Cultivate and educate a "cyber savvy" culture in the military, business and industry that is

trained and accountable for meeting information assurance guidelines and practices. Determine and actually apply appropriate penalties for willful negligence of best security practices; failure to do so invites continued apathy that will ultimately lead to compromised systems—or worse.

- Invest in resources to detect anomalous activity of intentional insider threat…track current activity, analyze and predict future insider activity (Insider Threat)
  - For the military, adopt best practices from business and industry that monitor system user activity for anomalous behavior. This includes automated system monitoring for willful disregard of established IA practices (inserting drives into or connecting hardware to USB ports) and detection of out-of-cycle system use indicative of abnormal after-hours activity or activity that repeatedly seeks to gain access to unauthorized system levels.
- Procurement cycles and acquisition process lags behind technology improvements; for example, retrofitting systems to meet security requirements
  - Move beyond talking about the need for policy changes to actually addressing the glacial acquisition process. Cutting edge technology, defensive or offensive, is sometimes obviated in weeks, days or even seconds in the cyber arena. Rapid identification of new capabilities must be followed with rapid acquisition and fielding to get inside adversary operational loops.
- Industry fears of hiring or educating people with "attacking skills" (went against corporate interests); however, these people are the most knowledgeable with the threat (Info Assurance)
  - Industry and the military have to identify, recruit and capitalize on the "digital natives" that have matured in the digital age and are now entering the workforce. The "hacker teenager" will have the requisite skills needed for a career in cyber security in business or in the military. These individuals possess the intuitive knowledge and cultural and IT skills that form the foundation of effective cyber security managers or "cyber warriors." For the military, prior to or immediately following enlistment or commissioning, the Services must quickly identify those with desired skills and provide the appropriate training for defensive and/or offensive cyber operations. Bonuses normally offered to individuals with specialized training (nuclear-trained operators in the navy, linguists, medical and legal professionals, *etc.*) must also be offered to these individuals as well. However, failure to provide a continuous intellectual challenge will likely lead to departure from the military, regardless of the monetary compensation.

Transcript

CAPT Davis: Welcome to Omaha. I have the pleasure of introducing Ms. Priscilla Guthrie this morning. She'll be speaking to us shortly on, I think, cyber threats. She's currently the director of information technology.

(Introduction.)

Ms. Priscilla Guthrie: Thank you.

Okay. So you're going to have to. This ear doesn't work. Something happened on the plane, so you're going to have to tell me if you can't hear me. Can you hear me at the back?

So really, I'm just the warm-up exercise because the real value in this session is the work that you'll do in the break-outs immediately after.

And, you know, you're going to work on three specific areas, all of high importance to mitigating the threat. One is the supply chain, which is a huge problem with Internet department. The pesky problem of Information Assurance which has been with us forever and the question of insider threats to cyberspace. So I did some thinking. And I would like to say that we have this all in together but that's not really true.

I did some thinking, though, about what might be useful to keep in mind as you go through your deliberations this morning.

And I came up with six topics that I think are useful as you frame your discussions this afternoon—or this morning.

So the first one sounds really simplistic. And people used to say this to me and I'd go, Oh, my goodness, you know, what do they mean by that and you've got to be kidding me.

But it's really—when you're working an issue that's as broad as this that crosses as many boundaries as this, this being cyber, I think that you need to put together all of the pieces to work things on a very large scale. So you need lots

of people, their organizations, the tools, and the policies to make things work. And one way to do that is to make sure that you have a shared vision, and that's the thing I used to think was fairly trite and simplistic. But certainly we make better progress when we go after something and we have a vision of where we're headed.

You know, one of the things that come to mind when I think about that is NSA. NSA put together, I thought, a very good piece of work. They called it the GIG component, the IA component of the architecture. Their first investigation, I think was 2300 pages and the second version was 3600. I mean, it's huge. And I think that that doesn't work as a shared vision because nobody can sit down and read that much, assimilate it, talk about it. It had too much technical detail. Good piece of work, but it needed to be brought up to be useful as a part of a shared vision.

So when you're considering your topic this afternoon, please think about whether a shared vision of the challenge and what's required. One other thing that comes to mind just as an example, and this dialogue continues is that sometimes when we talk about security, talking about the technical pieces, we talk about having a standard environment because it, you know, fixes, helps the noise floor and everybody knows what they have, and then the other community comes in and says no, it's better if you have diverse equipment because it's harder to attack. Well, we're not going to make a lot of progress if we go off in both directions without anyone talking to each other and figuring out which way we're going we're better off picking one and deciding we're off and moving to the other. So the first thing I would like you to keep in mind is the concept of having a shared vision.

The second thing that came to me that I thought might be useful in your deliberations is the idea. Now, remember, this is a very large effort with a lot of different people involved and it crosses a lot of boundaries. And is the idea of having all of the key elements engaged. And when I say key elements, I think up and somebody said yesterday the policy makers don't count because they are so slow. But I'm going to put policy-makers there because they've got to be informed by the technologists and most importantly the operators. So not operators, as in network operators, but operators, as in the people who actually do the required mission.

So, you know, cyber is no longer separate from the fabric of our society. We heard that yesterday. And it has and is changing the way we work and live. So I think it's increasingly important that all three of those components sit together, work together and talk about problems. They're mutually interdependent. And it's been my experience, particularly in the cyber arena, that we tend to almost stalemate ourselves when we don't have all of the pieces together, because you've got the policy-makers who say, gee, this is what I think can happen so they make a policy. I think the bilateral agreements are a wonder example of that. You know, we made bilateral agreements in a different time and era. And now we still have bilateral agreements but we have a different technology and set policies that are possible. We need to figure out how to work that.

So in your deliberations, please think about whether or not all three components are sitting at the table together because I think that's part of having the shared vision, they all understand, and then bringing all of the pieces together to debate together the topics and figure out what the best way forward is.

Okay. The third thing that I would like to mention, and this is hard. It's in this era, in this area, it's very easy to go after the easy answers rather than the good answers. And admittedly some fall in both stacks.

You know, cyber, as we all know, is huge and it's growing. Our government, and maybe I should say governments, are not exceptionally well-structured to go and map to the cyber environment, which is global and interconnected.

Certainly we know that we have to cross what we perceive to be organizational boundaries. So government to government, government to industry, industry to government, NGOs, allies, I mean, it's—it doesn't map so nicely. And we all have a human tendency to want to take on tasks that we know we can do because it's within our area of responsibility and authority.

So it's easy to see why we go and tackle a task. I mean, I do this. I have a tendency to want to partition the task so that I go after something that I know I can do with the resources I have.

And a couple of pet peeves of mine, you know, don't take offense, this is just my little list, but things that fall into this category for me at times. You know we go through a program milestone, and the goal is to get the milestone, not so much to think about the way the program operates. And I don't mean that everyone does that, but the incentive is to get through the milestone.

There's a desire to get an authority to operate so we can operate systems rather than to go and think necessarily about how, again, this system, system which I don't like, operates in a broader environment. And then the great system by system looks rather than environmental looks.

So again, when you deliberate this morning, think if you cannot just about the easy things to go after, but think about the problem in the broadest context, and then go look at the things you can pick off rather than doing it vice versa. I think the important thing is to make sure we're not wasting scarce resources and the resources will become more scarce. That we're not wasting resources going after something that was easy when we could have had something that was good as well.

So there's six of these, so bear with me.

Fourth thing, are the choices assessed strategically? You know, in the current environment, certainly we all recognize the need to go after things that are operationally required. We know that they must take priority. But it's important, I think, to note that sometimes you can do both. And I have an example. I won't use names, but some of you may recognize it where a person wanted to go after something that would allow cultural change, and he implemented an environment—this is not a cyber environment, but it was an information sharing environment—that facilitated different ways of communicating and collaborating. And it was wonderful. But as it worked in one environment, it didn't scale to the broader environment. It was a great example of a place where if he had done the implementation just slightly differently, it would have scaled. And that's what I mean by making a strategic vice current choice, a choice based on current requirements. He could have had both.

Sometimes you can't have both. Sometimes you pick one or the other. But I think, again, the important thing is to have the operators, the policy-makers and the technologists in the room as you make the trade so you understand what the cost is, what the give away is, what the trades are. It will also help build better shared awareness of what our environment, our operating environment is over time.

Okay. Fifth, this is the hardest one for me to be—to give you good examples for. But it's really is there are a risk management framework. And I think everybody is thinking that way.

You know, this, as we said, cyber is a global interconnected environment that increasingly supports this evolving social fabric in which we live. It also supports national defense. It is never going to be static. Somebody said, You know, maybe we can get a solution. It will never be static because it supports and is part of the human enterprise. So there's going to be no final answer, there's no perimeter guard that's going to do everything. There's no identity management. There's no one thing, there's no set of things that will always work.

And so rather than go and say, you know, what's the better answer for protecting the environment, I think that we really need to go and build a mental model for risk management in this arena. And again, the model can move, but it has to be a model that we understand and can work with.

I think yesterday we heard some discussion of Intel gain/loss, and there's been lots of discussion about Intel gain/loss over the years. But now I think we have three, perhaps, groups that we have to consider. So the Intel gain/loss, the traditional discussion, the operational—now don't think network operations, think traditional and non-traditional operators in the broadest sense.

And then the third thing I put at the table are the network operators and the network operators have a requirement to operate the networks to facilitate other missions and also to maintain the social fabric. And so when we think about this risk management model, I encourage you to think about those three communities and how they would fit in a risk management model and how this risk management model could be used in real-time at machine to machine speeds to allow decisions to be made, areas to be cutoff. You know, I think the one topic somebody brought up was an operator might be the deployed battle group and the deployed battle group might decide there was a denial of service attack underway and they had to operate so they decide to disconnect from the rest of the—from the GIG, if you will.

Is that a good call or a bad call? How does the call get made? Who makes the call, who's the authority, who's responsible? That goes back to the organization not being especially well-mapped to do cyber environment. So how do we build a mental model for risk management that will allow us to understand what kinds of things can be done at machine-to-machine speeds and what kinds of decisions we should make as we move forward.

Okay. Sixth thing. And this one, again, maybe sounds a bit trivial, but I'm going to ask you if we've kept our focus on operating, not operating the networks, but operating as in the broad spectrum of operations that the department, the government has to support.

Cyberspace, as Admiral Mauney noted yesterday is a made up or constructed domain which makes it different from the other domains. It's a domain that must be maintained. That was why I added that third party, the network operators to the three parties that we have to look at in gain/loss.

NSA's model seems to be worth considering. They came up with a model that said, I'm going persistent monitoring and response. And the response was what can we do at machine-to-machine speeds to keep the environment operational, so rather than thinking just defensively, think about what it's going to take to work through a problem and continue to operate. Don't just think about the defense piece of it.

So those are the six things I'm going to encourage you to consider. Is there a shared vision? Are all three elements, the policy-makers, the technologists, and the operators at the table? Is the work segmented so that you go after a good answer rather than just an easy answer? Are the choices being assessed strategically? Are we working to the vision in an OP sense, a policy sense, and a technology sense, and are we looking at how the choices fit into that vision, OP. Is there a risk management framework have we kept our focus on operating?

We absolutely know that no matter what happens, we will be a target for years to come. And so I would encourage you to focus on doing what we do so well, and that's getting the very best shared situational awareness for all our people, not just situational awareness of the network, but situational awareness in the broadest sense so that operators can look at the pieces that they need to see do the job at hand.

And then focusing on leveraging the great agility of our forces to take that situational awareness and do the job that needs to be done, responding quickly and effectively.

And with that, I encourage you to think of those six things, and we're looking forward to seeing what the breakout groups deliver.

Thank you for your time.

Chapter 11

Track 3—Cyberspace Deterrence

Track 3—Cyberspace Deterrence

Track Lead/Speaker
Brig Gen Susan J. Helms, USSTRATCOM J5

Breakout 3.1: Accountability/Attribution—
Col James LaBombard/J53
Breakout 3.2: Cyber Policy and Redlines—
Mr. Greg Weaver/J5B
Breakout 3.3: Imposing Costs—
CAPT Steve Pettit/J52

Objective
Examine the similarities/differences of a cyberspace deterrence model and support the Commander's symposium themes of meeting cyberspace threats, enhancing national security, and maintaining freedom of action.

Key Takeaways

- Characterization/attribution is a key aspect to deterrence policy and responses to hostile cyber event. Accurate attribution is more important than prompt response and lends to U.S. deterrent capability in this domain. In the characterization/attribution phase it is a key aspect to deterrence policy and responses to hostile cyber event that we are able to distinguish between who tactically conducted the attack and who is strategically behind the attack (the decision maker).
- Deterrence strategy must be tailored to address an array of potential adversaries. Response options will obviously need to be dynamic.
- We need to be consistent; declared redlines may well come to apply to our own execution of cyberspace operations. Redlines may need to take an ambiguous form to avoid adversaries "beating the system" and only affecting our networks up to a certain point.
- On imposing costs: A full spectrum of effects (DIME) must be available to USG. Responses may come in a cyber or non-cyber form. Be cognizant of controlling 2nd order effects and collateral damage. Before we conduct cost imposition we must ensure U.S. defenses are ready for a response of any scale. We cannot threaten responses we are unwilling to pursue or cause a redline to drive a policy that unwittingly drives to escalation.
- Deterrence redlines should focus on the effects of cyber attacks that threaten vital interests; potential for articulating more detailed redlines in crisis/conflict based on context. Individual cyber events may seem small by themselves, but added to one another their complementary effect could be critical. Redlines should be internal (directing our actions), and external/declaratory to establish where the U.S. stands on acceptable and unacceptable behavior.
- We should consider basing a national declaratory policy on a set of international norms in cyberspace, but those norms are yet to be established. Should we thus take the lead in developing them? A new "Law of Armed Conflict" must include cyber elements.
- Our reliance on the "cyber" domain will affect how we react. We need to avoid a self-imposed denial of service in response to adversary activity. Even though the adversary did not directly affect our network, the desired outcome is accomplished.
- Precedent is key. Our "first" response to cyber attack (public/or not) should be proportional and focus on the attributed attacker. This lays down the consistency of U.S. Cyber Policy for future would-be adversaries.

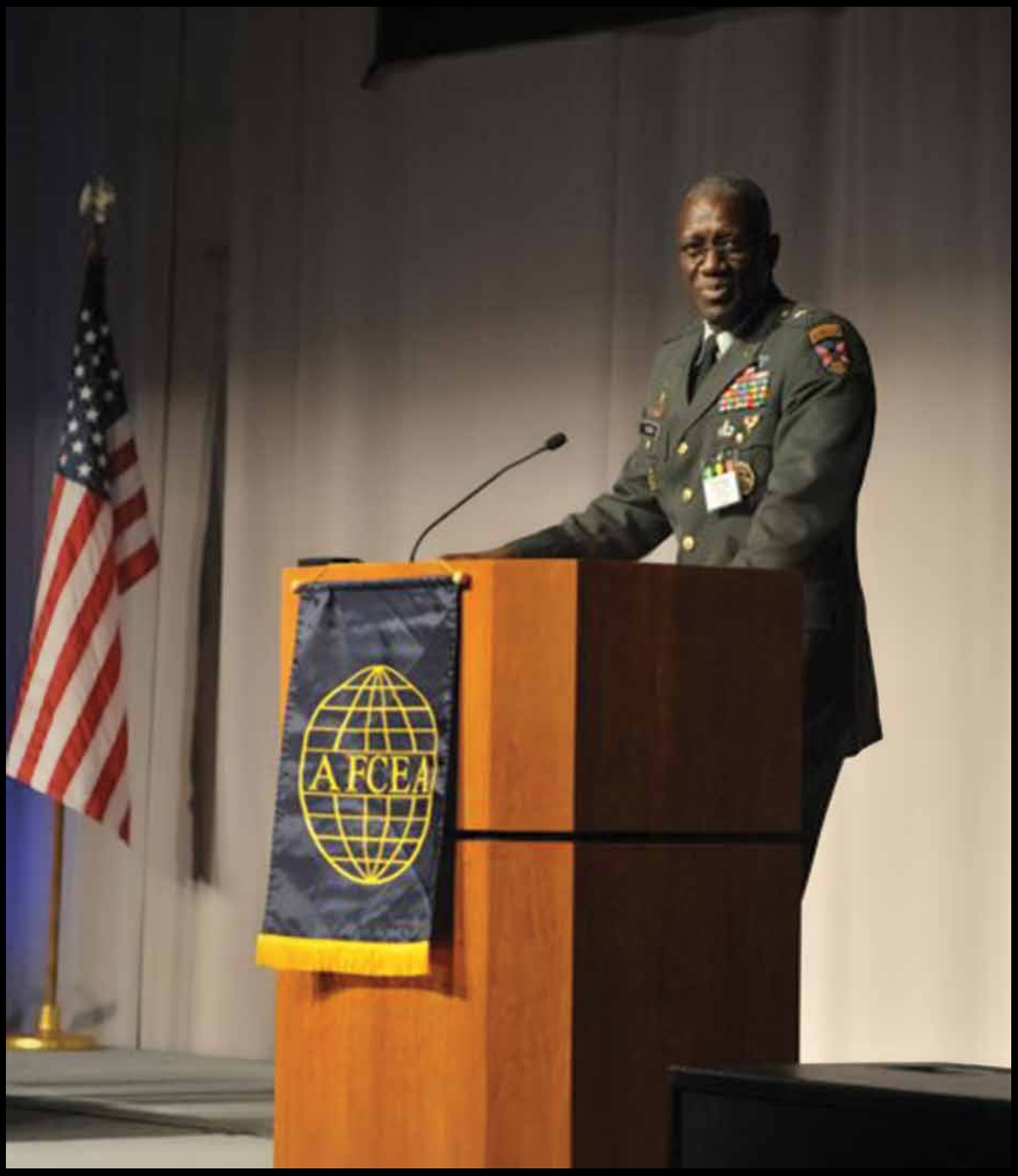
Recommendations/Action Items

- Create a Cyber Event "clearing house" at the DHS or NSC level. We need effective and accurate attribution. When does an espionage intrusion cross the line into computer network exploitation? One center can more accurately determine the global impact. Many and fractured centers will get only a local/regional view of the problem.
- The equivalent of a "Law of Armed Conflict" should be developed for Cyberspace. Set guidelines, rules of conduct, determine authority, and outline courses of action. Having a large stake in this, the U.S. should lead this effort on an international scale.
- After the organizational structure is agreed upon and established for the new "Cyber Command", its first task should be to develop cyber policy (redlines) and create a "cell" that folds in all services and defense agencies as well as non-DoD institutions (i.e, DHS, CIA, DoJ, DoS, *etc.*) to increase situational awareness. Cyberspace is not the sole responsibility of DoD; all aspects of national power depend upon freedom of action in this new domain.

Guest Speaker/Track Discussions

A complete transcript of the track discussions is unavailable. Brigadier General Susan Helms opened the track discussions by laying out some baseline thoughts on deterrence strategies, comparing old Cold War deterrence and the changing dynamics of looking at deterrence for the cyberspace arena. The track then broke up into three breakout sessions which developed the above key takeaway and recommendations.

Closing Remarks



Speaker—Major General Abraham Turner, Chief of Staff, U.S. Strategic Command

Symposium Closing Remarks

Speaker*: Major General Abraham Turner, Chief of Staff, U.S. Strategic Command*

Major General Turner: Mr. Beckstrom, thanks again for that wonderful message. I really appreciate the points. And thanks, Kevin, again for introducing me here, and I want to say thanks all of you for coming out this afternoon. Now is my time to say thanks to everyone for coming out to Omaha for the past few days. We had such an outstanding turn out, about 1,582 stakeholders, folks from industry, government, academia, and also from international partners here. Give yourself a round of applause for being here in Omaha.

Now, I recognize how busy everyone is being away from our offices for extended periods of time, but the work you've done here this past week has been just truly outstanding and certainly important to us all. You see, the work that you've done has provided us a foundation to really take a close look at some of the ongoing challenges that we are going to face as we move towards operating in a safer and more secure is cyberspace environment.

And on behalf of our great Combatant Commander, General Chilton, and on behalf of the entire USSTRATCOM team that's here, we want to say thank you for being here. We want to say thank you to the panelists who participated in the different panels over the past few days. We want to say thank you to those speakers, which you just heard a great one here just minutes ago, for attending. And more importantly, thank you for actively participating in all of the different venues that we had here over the past few days. I would also like to say thank you to Lieutenant Governor Sheehy for opening the symposium yesterday. If you recall his opening remarks, he referred to one of the news programs, I think it was Good Morning America, who basically identified Nebraskans as the happiest people in the nation, just recently. I'm certain as you leave this state, you have a better appreciation for that title and would ask that as you return back to the East or West Coast you share what you've seen here in Omaha, to your friends and to your families, because we want you to continue to visit this great community.

Now, as you know, General Chilton's vision for this cyberspace symposium is to make this an annual event and we plan to do just that, although this is only our first. And I believe that this has been a very great first step towards realizing that vision because I think so we've made history here this week. Just think of the numbers that have attended. Think of the different mediums that you represent. Think of the expanses of the news that this symposium has reached. Just early this morning I was talking to our Combatant Commander about Xinhua, the Beijing China news media article that was printed just yesterday addressing some of the issues that we were discussing here over the past few days. What great outreach.

With the changes in cyberspace occurring at speed of light, it will continue to take the best efforts of us all to stay abreast of the latest. It behooves us all to reach out in the world of technology to try to find the very best answers to some of these challenges.

Now, as I go about saluting people who have participated here, I must tell you that we will walk away with some key points that I want you to capture as you move. And let me have the slide very quickly. I've only got four of them that I will address very shortly.

First of all, the idea that there must be a shared situational awareness in cyberspace and that's important, of course, because with shared situational awareness it provides us a common operating picture so that leaders will stay informed and make informed decisions.

We also understand we will continue to face a persistent dedicated adversary, or I should say adversaries including insiders and also supply chain integrity threats that we have discussed throughout the last few days. We must change our cultural approach to cyberspace. We talked about the pressing needs of good hardware, that is technological tools to use. We've also talked about software, but more importantly we talked about operators who were technologically savvy so that they can help us defend our interest in cyberspace. And then finally, I think, we validated what we all initially suspected, and that is that future progress will depend upon an integrated team approach. That is a team of professionals from the Department of Defense, a team that consists of those from the commercial, business, international arenas.

As you head back to your offices and your over-stuffed inboxes that you have out there around our great nation, I'd just hope that you leave understanding that we appreciate you having taken time to be here for the past

Closing Comments

- Shared situational awareness in cyberspace is important

- We continue to face persistent, dedicated adversaries

- We must change our cultural approach to cyberspace

- Future progress will depend on approaching the challenges and opportunities in cyberspace as an integrated team

couple of days. And I hope that you've made valuable new contacts here. We would ask to you reach out to them, maintain those contacts that you've established here over the past few days. And I encourage you to maintain contact with us here at STRATCOM.

And in closing, let me state the obvious. Any conference of this magnitude and success would not reach the levels of success that it has without the hard work of some great people. And if you would just bear with me for just a few seconds, I want to highlight a few of them. And I'll start first with the AFCEA team led by Kent Schneider and his team that worked with him very closely, Becky Nolan, General Dubia, and also Steve Strippoli. They are here, and I'd ask you to give them a round of applause for the work that they've done here. (Applause).

We owe a debt of gratitude to the Qwest Center, especially the leadership that helped organize this, Shawn Olsen and Natalie Knolls who coordinated the entire event for us. We also would say thanks to the great food service team that came out and zipped this place just right getting it ready for us throughout the day's activities.

And then also I would like to say thanks to the exhibitors who presented some great products downstairs and I think that you will agree that we are certainly on the right tracks as we take a look at the future as we move towards bringing about a safer and more secure cyberspace environment.

And finally I would like to say thanks for the entire USSTRATCOM team. We had just recently here today you heard Kevin Williams who directs the Global Innovation and Strategy Center who has sponsored this. Kevin thank you very much for all of the great work you and your team, Liz Durham-Ruiz, you also had Don Harding who worked with you. Thanks again for the work that you've actually done to make this a success.

Two days of hard work. Two days of listening to some great speakers and enjoying the views from some great panelists. This is our first attempt at getting it right. You have helped us to make it right. Fifteen hundred and thirty two members here today and yesterday to make it right the first time. Thanks again for being here. Thanks for traveling all across the United States and elsewhere to be here in Omaha with us. And with that, we offer you safe travels. We offer you our very best wishes as you depart here late this evening and tomorrow. And with that I would like now to introduce to you the Combatant Commander of the United States Strategic Command, General Chilton.

Speaker
General Kevin P. Chilton, Commander,
U.S. Strategic Command

General Chilton: Do I have a great chief of staff or what? How about a round of applause for General Turner.

I can't tell you how many times people asked me, how do you keep all of these missions and things straight at STRATCOM? I say I can't, but I've got a staff that is just phenomenal. And Abe, you're right, a lot of hard work went into this program that we've all be participating in, by the STRATCOM staff and by the AFCEA team, and so I would echo your thanks to them. But really you all are who made it special. There is someone else I want to recognize here. He worked for me last year and the good news he still works for me, and that is General Carroll Pollett. He was the former Chief of Staff for STRATCOM last year…the Commander of JTF-GNO…Director of DISA.

It was sometime last year, about a year ago I think, there was LandNetWar, do I have that right? LandWarNet conference down in Miami, and they wanted a speaker to come down and talk about cyberspace and I said, that would be perfect for you to go to General Pollett, that's an Army program. You can go down there and they will understand you. They will say Hooah with every other paragraph, and they'll know what you're talking about.

And he said, No, sir, you need to go down and speak down there.

And so I went. And boy was I glad I did. I think there were 7,000 great cyber warriors down there from the United States Army, and I was just so tickled pink by this to see that many people in one venue all worrying about the same important problem that we worry about at STRATCOM every single day. And it was at that point I said, we've got to do this at STRATCOM because we've got the mission. It says right here in this document, the President signed it. STRATCOM is the cyber command for America, for the Department of Defense. It says right there. You're in charge of operating and defending the DoD GIG. We've got to do something like this. We've got to bring thought and ideas and focus to this mission set with a similar conference here in Omaha, Nebraska. And we need to do it in a big way. And I was introduced to General John Dubia down there from AFCEA. And I said I want 7,000 people in Omaha. He said, General, we've been building up this program down here for a long time in Miami, we didn't start with 7,000 people. He says I'm thinking you've got to set your sights a little lower, maybe about 500 at the first conference. I said no, 2,000 General. I'll negotiate down there.

Well, look, you don't measure success I don't think by the number of people who come to your conference, and I never believed that. I wanted the challenge. But part of our work here, part of our work is missionary folks. You know what I talked about earlier at the opening remarks was changing culture, conduct and capability. This is the culture right here. If you didn't get it, and I'm pretty sure every one of you got it before you came here and that's why you came here, but if you didn't get it before you came to this conference, I know you've got it now. Because we've had some tremendous speakers, tremendous panels, diverse views. You've had an opportunity to voice your ideas in the track sessions, and I'm going to get feedback from those track sessions, and I'm going to pay attention to what you all had to say.

We have so much work in front of us, so much important work to do, and I'm just so thankful for you all taking time out of your busy schedules to be here and show your interest and emphasis in this mission set.

At STRATCOM we do space, we do cyberspace, and as my 3 likes to remind me, oh, by the way we do nukes, too. But I tell you, those are three important global mission sets for the United States of America which we take very seriously, we pay attention to 24/7 at the headquarters, and we are served by phenomenal components in the JTF-GNO led by General Pollett and General Davis, and by the JFCC Network Warfare led by General Alexander and General Vautrinot. And I would appreciate it if you give those individuals a round of applause because they are doing this work every day for us, for America.

Again, ladies and gentlemen, thank you so much for being a part of this first cyberspace forum here at Omaha, Nebraska, hosted by USSTRATCOM and AFCEA. It will be the first of many, but we can't do this once a year. We can all gather here and share ideas once a year but the missionary work starts tomorrow when you head home, and we've got to keep working this problem, sharing ideas, exchanging information because the work in front of us is absolutely critical to the defense of America.

God bless you all. Safe travels home.
Thank you very much.


UNITED STATES
STRATEGIC COMMAND


AFCEA