◆ SPECIAL SUPPLEMENT TO THE CYBER DEFENSE REVIEW ◆

JSA 2016 PROCEEDINGS

APRIL 20-21, 2016

SYNCHRONIZED SECURITY

PUBLIC ◆ PRIVATE PARTNERSHIPS IN CYBERSPACE

JSA
JOINT SERVICE ACADEMY
CYBER SECURITY SUMMIT

THE ARMY CYBER INSTITUTE AT WEST POINT

COMMENTARY
KEYNOTES
PANELS

PUBLIC ◆ PRIVATE
PARTNERSHIPS IN
CYBERSPACE

JSA
JOINT SERVICE
ACADEMY
CYBER SECURITY
SUMMIT

LEFT TO RIGHT:
SECRETARY JOHNSON,
SERVICE ACADEMY CADETS,
USMA CADETS WITH CDX 16
TROPHY, USNA ATTENDEES

JSA 2016 PROCEEDINGS

INTRODUCTION

THEME

Synchronized Security: Public-Private Partnerships in Cyberspace.

VISION

To synchronize government and private industry efforts to secure and build a more defensible cyberspace.

MISSION

To provide a platform where senior leaders of government, industry and the service academies converge to build meaningful partnerships for relevant cyberspace initiatives.

The Army Cyber Institute (ACI) and Palo Alto Networks co-hosted the Joint Service Academy Cyber Security Summit on April 20-21, 2016 at West Point, NY. Colloquially known as "JSA", this conference has already become the premier cybersecurity event for defense and corporate leaders. This year's event featured 23 chief executives or commanding generals, and more than 50 additional C-suite executives representing 13 of the 16 critical US infrastructures. The discussions and engagements focused on synchronizing government and private industry efforts to secure and build a more defensible cyberspace domain.

As General (Ret) Keith Alexander told us, US cyber defense is not an issue that can be handled by a single agency or supported by one legislative initiative. JSA laid the groundwork for future relationships by examining issues pertaining to the Internet of Things, Industry Initiatives on Threat Sharing, and the Role of Government. A recurring theme should stand out from this report: information sharing is a key component in our national cyber defense.

The summit included a panel on the role of the Service Academies in the development of cyber leaders and their respective approaches to developing trained cyber operators for the nation. JSA also included keynotes by the Secretary of Homeland Security, the Honorable Jeh Johnson, Congressman Mike Pompeo, Mr. Richard Ledgett, Deputy Director, National Security Agency, General (Ret) Raymond T. Odierno, and Mr. Mark McLaughlin, Chairman of the National Security Telecommunications Advisory Committee, and CEO, Palo Alto Networks.

Our national understanding of how cyber has changed the world is nascent. This is why we need events such as JSA because public-private collaboration contribute mightily to this conversation. The response to JSA was overwhelming. Participants reported in JSA surveys that they found the panelists to be excellent and to the point. Others reported the keynote speakers were outstanding and timely in their comments. More than eighty percent of the audience told us the event exceeded their expectations. We would like to thank all of the individuals who participated in the conference for their insight and active involvement in addressing challenging cyberspace issues. JSA was made possible through the support of Palo Alto Networks.

Andrew O. Hall

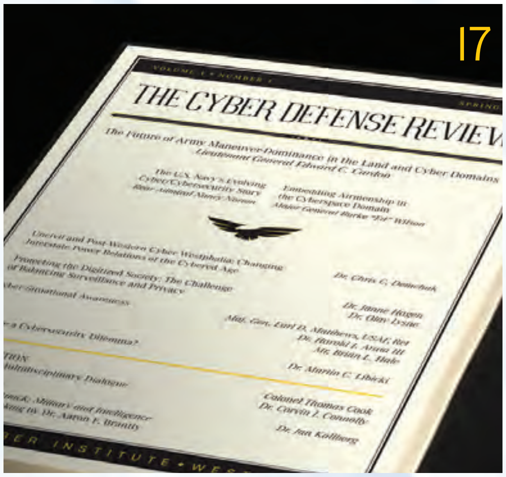
Colonel Andrew O. Hall
Director, ACI

This summit report was prepared under the direction of Colonel J. Carlos Vega, the ACI Director of Outreach, and Colonel Daniel Bennett, the ACI Director of Research, and was edited by Dr. Corvin Connolly, in coordination with research fellows Dr. Aaron Brantly and Professor Stephanie Pell. The opinions expressed in this report are those of the authors, and do not represent the official position of the United States Military Academy, the Department of the Army, nor the Department of Defense.

CONTACT
Army Cyber Institute
2101 New South Post Road
Spellman Hall
West Point, New York 10996

The views expressed in these proceedings are those of the authors and not the U.S. Military Academy, the Department of the Army, or any other agency of the U.S. Government. Copyright protection is not available for official publications of the United States government. However, the authors of specific content published in the Joint Service Academy Cyber Security Summit Proceedings retain copyright to their individual works, so long as those authors are not United States government personnel (military or civilian). Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.

This publication of the JSA Proceedings was designed and produced by Gina Daschbach Marketing, LLC.



CONTENTS

JSA PROCEEDINGS INTRODUCTION

APRIL 20, 2016 – THAYER HOTEL, UNITED STATES MILITARY ACADEMY, WEST POINT, NY

JSA PROCEEDINGS ESSAYS

APRIL 21, 2016 – WEST POINT CLUB, UNITED STATES MILITARY ACADEMY, WEST POINT, NY

APRIL 20 WELCOME REMARKS

COLONEL J. CARLOS VEGA ◆ OPENING REMARKS

On behalf of our host Lieutenant General Caslen and Mr. Mark McLaughlin, welcome to West Point for this great event. I'm Colonel Vega. I'm the one who's been sending all those emails to you. But really the muscle behind all this is Lieutenant Colonel Glenn Robertson.

So, welcome to the event. The itinerary is inside of your program. We want to welcome the head table: Lieutenant General Caslen, General Odierno, General Alexander, Lieutenant General Hernandez, Mark McLaughlin, Mr. Ledgett, Lieutenant General Cardon, and many, many more of you here who are special within your own groups. We recognize that you are the Who's Who of this industry or you would not be here today.

Thank you for taking the time to spend this evening and tomorrow with us. We hope this JSA event not only meets your expectations, but exceeds your expectations. With that, I would like to introduce the Army Cyber Institute Director, Colonel Andy Hall.

COLONEL ANDY HALL ◆ INTRODUCTION

Well, thank you very much ladies and gentlemen for joining us today. I've had a chance to be in charge of the Army Cyber Institute since the first of April, and I'm really excited to co-chair this event with Mark McLaughlin. I have spent quite a bit of the last three years working with Colonel Greg Conti and the rest of the Army Cyber Institute, so it's really exciting for me to get a chance to join this team.

This conference provides an outstanding opportunity to highlight the work that our Service Academies are doing. We are going to be focusing on each of the academies, the work they are doing with cadets, and to show you what Army, Navy, Air Force, and the Coast Guard are all doing to prepare the next set of leaders. It is going to be a really exciting presentation.

Tomorrow, we are going to talk about a Cyber Grand Challenge with the Internet of Things. Last JSA, we looked at the issue of encryption, which in the year since, I think we've all seen in the news. The Internet of Things will continue to be in the news, and at the forefront of everything we do. We think that will be a great panel tomorrow.

Then, we're going to take a look at the key ideas from industry and government. We all have an important role to work together and share ideas. I hope this will be an outstanding opportunity for conference participants to come away from this summit thinking of some new and innovative ways that we can all engage.

One of the key ACI events we have coming up in September is the Army Cyber Talks in New York City. We are hoping to see a good number of you in New York City for this important engagement. We are looking forward to a great event, and next I would like to introduce the Superintendent of the United States Military Academy, Lieutenant General Caslen.

LIEUTENANT GENERAL ROBERT L. CASLEN, JR.

Well, thank you very much Andy. I would like to welcome all of you to the United States Military Academy and this great conference.

As Andy said, I'm the Superintendent of West Point. It's really an honor to be able to work with our cadets every day. I think if the average American wanted to see what's right with America, they would come to West Point and take a look at the cadets and see what's going on here. They will feel good about the future of our Army, and the future of our nation. I'm really proud of them.

It's truly an honor to have at the distinguished table: General Alexander and General Odierno. Gentlemen, thank you very much for coming. Lieutenant General Cardon, the Commander of Army Cyber, thank you very much, and your predecessor, who is the Chair of Army Cyber Institute, Lieutenant General Hernandez, great to have you. Mr. Ledgett and Mr. McLaughlin, thank you both for being here and for all that you've done to sponsor and put this great conference together. We are thrilled that you are here.

I also want to give a shout-out to the Army Cyber Institute for organizing this event. It's not an easy task, and you put some in long hours—thank you very much. This summit brings together senior leaders and decision makers from the Department of Defense, Department of Homeland Security, National Security Agency, and the private sector. You have come together to talk about things that are important to the public and private sector. It's important to have this dialogue, and to find ways to build meaningful partnerships for cyberspace initiatives. We are honored by your participation in this summit.

Our mission at West Point is to educate, train, and inspire leaders of character. We develop them really over four separate means that are totally integrated every day in a cadet's life. We develop them militarily. We develop them intellectually with our academic program. We develop them physically, and we develop them through character. We believe the most important part of this development is their character development. Because you can be competent in all those other things, but if you fail in character, then you fail in leadership. As a result, we have become tremendously focused on leadership development. Our mission at West Point is to be the preeminent leader-development institution in the world. We are very proud of that.

West Point was founded to facilitate the extension of the land domain as America expanded to the West. But now as we sit here today over 200 years later, the domain we are interested in is this new domain called cyberspace. Recognizing that these critical threats are out there, we established the Army Cyber Institute three years ago.

> THE ACI HAS A BRILLIANT PURPOSE AND A BRILLIANT MISSION. ”

The Army Cyber Institute was the brilliant idea of the former Chief of Staff of the Army and the former Secretary of the Army, General Odierno, and Secretary McHugh. I had the honor to work with them to facilitate the establishment of the Army Cyber Institute.

WELCOME REMARKS

The purpose of the ACI is to create knowledge, so that we can dig in and establish research and understand this domain, and understand where our adversaries are operating so that we, in this particular world, can shoot ahead of the duck instead of shooting behind the duck like we tend to do in this domain.

The second purpose is something that is particularly unique and brilliant, and that is to establish public and private partnerships. The partnerships are necessary because we have common interests in the public and private cyber domain. The ACI has a brilliant purpose and a brilliant mission. It is off to a great start, and again, I thank them for their efforts in putting this conference together.

This summit has grown from our efforts to build these public-private partnerships. Government agencies, the military, academia, and private industry—they are all doing cyber work. The JSA is about synchronizing those efforts. Our conference is about teamwork. Babe Ruth said a long time ago, "The way a team plays as a whole determines its success." He said, "You may have the greatest bunch of individual stars in the world, but if they don't play together, the club won't be worth a dime." In other words, if the right people focus on the right problem they'll generate the right results.

West Point is really proud to host this year's JSA. All of our national service academies: Navy, Air Force, Coast Guard, and the Merchant Marine offer state-of-the-art education and information technology in cybersecurity. All of our services are working together to defend America in this cyber domain. The US military has the best technology because of our strong connections with the most innovative tech community in the world. We must reinforce the strong ties between the military and our private innovators. Public-Private Partnerships are nothing new to our service academies. Our national defense has always relied on Public-Private Partnerships. Just across the river from where we sit tonight are the ruins of the West Point Iron and Cannon Foundry. The civilian enterprise, which was incorporated in 1817, enabled our young nation's defense and commerce. In addition to cannon for the Army and Navy, the foundry produced the nation's first steam engines as railroads transitioned America into an industrial power, and built the nation's first iron-hold ship. Led by Robert P. Parrott, a West Point graduate and military veteran, the West Point Foundry is an early example of innovation made possible by Public-Private Partnership. It was collaboration between government, industry, and academia that brought us the Internet and GPS. Before that, communications satellites and jet engines, and who knows where today's collaboration is going to end up. I hope this summit will generate some meaningful dialogue and you walk away convinced that cybersecurity is a team sport. It's going to take all of us working together to tackle the nation's most significant challenges in this domain. We have great panels, and keynote speakers lined up, and I know it's going to be a worthwhile, productive next couple of days. Welcome, thank you all for coming here and enjoy this summit. I hope it'll be worth your time and your efforts, and we look forward to being with you for the next couple days. Thank you very much.

CADET JACKSON PARTICIPATING IN Q&A

SERVICE ACADEMY PANEL

LEFT TO RIGHT: LCDR BENIN, MAJ CHIARAMONTE, CAPT (R) TORTORA, LTC LANHAM, DR. SOBIESK

DR. ED SOBIESK ◆ ARMY CYBER INSTITUTE

Good evening! My name is Ed Sobiesk, and I am the Division Leader for the Education and Support Division of the Army Cyber Institute at West Point. Tonight it's my privilege to moderate this panel on Academy Cyber. When it comes to the national security of our country and the cyber domain, we are absolutely one team. So, what you see before you is the combined cyber programs that form the foundation for our military cyber force. We are excited tonight to share with you where we have been and where we are today. But, more importantly, what our goals and aspirations are for the future. We are going to go Army, Navy, Air Force and Coast Guard and each speaker has about five to ten minutes.

LIEUTENANT COLONEL MICHAEL LANHAM ◆ U.S. MILITARY ACADEMY

Good evening ladies and gentlemen. My name is Lieutenant Colonel Michael Lanham, and I'm the Director of the Cyber Research Center within the Electrical Engineering and Computer Science Department at West Point. I'm a director at one of the 20-plus centers the Dean has set up at the institution.

The mission of the Electrical Engineering and Computer Science Department is to educate and inspire cadets to be leaders of character prepared to think critically, innovate, and apply engineering and technology expertise as Army officers. Our graduates go into all 17 basic branches of the United States Army. We do not generate only cyber cadets. This branch only came into existence two years ago. I happen to be a proud member of that branch, but we have 16 other basic Army branches that our graduates join.

The program is a four-year program, and much like every other four-year institution, we have a sample of computer science for everybody. Within my department this is T-shaped education for breadth and depth. There are two primary courses for every single cadet: IT 105 and IT 305. These are freshmen year and junior year courses. The junior class is taken by all the students that chose not to major in a science, technology, engineering or math degree. The cyber degrees are primarily electrical engineering, computer science and information technology. Those are the three ABET accredited degrees within the department.

West Point includes the Margin of Excellence—all the additional development programs that complement the core programs funded by the government, such as out-of-classroom leadership experiences, cultural immersion opportunities, and extra-curricular activities. The most important Margin of Excellence are Summer Internships. These are three to five-week opportunities that you

SERVICE ACADEMY PANEL

(government and industry) offer our cadets. It's not just our cadets in this department. It's across all 13 departments. Across all 40-plus academic disciplines, degree programs, within the academy. There are 40-plus academic degrees that the academy conveys to its students when they finish their 47-month journey.

We have a 15 year relationship with the National Security Agency across 10-plus departments in the Academy, and over 70 cadets interning each academic year and exposed to what the strategic intelligence community has to offer. It continues to grow and for that we thank the NSA leadership past and present.

> WE REALLY ARE SHAPING THE WAY THE NATION, AND EVEN THE WORLD, IS LOOKING AT WHAT CYBER IS GOING TO BE.

The FBI sponsors our cadets in the Cyber Crimes Unit through philanthropic gifts, and the philanthropy of the Association of Graduates. We have many partners to thank for those opportunities. The last piece of the intern program belongs to industry: Boeing, Facebook, Google, Juniper Networks, and Cisco to name a few. Our cadets have opportunities at over 50-plus companies during the summer.

We have the Cadet Competitive Cyber Team, which is an official team of the academy. They actually get time away from athletics to practice hacking and cyberattack/defense. This excites the cadets; they give up their weekends to practice.

The last Margin of Excellence opportunity that I would like to discuss are future exercises to help organizations become resilient to cyberattack. Imagine if generals and their headquarters thousands of miles away from a front line were severed from communications for days or weeks. This would be a traumatic experience for multiple echelons of command, and one we want to explore.

The last thing I want to highlight is Controller Area Networks. Raise your hand if you have heard about the Jeep being hacked in *Wired Magazine*, or the other cars that can be actually made to run off the road. That excites our cadets. They want to be able to hack a car. Now, I'm not asking you for a car, but that kind of activity is one of the things that we can do. And we're in the process of working with TRADOC, and some other organization to get that kind of excitement to say, "You want to hack a Jeep? We can help you hack a Jeep." We'll start inside the laboratory and we'll keep going from there. But that's what our future is looking like. That kind of innovation. It's a mindset. It's not just about resources, it's trying to get cadets to commit their time outside of class. Because that's when you know you've captured their imagination.

CAPTAIN PAUL TORTORA, USN RETIRED ⋄ U.S. NAVAL ACADEMY

My name is Paul Tortora, and I'm the Director of the Naval Academy Center for Cyber Security Studies. On behalf of our Superintendent Vice Admiral Ted "Slapshot" Carter, I would like to thank the Army Cyber Institute and West Point for hosting this great event. The collaboration we have is ongoing.

Bottom line, our goals are the same. We decided several years ago that all midshipmen would get two mandatory courses in cybersecurity: one as a freshman plebe, and another course as a junior. We created a new cyber operations major undergraduate degree; fundamentals include science, programming, data structures, but towards the senior year they take courses in policy, law, ethics, and even social factors, the human engineering of cyber.

Every one of our students will be part of a Carrier Strike Group no matter what their career field; even if they are a Marine. Every one of our students has to understand the complexity of cyber; all Carrier Strike Groups have networks, systems, components, and must defend against cyberattack.

The class of 2015 is the first cadre of midshipmen possessing that awareness of cyber education. All midshipmen will receive cyber education and cyber awareness. We are still working on the summer professional core competencies, but in the academic world, I think we are steps beyond where we thought we would be in our development. We are adding a number of events, electives, research projects with private partnerships, and looking for ways to expand research not traditionally conducted in the Naval Academy classroom. The internship opportunities for our midshipmen are fantastic.

When I was a midshipman, there were no internships. You went to a ship and you ... went to a ship, and that was about it. Now they have these great opportunities to see what is going on in the cyber field, which is so dynamic and important. They still have to go to sea, but now they can have these great opportunities to intern with corporate America.

We are participating in cyber competitions, especially on the policy side. Our team won the NYU Cyber Policy competition in November. We are getting a new building. I do envy the size of the ACI staff, and I think they will envy the size of my new building. We will break ground in October, and finish by summer of 2019. We are moving a number of different majors into the building that have some nexus to cyber: computer engineering, computer science, information technology, the cyber major, and systems engineering.

MAJOR MICHAEL V. CHIARAMONTE ⋄ U.S. AIR FORCE ACADEMY

I'm Major Mike Chiaramonte from the United States Air Force Academy, and like my Army and Navy counterparts have said, we are doing cyber from the approach of all, the many, and the few. I'll do a quick overview of where we are in our academic programs. Freshmen at the United States Air Force Academy all go through a core computing course; we put about 1,000 cadets through that every year with 60% of that course focuses on cyber technology, how computers and networks are put together. The goal is to graduate lieutenants in the Air Force that understand the risks to our cyber enterprise, and how they can better protect themselves. They may go fly, go intel, become cybersecurity operators, or any number of career fields, but if they understand the important questions and considerations regarding cyberspace as a ubiquitous domain across everything Air Force does in air, space, and cyber, they will be better prepared to lead in the Air Force.

Our new degree, which we call computer network security is technically deep. Cadets engage computer forensics, in-depth courses into software, reverse engineering; we conduct two capstone classes on red team/blue team activities, which include social engineering aspects of foreign actors and adversaries operating on a network. The goal of this degree is to provide the cadet technical tools and the background to understand how a foreign adversary or malicious actor is going to operate.

We also do the summer research internships and send cadets to Palo Alto Networks, Intel Corporation, NSA, and 24th Air Force. It is important to have cadets engaged in real-world cyberspace activities. One, it motivates them, two, it is much more meaningful to engage on a project that has real impact than some esoteric example from the classroom.

Our biggest initiative is the Air Force Cyber Innovation Center. This effort started in October 2014 to create a three-pronged focused organization. This is an Air Force level organization hosted at the Air Force Academy for synergistic effect. The Air Force asked us to create an institute that is focused primarily on technology innovation. How do we come up with new capabilities that can be used in industry and within the government at a faster pace and more creative pace than we do today. We are studying the pedagogy that Silicon Valley and the high tech industry has taken to heart regarding innovation. It's easy to say the word innovate, but it's hard to actually go ahead and do it. We are studying human-centric design and transdisciplinary collaboration to determine what it takes to produce game-changing technologies. We have been engaging with the Stanford Design School and Carnegie Mellon School of Design to really understand this idea.

Our first project at the Cyber Innovation Center will start this fall, and is a request from Air Force Space Command and 24th Air Force to look at how we present cyber risk at the strategic and operational levels of war, so that a non-cyber person can understand quickly its impact on the mission. Currently, the military presents cyber risk from the standpoint of a system of red, blue or green. This is more of a trial shakedown cruise of our enterprise, and how we are going to operate our processes. We will bring industry into the classroom and projects with cadets and faculty, and not as a traditional capstone course with industry partners mentoring cadets, but rather as pure collaborators where industry goes through the entire process with the cadets, and come up with a joint solution. Hopefully, we can take those promising low fidelity prototypes, and provide to industry, so they can go ahead and develop and produce a valuable capability for the military. Leveraging these Public-Private Partnerships will bring capability back to the Air Force, so that we can use it faster.

SERVICE ACADEMY PANEL

LIEUTENANT COMMANDER JOSEPH T. BENIN ◆ U.S COAST GUARD ACADEMY

If they are the three bears, it forces me to wonder what we are; we must be Goldilocks. Regarding cyber, the Coast Guard Academy really looks more to the critical infrastructure and protection. We are very excited that our Secretary will be here tomorrow as the keynote speaker for this event. We look forward to partnering with everyone here to make our nation safe from the homeland security perspective.

I am Lieutenant Commander Joseph Benin. I am a 2001 graduate of the Coast Guard Academy and a professor at the Coast Guard Academy. For those not familiar with the Coast Guard Academy, we were founded in 1876, and have about 900 cadets, but expanding to 1,000. We also seek to develop and graduate competent leaders of character. We have eight academic majors. Most of cyber resides within electrical engineering, which is where I teach. The Coast Guard is this blend of authorities: regulatory, military, intelligence, and the maritime domain. There are certain things that Coast Guard officers and members can do that the rest of our military cannot do, which positions us to really contribute to national security in the cyber domain.

We are members of the Military Academy Cyber Education Working Group, and follow the Few, Some, and All approach. One of the innovations that we have at the Coast Guard Academy is our cyber range. This was started last year, and we give all of our cadets during their Second Class summer (between their sophomore and junior years) eight hours. It's all hands on where they get to experience what it feels like to be attacked in the cyber domain, or have malware infect your systems.

Our core curriculum review has mandated every cadet to experience 1 1/2 credits in our principal electronics communications security course, which will allow them to learn about cybersecurity. On the Some side, again, we focus on electrical engineering. We're currently pursuing cyber events with the NSA and DHS. We have curriculum coursework established with a capstone project and internships. Last fall, we started a risk management course and this semester we are offering a cyber intelligence national security policy course.

In terms of the Few-development, we focus primarily on our cyber team. We have two cadets with us today, Caleb Stewart and Trey Maxim, from our cyber team. This is the first year the cyber team participated in the CyberStakes exercise, which I'm very proud of. At CyberStakes they were second to Carnegie Mellon in terms of total number of medals received, which I think was very impressive.

In terms of the Future, we are standing up a Superintendent's council on cyber, which will be the precursor to what I hope is our port and coastal cyber center when the resources arrive. In June of 2015, the Coast Guard launched its cyber strategy, which includes the Coast Guard Academy. I thank you for your time and I hope if you are ever in New London, Connecticut, you come pay me a visit. I'd love to show you around. It's a beautiful campus. Thank you.

DR. SOBIESK: It is very interesting that all of the academies have different perspectives regarding cyber. This is based on our constituent needs. Cyber is continuing to emerge as a discipline with the two professional societies for computing, the IEEE Computer Society and the ACM (Association for Computing Machinery) have stood up a task force that is actually over the next two to three years defining the cyber discipline. The academies are involved in that task force and will keep track of where it goes. The cyber discipline will be greatly impacted by what you heard this evening. We really are, through the efforts of the academies, shaping the way the nation, and even the world, is looking at what cyber is going to be. Once again, thank you very much panelists.

COLONEL VEGA: Thank you very much; we really appreciate you sharing that with us. So, why is that important? What's a common theme when we reach out to you? We talk about the lack of talent that exists in this discipline. This is where the talent is being created. How good are these cadets? Ask them. Talk to them. We have a whole team back there. They are not employable yet; they have a contract. But they are extremely talented, and I would argue that collectively, the academies are producing far beyond what other institutions are creating for the offensive side of cyber.

KEYNOTE PRESENTATION

MR. RICK LEDGETT ◆ DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. Rick Ledgett serves as the Deputy Director and senior civilian leader of the National Security Agency. In this capacity he acts as the Agency's chief operating officer, responsible for guiding and directing studies, operations and policy. From 2012 to 2013, he was the Director of the NSA/CSS Threat Operations Center, or NTOC, responsible for round-the-clock cryptologic activities to discover and counter adversary cyber efforts. He was the first Intelligence Manager for Cyber, serving as principal advisor to the Director of National Intelligence on all cyber matters. Mr. Ledgett spent nearly 11 years in the U.S. Army as a SIGINTer, and between the Army and NSA, has completed six field tours.

MR. LEDGETT: I'm glad to have the opportunity to join you tonight to help kick off the Joint Service Academy Cyber Security Summit. The symposium's theme of 'synchronized security' is one that strongly resonates with me, and is a major focus of the National Security Agency. The over-arching idea of 'cyber as a team sport' or 'partnering in cyberspace' is frequently thrown around. But it needs to be more than just a catch phrase.

The truth is that now, more than ever before, the nation requires us to work together if there will be any chance of staying ahead of those that would use the Internet for evil. And by "us" I mean the private sector, academia, and the entire US Government. We can and must learn from each other. We need to understand our partners and how they operate, and help our partners understand us. This is why events like this one are so valuable to our future success.

This summit provides a unique opportunity to enhance the dialogue between security professionals, and to synchronize government and industry efforts to secure and build a more defensible cyberspace. We must find ways to share new ideas, technological advances, and information in real time. That's not just a goal worth working toward, it is a necessity. When we work together, our Nation benefits.

The cyber domain is where our Nation stores its wealth, treasure, and most important, our information. As a knowledge and information-based economy, our strategic advantage is the ability to access data, add value through analysis, and use the resulting information and intelligence to outmaneuver others. Our innovative ideas, business plans, and negotiating strategies are all online. So are most of the transactions and records that underpin our daily lives. It has been forecasted that 6.4 billion things, worldwide, will be connected to the Internet of Things by the end of 2016. This number is up 30% from 2015, and is projected to reach 20.8 billion by 2020 [Gartner, Inc]. Today, you can buy a refrigerator that can tell when you're out of milk, or when it's reached its expiration date, and send you an alert or automatically add it to your shopping list. There are Smart ice cubes; Smart light bulbs; and I recently read about the development of smart diapers that could be used to monitor infant health.

More and more devices have built-in Internet connectivity that are designed to provide added features with more convenience (and to provide more data to the companies that build them). Every single device connected to the Internet provides an additional attack surface to those who want to exploit them. As a result, we have the continuing challenge of identifying emerging risks and vulnerabilities that occur from the introduction of new or updated technologies to our network infrastructure; the risks are definitely out there.

Cybercrime is on the rise. Nearly 1 million new pieces of malware are released every day [CNN Tech, April 2015], and with 1.5 million annual criminal events, cybercrime is a real threat to anyone on the Internet. Broken down, that number represents an average of 4,000 criminal cyber acts every day, 170 attacks every hour, or nearly three attacks every minute [CBS, March 2015]. That means 135 attacks could occur during the time allotted for me to speak with you today.

KEYNOTE PRESENTATION

America has spent decades and countless dollars building the most formidable military forces the world has ever seen. But the biggest threat to our national security is not from air, land, or sea—it comes from the cyber domain. I do not have to remind any of you that a computer with an Internet connection in the hands of a knowledgeable adversary could wreak havoc on an individual, a business, a city, or a nation. Our critical infrastructure is not immune to the changing threat environment associated with the Internet of Things.

Critical Infrastructure and Key Resources (CIKR) industries have a strong dependence on Industrial Control Systems (ICS). Historically, ICS have been obscure relative to 'regular' information technology systems, and that obscurity had provided a certain level of protection against cyberattacks. ICS are typically proprietary systems with physical isolation or air gaps between Information Technology (IT) and Operations Technology (OT).

But there are several trends in ICS cybersecurity that are making that separation less effective. The rapid rise of devices that interface with ICS is a definite concern. Connecting ICS systems to the Internet has dramatically increased security vulnerabilities. Not only that, but our adversaries are willing to push the envelope to see how much access they can gain to ICS.

> THE BIGGEST THREAT TO NATIONAL SECURITY IS NOT FROM AIR, LAND, OR SEA. IT COMES FROM THE CYBER DOMAIN.

The Bowman Avenue Dam compromise is a prime example of this—no damage was done this time. But perhaps this was simply a proof of concept for future attack vectors. The adversarial 'cyber' threat actors that engage in targeted attacks continue to expand at an alarming rate. NSA's Director, Admiral Rogers, has told Congress that a nation-state or rogue group will likely launch a major cyberattack on US critical infrastructure networks before 2025.

The potential physical effects of a cyberattack on critical infrastructure have been demonstrated several times. The Aurora generator experiment at Idaho National Lab in 2007, the Sayano-Shushenskaya accident in Russia in 2009, and the Stuxnet worm in 2010 are all well-known examples in which software resulted in physical damage to ICS-controlled devices. But you don't necessarily have to destroy the equipment. There's been plenty of press recently regarding CIKR assets that have been targeted:

- The Ukrainian electrical grid black outs in December 2015, which was the first successful attack to take down an entire power grid. External attackers used stolen credentials to remotely manipulate the SCADA systems and turn off the grid. Attackers took additional measures to delay recovery time. According to ICS-CERT, employing best practices would have mitigated these events from occurring. [Open source: US CERT (DHS) declares cyberattack responsible for Ukraine power outages and revealed BlackEnergy malware found on systems. US Deputy Energy Secretary attributes cyberattack on Ukraine to Russia. No further official USG attribution.]
- Then, as I mentioned, there is the infiltration of ICS equipment of the Bowman Avenue Dam in Rye, NY that was highlighted in the recent indictment of seven Iranian cyber actors. Those same actors were involved in a series of distributed denial of service (DDOS) attacks directed against the US financial sector in 2012 and 2013.
- Another example is Black Energy malware that has been used to infect a number of ICS systems in the US over the last few years. That software has undergone a significant evolution throughout its lifetime—there are a number of versions that have been used to infect ICS systems. It is hard to know whether to attribute malware to a single group or several.
- Yet another example is the Havex malware that was used in 2014 in a number of cyber incidents directed against the energy sector. The malware can deploy multiple payloads; one payload, noted during the 2014 campaign, gathers information about connected control system resources within the target network. [Open source: (U) US CERT (DHS) Havex was used in an ICS focused malware campaign that uses multiple vectors for infection.]

Lastly, we should be alarmed that the utilities industry has been, and likely will continue to be, a target for Chinese state-sponsored cyber groups. No doubt China's military planners are aware of the value US critical infrastructure has to supporting our military and national economy. However, it is important to distinguish cyber espionage aimed at stealing data or intellectual property, and cyber espionage with the purpose of enabling future computer network attacks to disrupt, deny access, or destroy critical infrastructure.

We are seeing more Advanced Persistent Threats as adversaries work at establishing a hidden presence or blend in with the targeted organization, using multiple attack vectors over weeks or months to establish durable point of presence in key cyber terrain. As an intelligence professional, it's hard to imagine a purpose for this exploitation and persistence on CIKR networks as anything other than reconnaissance and pre-emplacement of tools for the purpose of interfering with the systems' operations. If the purpose was understanding how the systems worked, the adversaries would most likely get that information by targeting the manufacturers rather than the operators.

The bottom line is that our adversaries have a clear understanding of the potential effects of compromising an operational ICS system of a CIKR asset, even if just to force a system restart. This is a far more dangerous scenario than an IT system compromise. You can reboot an IT system quickly, but rebooting an ICS controlling a CIKR asset has more far reaching and damaging consequences.

While ICS assets are vulnerable and an increasing target of our adversaries, implementing basic defense measures can stop attacks in their tracks. For the sake of our critical infrastructure, we need to start being more responsive to the changes that need to be made.

Of course, these are tough issues; if it were easy, it would have been solved already. If you are interested in more detail regarding electrical power systems, and if you're having trouble staying awake, read the "MIT Interdisciplinary Study on the Future Electrical Grid"—it's available on their website. Chapter 9 covers communications and cybersecurity, and it's an informative and slightly terrifying read. The US Government has begun addressing these issues, and you will hear more about that tomorrow.

Of course it is not just threats to critical infrastructure that have us concerned. Cyber adversaries have infiltrated networks and stolen confidential or propriety data from major corporations in the aerospace, financial, information technology, defense, legal and professional services, and natural resources sectors—to name a few. The objective of this activity has been the theft of intellectual property, trade secrets, and other sensitive business information.

The May 2014 Department of Justice indictment against five officers of China's People's Liberation Army (PLA), along with reporting by private cybersecurity companies, demonstrate that units within the PLA steal US proprietary business information and intellectual property.

Former Director of the National Security Agency, General Keith Alexander, called China's cyber-enabled commercial espionage "the greatest transfer of wealth in history." Unfortunately, the skills needed to conduct malicious cyber activity have dramatically decreased with the rise of access to free platforms, software, and training over the past few years. This allows actors ranging from state sponsored entities to cyber criminals to conduct computer network operations with little to no experience or investment costs.

In addition to activities such as targeted distributed denial of service (DDoS) and defacement operations, cyber actors are engaging in espionage efforts directed at entities associated with the defense and aerospace sector. This information allows adversaries to counter the technical advantages of US weapons systems by designing systems that have similar capabilities, and by developing countermeasures. Such information collection endeavors include attempts to establish network intrusions by gathering information from individuals that may grant access to proprietary information.

The days of ungrammatical, misspelled emails purporting to be from long-lost friends are gone, or at least not used by nation-state actors or sophisticated criminals. These

KEYNOTE PRESENTATION

actors conduct research on social media and other open sources, combined with sophisticated big data analysis, to produce exquisitely targeted and completely normal-looking spear-phishing messages. For instance, on February 4, 2015, a Defense Intelligence Agency (DIA) employee's personal webmail account was targeted with an unauthorized sign-in alert themed spear-phishing message from Iranian cyber actors.

These same techniques are used by all the other nation-state actors and are the principal means they use to gather user credentials to enable access to the target networks. There are nation states with national strategies—against which they have put considerable resources —to grow their economy by stealing R&D from leading technology companies from around the world. China is a prime example of this activity.

> THE MOST POTENT WEAPON WE HAVE IS THE THREE POUND COMPUTER BETWEEN THE EARS OF ALL OF US.

The September 2015 US—China cyber agreement focused on four points, most importantly the agreement that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. The US and China also agreed to improve cybercrime investigations and related diplomatic dialogues.

Yet, private cybersecurity firms report that China's cyber operations continue to target and exploit US Government, defense industry, academic and private computer networks. The US government continues to express to China's leadership that cyber-enabled theft from private industry to gain unfair commercial and negotiations advantage is unacceptable and damages our bilateral relationship.

We are committed to working with the private sector, and other entities, to include other nations, to readily and rapidly share threat information, foster partnerships, and leverage our workforces' talents to secure our networks and face the complex and constantly evolving cyber threat. Aside from increasing cyber espionage vectors and threats to our critical infrastructure, cyberspace is also affecting the war on terrorism.

This brings me to the evolving threat that the Islamic State of Iraq and the Levant (ISIL) poses. For the foreseeable future, ISIL in all its manifestations—insurgent army, foreign fighter magnet, social media phenomenon, external operations cadre—is the number one counterterrorism threat we face. ISIL is adept at communicating online. They're on Facebook. They're on YouTube. There is something like 90,000 Twitter accounts associated with or sympathetic to ISIL, some with as many as 50,000 followers. Last year, ISIL produced nearly 7,000 pieces of propaganda, disseminated by 43 distinct ISIL media offices. The New York Times, by comparison, has around 25 foreign bureaus. With the click of a mouse, these extremists are poisoning the minds of people an ocean away, radicalizing people young and old, male and female, American citizens and non-citizens.

They are using strong encryption to protect their communications. In the not-so-distant past, terrorists would have to be somewhat tech-savvy to employ techniques to encrypt their communications. Now free, worldclass encryption is available right out-of-the-box, so even the least technical savvy terrorist can communicate via secure means. There are plenty of news stories about the encrypted messaging apps that ISIL is using, and the difficulty of breaking into an encrypted device even when it is in the hands of law enforcement. We also see ISIL talking about the desire to enhance its cyber capabilities. Although I would not characterize those current capabilities as being significant, I'm definitely concerned about the future.

I believe we will see some non-nation-state actors, in the form of ISIL and al-Qaida, increasingly use technology as a component of their strategy. That is a troublesome development for us. Fifty years ago government encryption was the predominant form of cryptography in the world. The commercial cryptography market barely existed. The US and other governments developed algorithms and produced the devices used to secure communications.

Today, commercial needs for encryption to protect sensitive transactions and keep corporate and personal data private dwarfs the needs for government-built cryptographic solutions. Because it is not economically viable for the USG to produce all of the encryption it needs, we see a rapidly increasing use of commercial cryptographic solutions to protect national security systems and all forms of critical infrastructure.

As this happens, the NSA has an increasing need to understand and assess the cryptography found in commercial systems in order to ensure that it is suitable for use in National Security Systems. We are responsible for defining the standards used to protect information that traverses and resides on classified and some unclassified USG networks.

As our reliance on commercial cryptography increases, our interest and interaction with the makers of IT products with cryptography will naturally increase. While the confidentiality of communications is important, the integrity of communications, software and IT equipment is of paramount importance. Cryptography plays an important and increasing role in this context. Over the past 30 years, NSA has been slowly transitioning from specifying classified government cryptography for protecting national security systems to recommending public standards designed by non-government entities for protecting even the highest levels of government information.

While we should not ignore the current debate over law enforcement access to encrypted communications, we also should not let that debate distract us from the critical responsibility that the USG and industry have in securing our public and private networks using encryption and other cryptographic tools.

We will need continued, strong industry and academic partnerships along with the ability to use all tools available at our disposal for a whole-of-government approach, including diplomatic, intelligence, law enforcement, economic, and technical activities. The complexity of emerging cyber threats requires the best talent America has to offer. We must continue to focus on educating a robust cyber workforce and developing a common core for cyber education.

NSA demonstrates its commitment to this through its Centers of Academic Excellence program and through its close partnership with the Service Academies. NSA not only sponsors cyber exercises, but each year we sponsor about 100 interns from the four academies for classified internships. This is a significant and necessary contribution to the development of future military leaders.

The men and women who participate in these classified internships will become some of the future leaders of the nation's cyber mission force. But regardless of their branch, they will rely on information and information systems as key tools to accomplish their mission. Due to the complexity of the operational landscape and the pervasiveness of cyber, it is important that our military leaders are technically competent. It is no longer sufficient for them to simply be good leaders—it is important that they train the way they fight.

We must continue our cyber education focus even as we forge new industry partnerships. History has shown that our military forces are better equipped through the strong connections that have been established between the military and private sector innovators. In return, industry has also benefitted.

Collaboration between government, industry, and academia has brought jet engines, communications satellites, high-performance computing, GPS, and the Internet. I cannot even imagine what is in store for us next, but I'm sure it will be exciting. We must work together to provide the United States a decisive, strategic advantage in cyberspace intelligence and operations by enabling full-spectrum cyberspace operations to defend our networks and, when directed, operate against foreign networks. When we partner together, we can more fully understand our adversary's tradecraft, capabilities, and intentions. This helps to ensure our infrastructure is protected from threats.

Ultimately, the end state should be one where USG-provided threat intelligence is fused with private sector data and used to protect information on all of our networks—including those of our allies. The most potent weapon we have is the three pound computer between the ears of all of us. It is the power of our ideas and our innovation that has made this country great. We must strive to harness the knowledge and creativity in our collective workforces, and provide a culture that embraces diversity of thought and ideas and inspires people to think outside the box when it comes to meeting emerging cyber challenges.

In a world where technology changes constantly, and our adversaries' trade-craft evolves just as rapidly, we have no other choice than to partner to make our critical national security systems and the nation's critical infrastructure more resilient and more secure.

TROPHY PRESENTATION AND Q&A

COLONEL VEGA: Are you all wondering the real reason why we're here tonight?

RICK LEDGETT: That's right. To present this big ass trophy to the winner of the Cyber Defense Exercise. There are a few points I wanted to make about CDX 16. We had cadets and midshipman from the U.S. Coast Guard Academy, the U.S. Merchant Marine Academy, the U.S. Military Academy, the Naval Academy, the Royal Military College of Canada, and a cyber protection team from U.S. Cyber Command, all of whom participated in the exercise. We evaluated them on their ability to operate, maintain and defend an exchange server, a chat server, a web server, and a domain controller. This year we also did something new. We did a platform resiliency challenge.

The CDX trophy is presented to the team that scores the most in the culmination of the 80 percent of the grade that is based on operating and defending those network services, and 20 percent based on the challenges. I would like to talk first about the winners of the 3 challenges.

The malware analysis reverse engineering challenge winner was the U.S. Naval Academy.

The host and network forensics challenge winner was the U.S. Military Academy.

The offensive ethical hacking challenge winner was a tie between the undergraduate and graduate teams from the Royal Military College of Canada. The past over all winners have been the U.S. Military Academy 7 times, the U.S. Air Force Academy 4 times, the U.S. Naval Academy 3 times, and the Merchant Marine Academy once. **This year for the 8th time, the winner is the U.S. Military Academy.** I would like to congratulate the Academy's Major Mike Petullo, Major Kyle Moses, Major Carl Olsen and Major Ben Kenkowski who served as the coaches and advisors.

QUESTIONS & ANSWERS

Q: I have to ask you about the encryption. How do we resolve this issue between private industry and the government with the threat of terrorism?

RL: A couple of different things. I think this is often phrased as a debate between security and privacy. I don't think that's right. I think its security of data and security of person, and that's the trade space you're talking about. Absolute security in any of those cases is not possible, but even if it were, I would argue against it. I think you need to have a balance. I don't know what that balance is, but I think the way to get there is to have a conversation about it. The conversation needs to be public, it needs to be informed by facts not opinions, and not policy statements dressed up as technical arguments. It needs to be conducted by people who want to collaborate and come to a conclusion on the right place to be; folks from the private sector, privacy groups and advocates, from the national security and law enforcement communities, academia, and Congress need to be involved in this discussion. What is the right place for the needle to be, and which laws should Congress enact. I think it's critically important for a couple of different reasons. One is, I don't think it's the place of any company or any group of companies to define where that needle goes, and I also don't think it's the place of any one government agency, or one particular branch of the government to do that. If we get this wrong, it'll be decided by a judge, a company or something else. I think it needs to be the whole group of us together reaching a consensus. If we delay too long in this space, there's going to be a big attack against the U.S., in which case, the needle swings to the extreme. You get bad laws that have bad effects on our society. We must have this national conversation sooner rather than later.

Q: Sir, you talked a little bit about the IoT and that will be the theme tomorrow, and it's certainly an emerging trend. Is this something the DoD should embrace?

RL: That is a great question. To quote Star Trek, resistance is futile. You will be assimilated. The military is now working on uniforms that have wearable networking devices in them. I don't know how you are going to keep that out of the DoD environment. Everything you buy is going to have an Internet activity associated with it. We're grappling with that at NSA right now, I can assure you. We have to figure out how to operate in an environment in which you have all devices connected. There is good technical research that's going on, but we also have to have the corresponding policy discussion.

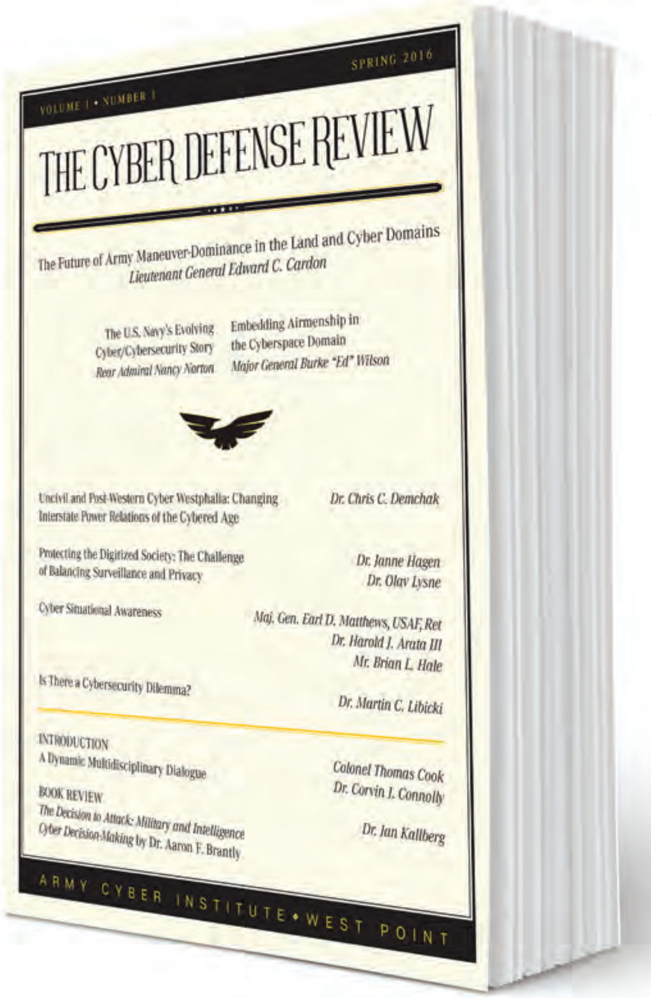
COL HALL AND SECRETARY JEH JOHNSON

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

We are proud to introduce the inaugural print edition of *The Cyber Defense Review (CDR).* This quarterly journal will generate an intellectual multi-disciplinary dialogue through thought provoking scholarly articles and essays on the strategic, operational, and tactical aspects of the cyber domain. The *CDR* will break down barriers and foster innovative solutions to global cybersecurity challenges. This inaugural *CDR* compiles perspectives from preeminent thinkers across the government, industry, and academia regarding potential challenges, impacts, and initiatives for consideration as we come to grips with cybersecurity.

This scholarly effort from the Army Cyber Institute (ACI) at West Point grew out of its commitment to focus on the intellectual properties present in cyber research, cyber education, and cyber outreach. The ACI is a national resource dedicated to engaging the Army, government, academia, and industry in impactful partnerships to solve over the horizon problems for the Army and the Nation.



VOLUME 1 • NUMBER 1

SPRING 2016

THE CYBER DEFENSE REVIEW

The Future of Army Maneuver-Dominance in the Land and Cyber Domains
Lieutenant General Edward C. Cardon

The U.S. Navy's Evolving Cyber/Cybersecurity Story
Rear Admiral Nancy Norton

Embedding Airmenship in the Cyberspace Domain
Major General Burke "Ed" Wilson

Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age — *Dr. Chris C. Demchak*

Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy — *Dr. Janne Hagen*, *Dr. Olav Lysne*

Cyber Situational Awareness — *Maj. Gen. Earl D. Matthews, USAF, Ret*, *Dr. Harold J. Arata III*, *Mr. Brian L. Hale*

Is There a Cybersecurity Dilemma? — *Dr. Martin C. Libicki*

INTRODUCTION
A Dynamic Multidisciplinary Dialogue — *Colonel Thomas Cook*, *Dr. Corvin J. Connolly*

BOOK REVIEW
The Decision to Attack: Military and Intelligence Cyber Decision-Making by Dr. Aaron F. Brantly — *Dr. Jan Kallberg*

ARMY CYBER INSTITUTE • WEST POINT

SUBMISSIONS
cyberdefensereview@usma.edu

SUBSCRIBE
Print: cyberdefensereview@usma.edu
Digital: cyberdefensereview.org

THE CYBER DEFENSE REVIEW

JSA PROCEEDINGS ESSAYS

OPENING LINES OF COMMUNICATION TO SYNCHRONIZING SECURITY

BY AARON F. BRANTLY, PH.D.

ASSISTANT PROFESSOR ◆ DEPARTMENT OF SOCIAL SCIENCES ◆ CYBER POLICY FELLOW, ARMY CYBER INSTITUTE ◆ CYBER FELLOW, COMBATING TERRORISM CENTER ◆ UNITED STATES MILITARY ACADEMY

As a nation, we are coming to grips with the technological changes enveloping our society. For all the significant gains achieved through the leveraging of cyberspace, we are confronted with a level of complexity that is challenging the traditional means by which the government, the citizenry, and industry interact. As a nation, we are interdependent through our mutual dependence on one another in cyberspace. Like almost never before, our nation finds it necessary to work together to achieve common goals, to synchronize our security. It is in this common dependence that our institutions of higher learning become conduits for training and educating those future leaders who will soon take up the necessary burdens of our ever connected society. Within the broad scope of higher education are the service academies who are training the men and women who will serve as the first line of national defense on the networks upon which we so heavily depend. It is with these burdens, and with the recognition of the task that lies before the nation that the Army Cyber Institute (ACI) facilitated the 2016 Joint Service Academy (JSA) Cyber Security Summit.

To synchronize security requires us to recognize the role that we all play in the common defense of the nation within the cyber domain. To this end, the JSA summit brought together a diverse cross-section of decision-makers from industry and government to build the foundations of a robust future. A future in which mutual trust is fostered through frank and open dialogue on often contentious topics. From the opening moments of the summit until the final speaker, the objectives were clear, it is necessary to open the lines of communication, to legally break down barriers to efficient security. The challenge of national cyber security at present appears insurmountable. Hacking incidents against corporations, financial institutions, entertainment companies, critical infrastructure providers, and the government seem to be increasing in volume and severity. The vectors of attack are diverse and often indirect. In an environment devoid of sufficient communication, we have gaps in our lines, and our flanks are woefully exposed.

The Deputy Director of the National Security Agency (NSA), Mr. Rick Ledgett, opened the JSA summit by framing the scope and scale of the challenge. He highlighted the numbers which undergird our fears. He stated that daily there are more than 1 million new pieces of malware released, and more than 4,000 criminal cyberattacks. He highlighted the systemic and intrinsic vulnerabilities of our nation's critical infrastructure and key-resources and focused his concern on the industrial control systems that manage everything from power grids to transportation networks. He highlighted the challenges posed by foreign state and sub-state entities that constantly probe US networks and steal intellectual property. Mr. Ledgett explained that we are bleeding the key intellectual property that makes our nation great. He spoke to the great scourge of violent extremists, particularly ISIS, and others leveraging our own technology against us, and their desire to advance offensive cyber capabilities to harm Americans. Yet, Mr. Ledgett's outlook, while measured, was hopeful; he stressed the need to facilitate collaboration, and NSA and other government entities efforts to develop the necessary relationships to close the gaps and guard the flanks. He closed with a powerful statement attesting to the potential that we as a society possess by saying: "The most potent weapon we have is the three-pound computer between the ears of all of us. It is the power of our ideas and our innovation that has made this country great."

The conference proceedings were broken down into panels and keynotes each focused on addressing a critical area relevant to a diverse set of interested actors. The first panel focused on the present and the future training men and women to meet the challenge of national security cyber from within the service academies. The visions of each of the academies is as diverse as the domains in which they operate, yet at the same time, they are each focused on providing a trained and innovative cadre of leaders to meet future cyber challenges head on.

The second JSA panel focused on the numerous legal and policy aspects of cyberspace, with an emphasis on the challenges posed by billions of new devices entering the global digital ecosystem. The panel, representing a broad range of interests from the ICS-CERT, to a major chip manufacturer, and both government and academia, highlighted the frustrations and challenges of securing the evolving connected world. Of particular note was their discussion on the lack of a market mechanism to instill secure development life-cycles into products. Addressing the concerns of "first-to-market" and security can, and are in most instances mutually exclusive except where there is significant potential for brand damage due to security vulnerabilities. While disheartening to recognize that the majority of platforms added to our global technical infrastructure will focus on expedience rather than security, the reality is that in some fields such as health or critical infrastructure systems, the need to pair speed with security should result in a more optimal outcome. The panelists discussed the need to balance concepts of security across ecosystems and devices in a legal environment that constrains both bad actors and governments alike.

The third panel highlighted the many challenges faced by various industry segments. While representing diverse fields ranging from social media and health care, to electrical providers, the panelists brought to the forefront both the variance of threats faced by each group as well as common problems. Within their common problem set, there is a market need for the establishment of information sharing and the resultant effectiveness that enhanced information can bring minimized risk. Here again, the importance of synchronization arose as central to the problem of addressing many of the cybersecurity challenges facing the nation. Rigorous testing environments, strong partner commitments, good processes, and robust communications might not prevent initial points of infection, but such information and practices will prevent, or at least dramatically slow the spread of certain attacks.

> TO SYNCHRONIZE SECURITY REQUIRES US TO RECOGNIZE THE ROLE THAT WE ALL PLAY IN THE COMMON DEFENSE OF THE NATION.

Nowhere was the information problem more pronounced as an impediment to synchronization than in the fourth and final panel of the day. Synchronicity cannot occur in the absence of trust. While the earlier panels focused on the challenges faced by various industries, the role of information sharing, and the evolving power of the Internet of Things, the end result is that for progress to be made, for information to be shared, for systems across the private and public sectors to be secured, requires a robust framework of trust. The panel included representatives from industry, Department of Homeland Security and the FBI, the key theme was that, while not perfect by any stretch of the imagination, the US is working hard to build the structures that facilitate trusted relationships. There is a need to both build internal capacity for various government agencies and institutions, and leverage external capabilities. We must have the ability to achieve measurable gains, and open our communications with one another. Government is not the sole provider of security, yet at the same time it plays a vital role in securing national cybersecurity. As the government develops the capacity to coordinate and facilitate responses to various cyber incidents nation-wide, it becomes increasingly important to demonstrate an ability to consistently and appropriately respond.

Amidst the JSA panel discussions were four senior leader talks given by the former U.S. Army Chief of Staff General Raymond Odierno (USA, Ret), Lieutenant General Edward Cardon, Commander, Army Cyber Command, Secretary Jeh Johnson of the Department of Homeland Security (DHS), and Congressman Mike Pompeo (R-KS-4). These talks focused on three major issues, each of significance to national cybersecurity. First, General (R) Odierno and LTG Cardon both focused on building the intellectual capital necessary to secure not only the present, but the future. While their emphasis was largely on Department of Defense (DoD) cyber issues, they also stressed industry's obligation to mentor and educate talented Americans. Facing a massive shortfall of trained cyber professionals across all sectors is a national security challenge, and one that cannot be addressed by government alone.

Second, Secretary Johnson addressed the robust cyberspace efforts currently under way by DHS. His emphasis on domestic governmental efforts illustrates a powerful recognition by the federal government of a critical need that is currently being inadequately met. By establishing the National Cybersecurity and Communications Integration Center (NCCIC), providing support to Computer Emergency Response Teams (CERTS), facilitating Information Sharing and Analysis Organizations (ISAOs), and a number of other potent initiatives, DHS has seen the competence and robustness of domestic cybersecurity markedly increase. While the domestic sphere of national cybersecurity is still incomplete, it is growing and adapting to the evolving threat landscape. Most crucially, DHS sits at the fulcrum of domestic cybersecurity efforts.

Third, Congressman Pompeo closed the conference by reminding all attendees of the value of information sharing, and the need to extend information sharing to Congress. He expressed a desire to include lawmakers in the process of understanding what legislation is required as well as what legislation needs to be amended. He indicated that information sharing between government agencies and industries will synchronize cybersecurity. This synchronization will positively impact the United States Congress as they write laws fund budgets and provide appropriate resources and enablers/constraints to achieve the cyber environment we desire. Congressman Pompeo closed by reminding all attendees that no amount of synchronization can function in the absence of trust. Trust is built by being honest about the needs of the nation.

The panel discussions and speakers are only part of the overall importance of the JSA summit. In a network environment spanning every industry and every aspect of our government getting to know other decision-makers and their thought processes is as important to listening to panels and keynotes. To truly synchronize security, industry and government must stand eye to eye and ask one another hard questions, and be prepared to receive answers that make us each uncomfortable. The Joint Service Academy Cyber Security Summit brought together a large group of diverse decision-makers from industry, defense and homeland security, and in so doing opened vital lines of communication that will serve as the foundations of national cyber defense and resilience in the years to come.

BREAKOUT THE CYBER SCOTCH . . . THIS ROUND IS ON US

BY STEPHANIE K. PELL

ASSISTANT PROFESSOR AND CYBER ETHICS FELLOW ◆ ARMY CYBER INSTITUTE ◆ DEPARTMENT OF ENGLISH AND PHILOSOPHY ◆ UNITED STATES MILITARY ACADEMY AT WEST POINT

“IoT [Internet of Things], that scares the hell out of me.” General Raymond T. Odierno (USA, Ret), the 38th Chief of Staff to the Army, minced no words in communicating his perspective on, among other things, the challenges inherent in securing the cyber domain—a space where public and private equities and interests are inextricably intertwined. NSA Deputy Director Richard Ledgett echoed the General’s concerns when, in describing the vast scope of the problem, he emphasized that, “the cyber domain is where this nation stores its wealth, treasure and most important information . . . our innovative ideas, business plans, and negotiating strategies are all online.” For better or worse, all of our ‘things’ are coming online. Indeed, Deputy Director Ledgett noted that, by the end of 2016, over 6.4 billion things will be connected to the IoT worldwide. The cold, hard truth is that every new device that comes online is an additional attack surface for those who seek to exploit those things, whether to gain access to our national treasure or to enable “future computer network attacks to disrupt, deny access, or destroy critical infrastructure.”

This ever-expanding connected world continually presents new challenges for securing our information in a manner that takes sufficient account of the human factor. That is, humans are often the true exploitable endpoints, if you will, of mobile devices and entire communications networks. Indeed, as panelist Dr. Andy Ozment remarked, “there are human beings behind everything we are talking about.” Simply put, cybersecurity is only as strong as its weakest link, which, more often than not, involves a human being. To succeed, information security practices must prove usable to human actors. Usable security is, therefore, a research area that continues to ripen for exploration.

How we go about securing our national treasure and critical infrastructure, which inhabits and often itself constitutes the online environment, is a daunting challenge. We don’t have to be the Deputy Director of the NSA, the Chief of Staff to the Army, the Commander of US Army Cyber Command, or the CEO of Sony to lie awake

at night brooding over threats posed by malevolent actors in cyberspace. Standard issue government employees and individual citizens who, for example, find that their email has been hacked or their highly sensitive personal information breached due to sub-standard security practices followed by their own government, confront these challenges and the myriad anxieties, great and small, they produce. These kinds of episodes, whether they occur due to government or private misfeasance or malfeasance, undermine our trust in the digital world, which discourages our full engagement with its economy, and distances us from the tremendous benefits it offers to humankind.

Highlighting yet another inventive milestone in the current rush to ‘cyber-ize’ seemingly everything by connecting it to the Internet and attaching the prefix “cyber” to its familiar name—in this case, a newfangled cyber toaster that literally burns the weather report onto the surface of your morning toast—Dr. Andrea Matwyshyn, panelist and astute commentator upon information security, noted the importance of considering IoT’s increased attack surface and once exhorted, “Well, breakout the Cyber Scotch!”

But if there is one silver lining to this arguably dark narrative, it is, ironically, the human factor. The resounding positive message from all of the distinguished speakers, panelists and participants at the 2016 Joint Service Academy (JSA) Cyber Security Summit was one of the necessity to form partnerships—public/ private/ academic partnerships where no one individual, institution or entity has the market share on good ideas or owns, exclusively, the problems and solutions. We need to have a real and honest dialogue with each other that ultimately promotes trust for purposes of a journey that we are all in for the long, arduous haul. We can and must do this.

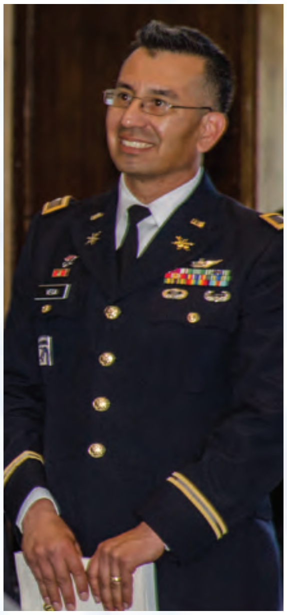
How such discussions, which are as multifaceted as the challenge itself, might proceed in the present and the very near future is, perhaps, one of the most pressing elements of the Cyber Grand Challenge. It is easy to criticize all of the various players and stakeholders in the eco-system. As hinted at by Congressman Mike Pompeo, however, such divisive rhetoric at best merely erects a barrier to useful communication and cooperation. At worst, however, it can obfuscate the real issues at stake. The real challenge before us lies in the hard work of listening to and educating each other. In this process we will learn to speak each others’ languages and understand each others’ perspectives, even when those perspectives run counter to our own specifically defined mission as a particular stakeholder in the eco-system. In short, we all must learn and engage in the art of empathy.

It’s time to roll up our sleeves with renewed commitment to continuing the hard work of understanding the perspectives and challenges that each ‘player’, big and small, faces so that we find workable solutions, if not perfect ones. This kind of dialogue among people will promote the kind of strategic thinking that, Lieutenant General Cardon, Commander of US Army Cyber Command, hopes, among other things, “will prevent strategic surprise.” So, as a provisional act of cautious optimism, we at the Army Cyber Institute invite everyone to “pull up a chair, put on your thinking cap and breakout the Cyber Scotch, top-shelf, please . . . this round is on us.”

CYBERSECURITY IS ONLY AS STRONG AS ITS WEAKEST LINK.

APRIL 21 WELCOME REMARKS

COLONEL J. CARLOS VEGA



We hope you were inspired by last night's ceremonies.

To our hosts Lieutenant General Caslen, Mark McLaughlin, and our United States Military Academy Cyber Chair, Lieutenant General Hernandez, General Odierno, General Alexander, and Lieutenant General Cardon, thank you for your support. I want to acknowledge you, our audience. This was an unadvertised event. By invitation only; when we decided who was going to get the invitation we said it had to be someone who is a person of influence, a thought leader within their company, within the discipline, within their domain; that's why you are here. You are the true VIP's at this event, so thank you for coming.

With that, we'd like to start with the introduction of Mr. Mark McLaughlin. Mark is a 1988 graduate of the United States Military Academy. He is the current Chair of the National Security Telecommunications Advisory Committee (NSTAC), and serves as President, CEO and Chairman of the Board of Palo Alto Networks.

There is one thing I forgot to mention; one special announcement for one our key leaders. An individual who is larger than life; I would like to acknowledge that it is Rick Howard's birthday today. So Mark, if you don't mind joining us up here.

MR. MARK MCLAUGHLIN

Good Morning and a happy 39th Rick! It is a great privilege for Palo Alto Networks and myself to sponsor this event. Just real quick background: A little of two years ago, I was invited to visit the Army Cyber Institute and met with Lieutenant General Hernandez and Colonel Vega. I was sitting in their offices, which is a little bit of an overstatement outside the gate area and it struck me what they were doing at the ACI was so much like a startup. So here we are for the second year in a row. It's just fantastic to see how fast this has grown in one year's time, and I think the future looks exciting. It is a total privilege for me to be part of this network. I think this year's theme of Synchronizing Security is spot-on. We have a giant job of maintaining, and at this point, I actually think restoring trust in the digital age. We are living in a totally different age because of digital technology, it's outstanding! We think about what has occurred in the last ten to fifteen years, things like cloud computing, SaaS, mobility, and social network, etc.; these are a list of things that are positives. It is hard to imagine living a life without Internet connection. But the very things we like about this new age, productivity enhancement, has a flip side of which is security. I believe security is actually a marker on the table for trust. If people do not trust digital networks, they are not going to use it, at least not as much as they use to. If that occurs, we will have the largest economic impact that has ever occurred in history—those are the stakes.

If you think about banks and money, there is not any money anymore, just a concept. It is all digital. If you check your bank balance on an iPad or phone, and if we all had $1,000, and seven minutes from now we check again, all we had was $10 in the account, this meeting will be over. Everybody will be in the hallway trying to find a solution, and attempting to put their hands on something physical. Importantly, it would not matter whether it was actually gone. All that matters is the perception that it was gone, and in the digital age perception is reality, and perception is completely vital to the trust of the systems. In that case, you no longer trust your financial institution and that is a real problem.

In the last six months you may have read about ransom attacks. These bad guys are completely disabling hospital systems using ransom attacks because they know it's a life threatening situation. That's happening right now at multiple hospitals. If people stop trusting the very infrastructure that underlies the digital age, whether the financial system, healthcare, assets like critical infrastructure control systems. In the digital age there is a fine line between a well ordered highly productive society and one in chaos, and the line is razor thin. The next macro trend to impact all of us is Internet of Things. You have fifty billion more inputs in the Internet, and from an IoT perspective it is going to touch all of our lives, from folks in uniform, hospitals, banking industry, and personal data.

Three things are really necessary for us as a society to figure out in order to change the dynamic. One is technology; we have to figure out how to do more prevention and it's never 100 percent, but the more that we can get done, the more we can raise the cost to attackers. We have to get that done.

The second thing is sharing information. The third thing is education. It is critically important that people start to take responsibility for their actions with proper cyber-hygiene: employees, it can be the troops, or your kids. On your table is a book that the New York Stock Exchange just published; we are proud to participate in that important publication. "Navigating the Digital Divide" teaches us how to think about cybersecurity and fiduciary responsibility in a non-technical way. We are proud to be associated with the Tech Museum of Innovation in San Jose, California. This is a fantastic museum, and if you are in the San Jose area, please check it out. It is something we would love to see replicated across the United States. There is a common exhibit called Cyber Detective that we sponsor. It's twice the size of this room and focuses on cybersecurity. The exhibit is geared towards kids from 7-19, and teaches them how to defend against cyberattacks.

What are we doing here at the JSA Cyber Security Summit? One is conversation from the technology perspective regarding more automation in this environment. The second thing is from a sharing perspective, in fact there are conversations and relationships that will be formed. There will be no meaningful sharing in the future without the personal relationships of people trusting each other. And third, from an education perspective, it's exciting to see the cyber focus at all the Service academies.

The last thing I'd like to mention is leadership. We have leaders that clearly made JSA a priority to be here and spend time in this space. I thank everybody for doing that!

It's my privilege to introduce the next speaker.

Lieutenant General Edward C. Cardon was born in Texas, raised in California and was commissioned as an Engineer Officer from the United States Military Academy in 1982. LTG Cardon has commanded at every level from company through division. Prior to assuming command of the United States Army Cyber Command, he was the commander of the 2nd Infantry Division based in South Korea. His education includes a Bachelor's of Science Degree from the United States Military Academy and two Master's Degrees—one from the National War College and the other from the United States Naval Command and Staff College, both in National Security and Strategic Studies. Today, I understand that he will be providing an update of the status of cyber in the Army, and I welcome LTG Cardon. Thank you Sir!

ARMY CYBER UPDATE

LIEUTENANT GENERAL EDWARD CARDON ⋄ COMMANDER, U.S. ARMY CYBER COMMAND AND SECOND ARMY

It's really a privilege and an honor to be here today and Mark thanks so much for the introduction, and a warm welcome to all the distinguished leaders here. First, I want to start out by congratulating West Point for winning the Cyber Challenge. I took some grief for that last year in the Cyber Command updates, and this year, I can't wait to get back to our next update, so well done!

I want to build upon what Mark talked about and the IT revolution, which has clearly transformed our society; it's also transformed our military. But to me there is another revolution ongoing right now, and that's in wireless mobile, Big Data, encryption, and Internet of Things. We start to think about how this is going to interface in an environment where threats are increasing. I would say over the last two or three years we have seen more destructive attacks. The vulnerabilities are going up along with the challenges. The complexities are increasing with the Internet of Things. And with North Korea and Sony, and last night Mr. Ledgett talked about the Ukrainian cyberattack, what's the Army doing about all this? Six years ago U.S. Cyber Command was formed, and from that the Army created Army Cyber Command. It will be six years old this September. I still consider ARCYBER a startup, that's what our Silicon Valley teammates have called us. But we handled the creation of ARCYBER a bit differently; I will argue we did things harder because we created a new command, we just didn't take another command and re-designated Army Cyber Command.

I want to give you an update on just the last two-and-a-half years. In addition to the ARCYBER stand up, the Cyber Center of Excellence was stood up. The way we develop our Soldiers and civilians, and the way develop doctrine, all of that is done in our centers of excellence. That was established in the last two years at Fort Gordon in Georgia. The Army Cyber Institute was also stood up. I was here when it was just two people and now look at it today.

We are creating tremendous synergy at Fort Gordon because you have the Army Cyber Center of Excellence, the National Security Agency in Georgia, the Cyber Protection Brigade, which was created in the last two years, and the 7th Signal Command, which handles all networks in the continental United States. There are military intelligence units and the list goes on. There is no place that we have that level of synergy.

You hear a lot about the Cyber Mission Force, and its 133 Cyber Mission Teams; the Army was tasked with standing up 41 of these teams. In September of 2013, we had 2 at the initial operating capability. Today, we have 36, which 10 of those are fully operational, and we already have our first National Guard in Cyber Protection Team at initial operating capability. The Army also decided in addition to the 41, we're going to build 21 more teams. There are 11 National Guard and 10 in the Army Reserve and those are being built over the next two years.

A critical piece of this development is the establishment of a Cyber Branch. The last branch the Army created was Special Operations in 1987, before that, Aviation in 1984. I view this as the first new branch of the twenty-first century Army. The Cyber Branch is essential to manage and provide a pathway for cyber officers, Soldiers, and civilians to move up. How fast was this done? It normally takes about five years to establish a branch, but under Secretary McHugh and General Odierno's leadership, just five months. The branch is established today with 350 officers, and a number of Cadets you saw last night will soon join the new branch, which is a very competitive process with one out of seven applicants selected.

We also recognize the Cyber Mission Force supports our combat priorities, and there is also this responsibility of cyber for the Army and we call it Cyber Support to Corps and Below. This was just an idea a year ago with no real capability other that adapting other capabilities. We've done a series of pilots; we just finished one at the National Training Center with the Stryker Brigade, and it's the first time that we had a Brigade Commander using cyber effects integrated with what he was trying to accomplish on the ground. We've learned a tremendous amount and this is starting to scale in a much larger way.

The Army is identified as Executive Agent for Cyber Training Ranges for the Department of Defense. We just got that mission about a month ago and there is a lot of money against this. The Army worked to get this mission because when you think about it, it's training that is going to determine who has the best cyber operations. I believe the way the Army has set up its training and delivered the combat dominance that we have seen over the last fifteen years, we can do the same thing with cyber.

Mark touched on hacking cars, Internet of Things, and I recently did a talk on platform security. This is a growing problem, which Mr. Ledgett addressed last night. In 2011, cyber experts started talking about it might be possible to have a car hacked, and in 2012 they thought it was definitely possible. In 2015, cars were being hacked in America. You all saw the recent 60 Minutes episode; that's five years! Five years from idea to hacking a car. When you think about cars you normally think mechanical; we do not see one million lines of code that actually make it work.

Finally, we must address cyber acquisition, and the challenge that we can't get our cyber capabilities fast enough. I think the Army is trying new ways of acquisition with two unique initiatives; one is our idea of using cyber challenges to deliver actual capabilities. Our first one delivered capabilities in seven months, which does not sound very fast to some of you in industry, but for us its light speed. My challenge is to speed up the acquisition process–the core threat is moving faster and that's where the public-private partnerships are becoming so important. The Secretary of Defense is really driving cyber acquisition with the establishment of the Innovation Unit in Silicon Valley, which we have officers involved in. We are also involved in Silicon Valley with projects at Stanford University.

There are three areas that we share: one is risk, and this is shared risk, which Mr. Ledgett talked about last night. Whatever happens in the private sector happens in defense or vise-versa. It's agnostic. The other challenge is related to who is accepting the risk. Because for years we pushed risk off to the CIO community. The CIO community accepted risk on behalf of the organization, but that's not the way it is now, as we become more interconnected. I believe this is an area that we really should work on together.

The second shared area is culture. I absolutely agree with Mark that offensive cyber dominates the defense. I normally describe it this way – you're asking humans to be 100 percent right all the time regarding cybersecurity. That's not going to happen and we know it. If we can do some things with cyber education, develop the right architectures, and have our people doing the right network hygiene, we can really reduce those numbers. If we could bring offensive and defensive cultures closer together, I think we are going to be much better off.

The last area that we all share is our legacy systems. When we start connecting legacy systems to the Internet or into a closed network, we don't realize they consist of other systems. What is the way out of this? The first part is right where we are sitting, I believe its education and compliance. Secretary Carter is focusing on compliance – we are not going to accept these waivers anymore. So when I put the order out to disconnect about 150

ARMY CYBER UPDATE

systems, I received some very interesting phone calls. My point is that changing the culture is essential, but it goes back to the education.

The second part is a process and I'm not a big process person, but we have the right people to make our processes work. I was recently at Boeing looking at their cybersecurity, and it's very interesting the extreme control they have over their architecture that goes into their aircraft.

But the last part of our process deals with mission assurance so we can accomplish the cyber mission on behalf of the United States. We have to think about supply chain, human resources, and logistics. How do you assure that you can deliver that message to the right place at the right time? And I think that's part of the way we have to adjust our processes.

I look forward to the questions. Thank you very much!

QUESTIONS & ANSWERS

Q: Great job on getting the Cyber Mission Teams stood up, I think what would help especially for industry if we can go over the philosophy of what the teams are for?

A: Very quickly, I'll give a description of the Cyber Mission Teams. There are five types of teams. We start first with the National Mission Teams and the National Support Teams. These teams work hard. I often describe them as hacker vs. hacker. We have the National Support Team, which heads the back-end analytics and the capabilities. Then there is the Cyber Combat Mission Team, and Combat Support Team. They work with commanders around the world in accomplishing the big jobs. That's roughly half of the force. The other half of the force is focused on the defense and the Cyber Protection Team.

L TO R: ACI STAFF LTC JAMES FINOCCHIARO, LTC DANIEL HUYNH, CPT MATTHEW HUTCHISON

L TO R: COL ANDY HALL WITH GEN (R) RAYMOND ODIERNO

KEYNOTE PRESENTATION

GENERAL (RET) RAYMOND ODIERNO

I was told I have 45 minutes. One day this fourth grader was doing a report for a class on Julius Caesar. He said Julius Caesar was a great man. He commanded thousands upon thousands of forces and was a political leader. He gave a long speech, and they killed him. I have learned from that time, it is probably not a good thing to give long speeches.

First, I'm not a technical cyber person, but I'm the person and people like me who you should focus on: Commanders, Chief Executive Officers, leaders, because they are the ones who are going to help make cyber work. Defend against attacks whether it be in governmental entities or private entities. Unless commanders in the military, or civilian leaders in our government, or Chief Executive Officers decide this is an important problem it will not get solved. One of the things I want to talk about this morning is what we need to do in cyber. I'm going to talk about three things: first, I'm want to take a minute and discuss the Army Cyber Institute; second, I want to talk about some of my experiences and lessons learned as Chief of Staff; and third, I want to talk about my new role as Senior Advisor for Jamie Dimon at JPMorgan Chase. One of the things he asked me to do is take a look at cyber, and I want to give you some initial thoughts from the short time I've been working in the financial sector.

First, I think everyone believes and understands that cyber is a real threat. We know these threats are incredibly dynamic and are changing constantly. The threat is evolving, it's sophisticated, and you have both state and non-state actors trying to use these threats against us and our industries to influence and gain power around the world. The tactics and techniques used by our adversaries are constantly evolving. Those are the challenges that we all face.

The one thing I have learned in leading complex operations, you have to have a comprehensive approach to solve any difficult complex problem. The solutions we must develop cannot be just governmental or military solutions; we have to build this synergy within our government, with other governments, and also with private industry. That's the only way that we are going to solve this problem. It is up to us to think through these challenges. I think that's one of the real things that we must do at the Army Cyber Institute. I remember four years ago I came here to visit, and understand, I had been the Chief of Staff of the Army for about six months, and we had a huge cyber problem and I wanted to solve it here with West Point's Army Cyber Institute. It's truly great to see how far it has come. There were a couple of things I wanted to do. First, build partnerships between other educational institutions, whether it be Stanford, Carnegie Mellon, or Columbia. I want to build relationships with private industry and partnerships with the financial sector and with the energy sector, etc., etc.

There are a couple of things that we have to do. Obviously, I believe the ACI needs to focus on cyber policy; US policy and international policy, because in many ways that is going to drive how we solve these cybesecurity challenges through a comprehensive approach. New policies have to deal with public-private partnerships, intergovernmental partnerships, and international governmental partnerships.

We also have to expand our technical and operational expertise. I worry more about the operational expertise than I do the technical expertise. And that goes back to the Commanders and CEO's that I talked about earlier. The reason I've become so engaged with cyber goes back to 2007 when I was in Iraq 2006-2010; first as the Multi-National Corps-Iraq Commander, and as Commander, Multi-National Force-Iraq. Up to that time, I really had not thought much about cyber, but that soon changed because of events on the ground. First, we had an insider threat with Private Manning while I was in Iraq. It had devastating effect! We had external attacks on our systems from other governments so I realized we had a problem. Then I had a visit from a guy named Keith Alexander; when we sat down and talked about cyber capabilities

KEYNOTE PRESENTATION

that could be put into place allowing the Multi-National Force to gain advantages on the battlefield.

So for the next four years, I learned from experiencing the importance of defending yourself from insider threats, the importance of discipline, and the importance of understanding that if you do not follow rules, you are going to have problems with your own capabilities. I learned about the external challenges with people always trying to phish and get inside your networks, steal data, and shut you down. I also learned about the potential of offensive cyber operations. I became a huge fan and understood the operational necessity of cyber operations. What I just described from a military standpoint, I believe applies to civilian industry. There is nothing I said that does not apply to any civilian company developing their cyber capabilities. I believe it's important that we continue to think about cybersecurity, collect and develop best practices. And oh by the way, conduct after action reviews in the Army. When I first came in the Army, we didn't do anything like that, but in the 1980s we went to our combat training centers where we gave brutal after action reports on how well you did, and mostly how poorly. That's what made us grow the Army. We have to do the same thing in cyberspace. We have to constantly conduct assessments on how well we're doing. We have to have outside teams, red teams as we call them to make sure that we take a hard look at how we are protecting ourselves. We should also think about what I call active defense. This applies more to civilian entities because they are allowed to defend themselves. I believe there is room for active defense; be more aggressive in defending yourselves against threats. I think it's important that we think through this problem and how we might want to handle active defense in the future.

THESE CYBER THREATS ARE INCREDIBLY DYNAMIC AND ARE CHANGING CONSTANTLY.

We have to take on two words—what does cyber intelligence mean? How do we develop cyber intelligence? What is cyber intelligence? What does it mean to the military? What does it mean to our government, and what does it mean to our civilian enterprises? What do they need? What is the information sharing that is needed in order to deal with the cyber challenges we face? How do we define and share protocols in this space, and how do we train and retain the workforce? Other questions that need to be asked regarding employee compensation. I believe that is not what keeps people. Whether it's in the civilian or the governmental sector, it is all about job satisfaction, and creating an environment where employees believe that they can work and contribute in a dynamic workplace developing new capabilities with the freedom of action to come up with new techniques, and that their work is appreciated. And if you do that with the right compensation you will be able to keep people involved in the cyber domain. It is important that leaders of your organization, the Chief Executive Officers and Commanders, recognize this important retention construct.

Finally, I think we have to build methods of collaboration. Again, with a comprehensive approach. I would love to see the Army Cyber Institute take a look at how we can improve collaboration within our government, other governments, and with private industry. That collaboration will be a key to our success in the future. So, although ten months ago I could have directed the ACI to do all these things, I just have to ask that they look at doing some of these things.

I just want to spend a minute on my cyber view when I became the Army Chief of Staff. We were behind the power curve when it came to cyber, and frankly we talked about standing up the Army Cyber Institute, and the Cyber Center of Excellence, and addressing training. If I told you how many times people told me there is no way we can do this, or we shouldn't do it, it's not the right thing because there are a lot of others stovepipes out there. It takes leaders to work through these challenges and provide a bigger vision that allows you to make sure you reenforce what is necessary to move forward. We need that leadership today because it's getting more complicated. I had not heard of Internet of Things until this JSA conference. That scares the hell of me! That's going to present new challenges for us. We are going to have to aggressively come up with the solutions to solve problems associated with Internet of Things.

I would tell you this, as leaders of change, you have to have a vision, you have to communicate that vision, and be resolute about it, you have to get in and you have to force resolution. In this industry we have to do that. It's been said at this conference that we do not have enough people interested in cyber or receiving a technical education, so why not? That's awful! We know the youth of today. This is right up their alley and you are telling me we can't get enough people to do this? That's leadership. This is a leadership issue. That means we are not being aggressive enough at setting up programs that allows young men and women to move forward in this area.

We have to figure out where those road blocks are. Why aren't we doing this? Not because we don't have the talent or capability, it's because we are not investing in it. What's happening is we do stovepipe investments. JPMorgan invests in cyber, the U.S. Army invests, Con Ed invests; we need to build synergies of educational opportunities that will allow thousands to be trained at a much cheaper rate to solve this problem. I think these are the kind of things we must look at.

The last military item I will talk about is strategic cyber. When we focus on strategic cyber at the national level, the objective is on protecting our critical infrastructure and making sure our nation is not attacked. We have operational cyber, which is for the joint commands around the globe to make sure our troops are protected and conduct operations. General Cardon touched on four levels of operations. We have not invested in this enough. In the future, tactical cyber gives us a huge advantage as we can conduct operations around the world. We need to develop enhanced capabilities in order to be successful in this space.

I mentioned at the beginning of this morning's talk, that last year I became a Senior Advisor at JPMorgan Chase. Let me just relay to you how JPMorgan views cyber. Obviously, it is a strategic priority. Information is the life blood for financial institutions and frankly it is of any company. Your ability to protect information is critical. There are incredible cybersecurity investments being made not only by JPMorgan, but by many others. The amount of money being spent on cybersecurity is significant. JPMorgan has about 2,000 people working cybersecurity around the world. JPMorgan runs 24/7 operations in the US, London, and Hong Kong. They have to protect themselves 24/7, and so for them there is nothing more important than cybersecurity. They have to do this by developing new technologies to defend their networks. Sometimes it is not even technology, it's the concepts and how you use the technology that is available. You want transactions protected, and enhance the processing controls to eliminate cyber fraud.

I think the financial sector is a leader in these areas, but with so much work to do. I have been pleasantly surprised that within the financial network sector there is no competition regarding cybersecurity. All the major financial institutions are either working together or want to work together to solve these problems. Because it is a common problem, and not about competition for clients. It is about self-preservation and making sure that we work together to come up with the right solutions to protect our financial institutions. It is important that financial institutions have strong and effective partnership with other government agencies. JPMorgan supports a framework for protecting critical infrastructure. This is about a comprehensive whole-of-government approach to solving the problem.

Let me just list a few things that I think are important to build this cooperation between government, financial institutions, and other institutions: intelligence sharing, contingency planning, conduct national level exercises, develop best practices, vulnerability evaluations, and streamlining security clearances. These are things that have to be done between the government and private industry in order for us to deal with this ever evolving threat.

As I said earlier, this cyber threat is growing from state and non-state actors. In some ways, I really worry about non-state actors because they will not be regulated in any way. We must mitigate our vulnerabilities and the best way is through collaboration. Real honest collaboration within the government, and with government and private industry. These are the real issues that I think we should talk about when we get together at the JSA. These are the issues that we have to solve. Addressing these issues will allow our technical experts to assist in solving the technical issues of protecting our networks. I want to compliment everyone today for putting JSA together, an incredible forum, something that I believe is critical to our nations' security, something that is critical to our economic security, something that is critical to our way of life, because I believe within the next five years there will be an attempt to conduct a devastating attack on our infrastructure somewhere in the United States. With that, I thank you very much.

CYBER GRAND CHALLENGE PANEL

LEFT TO RIGHT: MODERATOR DR. ANDREA MATWYSHYN WITH PANELISTS MR. MARK BRISTOW, MR. SCOTT MONTGOMERY, AND PROFESSOR STEPHANIE PELL

INTRODUCTION

Good afternoon. I would like to introduce Dr. Andrea Matwyshyn. She's a legal academic studying technology innovation and its policy implications, particularly corporate information security regulation and consumer privacy. She is currently a full professor of law and professor of computer science at Northeastern University, a faculty affiliate of the Center for Internet and Society at Stanford Law School, and a visiting research collaborator at the Center for Information Technology Policy at Princeton University, where she was the Microsoft Visiting Professor during 2014-2015. She is a US-UK Fulbright Commission Cyber Security Scholar award recipient in 2016-2017. Thank you very much for joining us.

DR. ANDREA MATWYSHYN

It is a great honor to be with you today, and I thank the organizers for inviting me. It is a privilege to talk to such an esteemed group.

Today, if I may, I'll share a few thoughts with you on the topic at hand with respect to security and the Internet of Things, and after doing so, I will briefly introduce my esteemed co-panelists and turn it over to them for brief comments followed by some interactive questions among us, the panelists. And then we'll open it up to questions to all of you.

So with that, please allow me to share a few thoughts about what I see as an emerging set of challenges with respect to the millions and probably billions of gadgets that we are connecting to the Internet, the Internet of Things. My comments will certainly reflect my own background in the private sector. I started working as a corporate lawyer in 1999 counseling clients on matters of information security and structuring corporate transactions. I shifted to academia, and followed the civil side, and had the privilege of serving as the Federal Trade Commission Senior Policy Advisor on security and privacy and their Academic in Residence in 2014. In that role, I had the privilege of seeing the challenges that federal agencies face, and their enforcement of data security.

As we consider the Internet of Things, I would like to highlight what I see as some avoidable emergent coordination challenges across different pieces of our information ecosystem. These challenges are partially from framing the way we are thinking about questions of security and information flow, and making our nation and its citizens safer. I'll share in particular four challenges, suboptimal framings perhaps, in the way we talk about these issues. The way we talk about these issues is particularly important in light of the Internet of Things because it crafts the presence or absence of a common discourse, which allows us to work together, either more effectively, or potentially less effectively.

The first of these challenges, and there'll be four in total, relates to a phenomenon that we might call Internet Exceptionalism. When we consider the Internet of Things, we are talking about technology and security, and not simply talking about Internet things. These are physical objects impacted by information flows and transformed through technology. This means that we frame things, as we heard from our amazing pair of speakers, with a mindful eye to the confluence of physical security questions, and digital security questions, and human elements in compromising or supporting the security that we are trying to engender in our systems.

In particular, IoT presents a formidable challenge to national security and consumer protection simultaneously, because IoT presents an attack surface and a vehicle where a remote attacker, whether it's a nation state, rogue actor, or criminal enterprise can compromise and leverage vulnerabilities in these devices to cause civilian harm in new ways that we have not seen before. This is a meaningful shift from my perspective in the possible attack vectors that we need to consider. It also highlights the urgency of synchronizing, in light of the theme of our conference, the discourse across public and private sector conversations regarding security.

This brings me to my second point. When I speak about technology and security, I tend to just use the word security, and that's a product of my own background in, primarily, the private sector, and the era in which I started working in this space. The second coordination challenge is that we do not pick the best words in all cases. In Congress, there's a risk of selecting technical sounding words that do not map perfectly to existing technologies or allow for the security researchers or the professionals who engage with them to understand the implications and practices and implementation that Congress or a particular regulator was striving for in choosing the words.

Unfortunately, the word cybersecurity is one of those words now in Washington, DC. Depending on which agency I am speaking with, and which group of very earnest, well-intentioned policy makers, they are operating from a slightly different operational understanding of what that term means. For example, the Federal Trade Commission does not use the word cybersecurity. They speak of data security. But, the DOJ and the FBI speak of cybersecurity, cybercrime, etc. Helping to construct common understanding of what the big picture security goals for us are, both in terms of our digital information flows, and our physical information controls—that's the next step.

This brings us to our third challenge. I call this the problem of "technology unsuitability" particularly when we're taking about critical infrastructure. There are some systems that are so sensitive or full of so much legacy code that connecting them to the Internet is simply too dangerous. In some cases we are connecting systems, not because we really need to or because we thought through the functionality gains that are not otherwise achievable, but simply because we can. Colloquially, you are talking what we call a better-with-bacon problem. I'm sure all of us has had the experience going to a restaurant with a vegetarian friend. The menu has a bunch of options and the vegetarian friend finds the option that appears to be vegetarian, but when the dish arrives there are ample sprinkles of bacon on top, because that's a hidden bonus, right? For someone, who's a meat eater, yes it would be, because bacon is tasty. But for a vegetarian it was an unexpected and unwelcomed surprise. Knowing the user, knowing the goal of the mission, in this case achieving a fully vegetarian meal, that's something that sometimes gets lost in the technology creation process, and in the technology deployment process.

The fourth item that I will highlight, and this is something that legal academics are guilty of, is the conflation of privacy and security. For me, those two are separate inquiries that relate to different operative notes of analysis. When we speak of security, we are talking about the properties of technical systems that are testable. We are talking about a basic level of care that we need to have in our society to ensure that my fantastic new cyber toaster, that emblazons my morning toast with the weather (real product by the way) is not also so vulnerable that it creates an avenue for an attacker to use that toaster as a point of entry onto my VPN, and my employer's network. Thinking through that attack surface in a holistic way is the inquiry we are undertaking with security. Privacy is about a social construct between an individual and a company, or an individual and society about the terms of data collection. That is something different, more socially constructed; a reality that's important to discuss, absolutely, but security is a scientifically testable set of properties of systems, and in that way we provide some differentiation. We benefit from this definitional rigor, and creating feedback loops, as we are doing at this conference, offers a positive step forward.

In my last minute, I'm going to present two controversial points that I hope will spur us to healthy debate and discourse. The first relates to information sharing. Although,

CYBER GRAND CHALLENGE PANEL

it is useful to share information, from my perspective, perhaps have not yet put in place the burden that should support information sharing to enable it to be more useful. Specifically, we should replace this paradigm with one of information vigilance. And so, instead of the brief-centric analysis or threat-sharing model, we should think about implanting reasonable floors of minimum security conduct across the board among all enterprises, private-public sector, etc., and correcting deficient structures and being able to classify and assess the severity of security vulnerabilities. But we need that to be able to scale, and have the data collection tell us what is going on in our system with respect to the security threats.

The second point to remember is that deterrence does not really work in this context, even though it is still the paradigm that some organizations are hoping will succeed with attackers. Deterrence will not work! We are sitting on a haystack of vulnerabilities with a deeply vulnerable ecosystem of critical infrastructure financial services, and IoT certainly. We are sitting on this haystack with a flame thrower and vulnerable to incoming attacks even as we might be successfully providing offensive maneuvers.

The vision that might help us here, and this is my last point, and then we'll introduce the esteemed panelists that I'm privileged to share this stage with. This idea comes from a somewhat obscure philosopher of science called Michael Polanyi. And what Polanyi told us is that when you have a really complex scientific problem such as security, to think of it as a coordination game, a puzzle, where you have a large group of equally skilled people working on this puzzle. They are working independently to put together sections of the puzzle, but they keep an eye on what everyone else is doing so that at the end of the day the puzzle comes together. Maybe this approach we take forward creates a holistic analysis of the strengths of each of our various pieces of the information of systems across Federal agencies, across the military, public and private sector, and to have this team using its best skill sets to make us all safer, while simultaneously coordinating in a loosely structured way. I would call that a reciprocal security inducement approach. And so I will leave it there, and now, I have the honor of introducing my esteemed co-panelists.

First, we have Mark Bristow who is the Chief for Incident Response and Management for the Industrial Control Systems Cyber Incident Response Team, ICS-CERT, at the National Cybersecurity and Communications Integration Center within the Department of Homeland Security.

Next, we have Scott Montgomery who is the Vice President and Chief Technical Strategist for the Intel Security Group at Intel Corporation. He manages a worldwide team of chief technology officers who lead the organization and the group's various business units responding to advanced technical innovation and security solutions.

Finally, but certainly not least, we have Professor Stephanie Pell, who is an Assistant Professor and Cyber Ethics Fellow at West Point's Army Cyber Institute where she teaches Cyber Ethics in the Department of English and Philosophy. She writes on privacy, surveillance and national security law and policy.

MR. MARK BRISTOW

Good morning, thank you very much for this opportunity, and thank you to West Point and the Army Cyber Institute. Thank you for bringing us all together today. As mentioned, my name is Mark Bristow. I'm the Chief for Incident Response for the Industrial Control Systems Cyber Incident Response Team (ICS-CERT). It's a lot of acronyms after all, it is the government. In my job, I bring a unique perspective to this issue. We are not tasked with supporting government defense, but specifically tasked and stood up to help private sector critical infrastructure organizations secure their systems.

I have the honor of working with private sector organizations on a daily basis who request assistance from the Department of Homeland Security to help them through some of the challenges they have in securing their environments. Just to give you a little perspective, last year we supported 295 different incidents at organizations across all the 16 critical infrastructure sectors; and that's just in 2015 Fiscal Year. We do a number of engagements with the private sector, and get a lot of what I call ground truth, and have some really meaningful conversations regarding the real challenges that you are facing. I would first posit that, especially as it relates to the Internet of Things, that the demand for this technology is significantly outstripping our capacity to smartly deploy and design. I think this is really the fundamental problem that we are having on the technical side; it's moving too fast. As we've been sitting here having these discussions today, there has been a couple hundred or maybe couple of thousand new devices plugged in to the Internet. This problem is growing exponentially and creating an interesting paradigm;

how do we actually start getting in front of the issue instead of lagging ever behind it?

Part of the problem is that we can't even agree on a definition of what Internet of Things means. If I took any ten of you in this room, and asked you to provide a definition of Internet of Things some of you might quote somebody else, some of you might come up with one, but I would probably get 15 different answers from ten people. Because it means different things to different people in different contexts. One of the issues we are having with this paradigm is framing it correctly.

We call it Industrial Control Systems issues. To give you a little context on just the ICS side of it, my definition of IoT doesn't really include Industrial Control Systems. At ICS-CERT we've been working with some security researchers who basically scanned the Internet and found 84,000 industrial control systems directly connected to the Internet in 2014. These are devices running buildings, running power plants, water treatment facilities. That's a big number. And this is a couple of years ago and having a very narrowly scoped definition of what some people would consider Internet of Things today. So, the problem is growing. Since 2014, we've had a couple of significant technical innovations that make this problem bigger.

Anyone have a Nest thermostat in their home? I'm going to pick on Nest a little bit because I've had a great session with one of their VPs of Development on a panel, and they represent the Internet of Things. If you're not familiar with Nest, they are the little smart thermostat that replaced the old Honeywell. And as a result it learns your habits and, so it knows that on Sundays at 2 o'clock you always take the dog for a walk, maybe it turns off the air conditioning to save you some energy. So there's cost efficiencies and its driving value for the consumer. These devices have been on the market for a couple of years now and they're actually getting a reasonably wide footprint. Nest in their earliest product had a built-in camera. The reason that it had a camera was a valid one. Their big challenge is determining occupancy. They want to know if someone is in the house, because even if you're working outside your usual pattern, if there's people in the house they don't want to turn off the AC or turn off the heat. They had a very rudimentary camera that basically detects motion in order to support that determination of occupancy. Well, that's all well and good, what if someone were to take over that Nest thermostat or break into Nest's corporate infrastructure? And, now they can start looking into, very low resolution, thousands and thousands or millions of homes around the world because they added that feature for a very, very legitimate reason. So we are getting a lot of unintended consequences when we start to design these products.

Another great example is Tesla. Any electric car drivers in here? I'm jealous if you have one. Tesla makes the electric cars and a good number of batteries as well. As energy demands are increasing and we're looking at grid reliability, one of the concepts that's come up is using those batteries that are moving around in those vehicles as batteries to support the grid. Electric power companies are starting to go to customers and offering 25% off your bill, if you let the company take up to 10% of your battery. It is a good deal for the energy company, they do not have to keep as much in reserve, which saves them money. Consumer get money back in their pocket. It is a win-win. But what enables this to happen? So now when you are pushing energy to the car, now you're pushing and pulling energy from the car and that requires coordination which means connectivity. So now that former one-way push now requires the energy company to talk to your car and your car to talk to the energy companies, so they can do that demand response. Now there's connectivity which did not exist before. Again what could happen if someone could get into your car and say, "I'll take the firmware"? Well, Tesla did that already. A little while ago Tesla came out with a new feature in their vehicles that said hey, we're going to be able to give you self-parking. It's going to park it for you. You didn't have to come into the dealership to get that software package installed, they push it to all their vehicles across the entire board wirelessly in one day.

While that's all great for Tesla, and they can make sure that patches and modifications are put in place, you can patch the entire Tesla fleet in one day over the web. This should be terrifying, right? Recently, I'm sure you're all familiar with the Ukrainians cyberattack on their electric power grid. I was part of the US government team that went to the Ukraine to work on that issue. One of the things that the attackers did in the Ukrainian example was override the firmware. It no longer it functioned as designed, and it could not be recovered in the field, or recovered at the manufacturer. What if I were to be able to get into Tesla's environment, and do the same thing to their firmware update? Tesla's vehicle footprint is probably less than one percent of the cars out on the road. But as these technologies are getting more and more embedded into our systems, we're going to see more and more permeate through the environment and these risks

CYBER GRAND CHALLENGE PANEL

that we probably didn't really think about when we were designing these products are starting to come into play in a more national context.

The final point I'll make is that this is a hard problem to solve. First, because it's already moving. At ICS-CERT, we deal with Internet connected control systems on a basically daily basis. The problem is just getting bigger and bigger as we move forward. We can say, hey this is why you need to patch your systems, this is the connectivity. But now we're talking about the general public, so it is entirely plausible that your mother-in-law may have a Nest thermostat installed in her house and never think about it again. And you don't really want them to really think about it again. They're never going to demand security in their products. They're not going to come back and say, hey you need to make sure that this Nest thermostat camera can't be hacked. That's not a thought that come across the general public. The challenge that we have and the question that I'll posit to the group is how do we work together to ensure that the vendors and product manufacturers that are typically responsive to pressures from the people they sell to, how are we going to encourage them, and incentivize them to start building the security into the product design at the beginning, so that it can't be utilized in unintended ways in the future. Thank you.

MR. SCOTT MONTGOMERY

I'm going to talk real fast. Thank you ACI for having me, there's a lot of bright talented people at Intel, but clearly none of them were available today. So, you got me. There's a great report, has anybody read the McKinsey Global Institute report on the IoT? I urge you to read it; it's not in jargon, if you're trying to get your arms around the Internet of Things, which I agree with Mark is the dumbest term in the history of marketing after the Cloud; that's the dumbest, then Internet of Things.

These are communities of interest, aren't they? This report by McKinsey points out two characteristics about why people are engaging, and what they're doing, and why they're doing it. Does anyone have any idea on what either of the two things are? They're not technical at all. One's improving one thing, one's improving the other thing. Can anybody guess? No guessers. I have Star Wars cards. All right. To sell more things, more targeted things, the right things, to their customers. One was to improve the top line. One was to improve the bottom line. The horse is out of the barn. There will be trillions of dollars spent on these devices because it makes companies more profitable and efficient.

We talk about being consumers and the desire for the toaster that gives you the weather. I just need toast, but there is one area where there is not a real separation between the IT technology and the operational technology. And that's healthcare. The Boston Consulting Group stipulates that the remote cardiac monitoring market in the US alone will be $1 billion in 2016. Let me say that one more time: remote cardiac monitoring. Anyone know what that is? That is your doctor making a change to your pacemaker over the live Internet. Did some go oooooh? Because I did that when I figured out what the hell that meant. But if your choices are to have a life-altering event in an emergency room or to have a change made over the live Internet, you'd probably opt with the latter. Insulin pumps, MRI machines, every device in healthcare is going live. The stethoscope is going to have an IP address. And it's not about convenience or the cool factor, it's about delivering better patient care, faster. So the horse is wildly out of the barn. There is no turning back, and we need to embrace these changes, because they will allow us to achieve mission assurance on the top line or bottom line on the private sector side. These devices are going to help us, so what do we do? Very quickly, there are four things that I would advocate.

First is know who you're buying from. The supply chain for these devices is going to be increasingly important. Figuring out what you bought and what you intended to buy is going to be critical. So identifying partners that are designing with standards, security and privacy, two separate topics, but in my mind critical.

If you look at ExxonMobil, for example, they make kerosene and gasoline in the same vat, but a different valve is opened for different ingredients, or the valve is opened for a longer time for one versus the other. At the end of the day the valve is open-shut, open-shut, open-shut. There's absolutely no information security value to it. There's no privacy value to it. But certainly there's the ability to be disruptive if you want to change a kerosene vat into something else, or make bad kerosene. So, the point is what is the device supposed to do, how do you measure deviations in what it's supposed to do, and how do you address those deviations as closely to the deviation time as you can? I heard the dam mentioned, the Rye Brook, New York, opened by Iranians. Does anyone know the size of that dam? It's like that big. It's really little, but the point is did that dam have to be on the live Internet? Maybe, maybe not. Did it have to be directly on the live Internet with a cable modem attached directly to the gate? Probably not. What's the purpose of the Internet enabling, what's the purpose of the device? Stay with it.

The next thing is automation. The number of live humans who are going to be monitoring IT is a fraction of what it needs to be. Whatever tasks can be automated or can be segregated by importance; really important tasks get an analysis, less important tasks get less analysis or automation. Automation is absolutely key.

The last thing is data classification. Not all data is created equal. I wear a particular brand of socks. It's not a secret. They're made by a company called Stance. I just told you, that's a piece of data about me that I just gave you. There's no value to it, but if you ask me for my social security number, I would treat it different. I would protect it and it's the same thing about your organizational data as well. We should be protecting the most important data with the most important scrutiny and the most important analysis. And the less important data, leave it to automation, leave it to less trained, less highly trained workers. That's my time. Thanks very much.

PROFESSOR STEPHANIE PELL

As alluded to by Deputy Director Ledgett last night, one of the most divisive publicly debated issues in the tech space over the past couple years has been law enforcement's claim to be "going dark" in the current digital world due, in part, to various kinds of encryption technologies that are being enabled by default. Indeed, some of you who attended this summit last year may remember a spirited discussion between the FBI's Sherry Sabol and computer scientists Matt Blaze and Bruce Schneier.

The Crypto Wars debate is best framed as *competing visions of security* spawned by tensions inherent in seeking to realize two very important policy goals: one of enabling strong cybersecurity or information security practices, and another of facilitating law enforcement's traditional public safety mission. Unfortunately, this debate has not advanced much since we all gathered last year, at least in terms of proposed solutions or policies that do not undermine good cybersecurity practices while accommodating, at least to some extent, law enforcement challenges in an encryption era.

With the recent *Clash of the Titans*, that is, Apple versus FBI, whose bloody battle was only deferred due to the work of professional hackers hired by the FBI who apparently found a way to access the data stored on an iPhone 5C running iOS 9, and the recent discussion draft of a bill released by two Senators from the Intelligence Committee that some in the tech community have called "effectively the most anti-crypto bill of all anti-crypto bills," it is fair to say that stakeholders on each side of the Crypto Wars are not finding solid, common ground for these goals to be reconciled.

Something has got to give. At a minimum, we have to discuss what avenues are actually available to law enforcement that do not undermine fundamental cybersecurity principles and practices, but that recognize some of law enforcement's challenges.

How does the Internet of Things (IoT) play into this discussion? Well, for better or worse, the ever-expanding IoT connected world provides new surveillance platforms and apertures for, among other things, the collection of communications content. In a House Energy and Commerce hearing on the encryption issue held just two days ago, Federal and State law enforcement witnesses acknowledged the general point that the Internet of Things provides burgeoning new trails of metadata that can, for example, help law enforcement more readily identify a target's associates as well as his comings and goings, among other things. But these government witnesses also made the point that metadata is not a substitute for everything. Sometimes, communications content is necessary. Sometimes, you need to know what suspects say to each other to prove intent and knowledge elements of crimes. I think it's a fair point.

Metadata, as useful as it is, cannot provide the solution to everything. Sometimes, communication content is needed—although and I say this as a former Federal prose-

CYBER GRAND CHALLENGE PANEL

cutor: law enforcement has never enjoyed comprehensive and unfailingly dependable access to what suspects or co-conspirators say to each other at any given time.

But, I respectfully submit that the IoT can serve as a mitigating factor to some, if not all, of the challenges law enforcement faces with respect to communications content. What do I mean by that? Well, most of us are aware, or should be aware, that the camera on our laptop sitting uncovered in the bedroom can become a window to our most private, intimate actions and conversations for law enforcement with a Wiretap order and for criminal hackers without one.

IoT devices provide all kinds of apertures for surveillance, from nanny cams, and now I understand Nest devices, which I have to admit we own, to smart TVs. In February of 2015, Shane Harris published a story about Samsung's smart television listening to conversations through an onboard microphone and relaying them back to Samsung to discern whether owners were attempting to give instructions to their smart TVs. Samsung's privacy policy informed users to be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third-party through the use of voice recognition.

Now there is some legal support for law enforcement's ability to compel third parties, with an appropriate court order, to use microphones and sensors embedded in their products to assist law enforcement with wiretapping. I'm not talking about the All Writs Act, whose general language was asserted against Apple by the FBI. I'm talking about a thirteen year-old case called The Company Case from the Ninth Circuit Court of Appeals. In this case, the FBI sought through its wiretapping authority to compel The Company to use its onboard driver assistance technology to record conversations going on inside the car. The government lost the case, but probably not for the reason that you might think. The problem the government ran into was that if the company opened this onboard cellular feature, which was a function of its vehicle recovery mode to help the consumer and authorities find the car if it was stolen—if it opened that function in order to help the FBI to listen to conversation in its current investigation, then the remaining emergency functions would not work. In other words, the listening feature could not be activated secretly in the recovery mode without disrupting delivery of all other onboard emergency features provided by the company. The court found that this technical predicament, if you will, violated the "minimum of interference" language of the Wiretap Act.

Specifically, the court found that while the "minimum of interference" requirement allows for some level of interference with customer service in the conducting of surveillance, such eavesdropping is not performed with a minimum of interference if a service is completely shut down as a result of the surveillance. By inference then, if the eavesdropping could have been accomplished without shutting down emergency features, it is fair to argue that the government would have prevailed. And, I think we may see the government making this argument in future cases.

Now I don't have to tell a room full of technologists and technically minded people that the IoT, as other panelists have mentioned, is a platform for hacking by good guys and bad guys. In the government's case it is a way into networks and devices that could allow it to access data either before its encrypted or after it's decrypted. In this case, the government may or may not need to seek the assistance of a third party company. So, the IoT as a surveillance platform may be one way to mitigate a government's "going dark" problems that does not involve introducing new vulnerabilities or backdoors into our networks. But even all of us law-abiding citizens here today should have a healthy degree of discomfort with the idea that our IoT devices, including the ones in our homes, can be used against us. Some yet uncreated avatar of the popular child's toy 'Elf on the Shelf,' or its Jewish equivalent, 'Mensch on a Bench,' may ultimately become a *Snoop on the Stoop.* Thank you.

AM: Okay. Thank you very much to the panelists for such insightful commentary. So, as moderator, I will take the prerogative of throwing out the first few questions.

One of the interesting points raised about Nest is this dynamic of machine learning and human learning. Which do we have more hope for? That we can build machines ultimately to accommodate the realities of human needs, or that we're just going to train humans to work with the machines that we can build. How do we build this next generation of devices in a way that recognizes that challenge of remoteness, and what other examples are there of these dynamics?

MB: That is an interesting question. This is one that comes into play in my field of work all the time in that you often have a remote operator taking an action in, maybe, a substation that's 500 miles away, and does not really have good situational awareness of what is actually happening on the ground. It brings up the point of there's going to be a lot of unintended consequences from connecting all of these systems that we now come to rely on every day. And the other question I get all the time is: What's going to save us? Training people or making better machines? And, the answer is unfortunately, it depends. It's going to be some combination of both. There are things that machines do very well and we should build machines that do that. But when it comes to certain levels of pattern recognition, and other things along those lines, there's no better machine than the one up here. Personal opinion, I'll take human analysts every day and twice on Sunday over a little box. But that little box makes those human analysts better at their jobs.

SM: With respect to the labor there is no labor. There is no human capability. Right now, (ISC)2, which is a workgroup of operators, analysts and their management estimates that by 2019 there will be 1.6 million fewer information practitioners and security practitioners and private practitioners that are required to carry out the existing slate of tasks, which does not include IoT. This notion that we're simply going to train up, it's preposterous. The machine learning and automation is what's going to drive us towards results, because there simply will not be enough hands-on keyboards or enough brains in front of monitors.

AM: So here's my second question. We talked about all these purpose-built devices. To what extent is adequate prior testing currently occurring in the market, and how does this present formidable challenges for both the public and private sector supply chain?

SM: Prior? Many manufacturers have what they call customer test, which is they ship it, and then they get live results, and then figure out what's broken. No, I don't think there's any adequate standard. I will say one thing, with respect to IoT, it's a little bit different than IT. There are two organizations when we discuss supply chain and standards that I urge people who are building devices to participate with. One is the Industrial Internet Consortium and the other is the Open Interconnect Consortium. The first is focused on building better devices so that people will not harm themselves and their architecture. The second organization is designed to create API's, so devices can talk to each other with greater reliability.

MB: One thing that is definitely lacking is negative testing. Many of these Internet of Things devices are built on commodity platforms and commodity components, because they're a lot cheaper to source, and easier to integrate. It is easier to buy a chip from Intel than to build your own. What you see is that these products will have a lot of capabilities that, maybe, are things that you didn't actually need, but they are available. And if you do not conduct negative testing to verify that those devices are turned off, an adversary may use that capability against you.

Q: COLONEL VEGA: When we met with venture capitalists in Silicon Valley, they made a statement that their challenge is being the first to market. "If I'm not the first to market then there's no need to secure anything, because I have nothing to secure." So, how do we incentivize those who are producing a product to secure something?

SP: Well, one thing that's happening is that venture capitalists are starting to shift their own priorities and which companies they fund. Some funds are looking for high-quality innovation that is less focused on maximizing the speed of profit, and more focused on building a more integrity-possessing product. There are resources that are available for IoT creators, and they're operating on a shoestring budget. The FTC put out a useful security guide that every company and organization should be aware of. And ISO recently released standards that create the bare minimum of creating information intake processes and vulnerability handling to improve security. So those are things that are nudging us forward, but with the deficit of enforcement, we have a long way to go.

Q: DR. BRANTLY: I wanted to continue on Colonel Vega's topic. If our IoT device starts broacasting that we're no longer in the house and turns off our air conditioning, does the hacker in the street who's watching our Wi-Fi network say "Oh, nobody's home, let's go rob that one." Or on the flip side, in a combat sense, we have devices broadcasting our location and sending out pictures while we're in the field, and results in reverse artillery targeting. How do we deal with this as we start positioning ourselves in this particular marketplace both from a criminal standpoint, from an industry standpoint, and from a protection standpoint to both develop and incentivize, as well as create systems that mitigate a lot of the risk?

SM: I will tell you, and it's everybody's favorite whipping boy, but I think the Target Corporation hack changed the paradigm of the board of directors room forever. It went far beyond retail. I don't necessarily agree that people are

CYBER GRAND CHALLENGE PANEL

simply going to get an FTC guide and start building better products, they're going to do it because they have financial incentive to do so, or tremendous financial disincentive to not do so. I think organizations where there's brand equity in particular are looking to do things better because of the perception, or negative perception, when they get caught not doing it correctly. I do think Target created some awareness in different kinds of organizations. I've consulted with five energy delivery companies at the board level this year, and it's because they do not want to be on the front page of the paper. I think there's tremendous incentive. There are probably 25 or 30 different kinds of standards that you could observe. Which one's the right one? If there was going to be government push, it would be on identifying requirements, not necessarily standards. What constitutes the best way to go about giving companies incentive to do it that way? I don't necessarily see the companies just saying, "Okay. There's no brand impact by building a $3 chip enabled device here, why should I spend $3.25?" I don't see that happening. It's only when it's brand impacting.

AM: Do we have any more questions?

Q: We're finding intentionally embedded malware by Chinese manufacturers in their electronics and their computer chips. So two questions: what are we doing to protect our electronics supply chain? And second question, is the consumer accepting the risk upon purchasing these devices? Must we transfer that risk to the manufacturer or the vendor to hold them accountable for inferior parts?

SM: Man, those are two really good questions.

AM: You take the first one, I'll take the second one.

SM: Let me tackle the second part first, because the first part's really hard. With respect to consumers, a hammer has basically two uses: one to hammer nails in and the other to pull nails out. Is the hammer manufacturer responsible when you use the claw end to go after your kid's soccer coach, because you didn't like how much time he played? The answer is, no. In the same way, are consumers' liable for manufacturing defects? Probably not. But are they liable for how poorly they treat their own privacy in particular, I don't know if you can hold the manufacturer accountable for that. How many folks have an iPhone? Like half. Anybody ever read the iTunes agreement? You're nodding, you didn't read it. It's like 28 pages. If I rolled it up and hit you over the head with it, you would suffer a serious injury.

I would say that we treat our own privacy in a very cavalier fashion until it's been violated. I don't know that you can hold the manufacturers accountable for that part. But can organizations like the FTC hold manufacturers accountable for knowingly or pushing ill-tested code or products out to mass consumption by consumers? I think the answer is, yes. With respect to supply chain, that's tricky. Certainly, there are trusted foundries that organizations like the intelligence community utilize, but I wouldn't call them cost effective. You're knowingly buying chips and components that were assembled by variety of different folks from a variety of locations, I don't want to blame China, I think it's all over the place, and some of the problems are inadvertent rather than malicious. But, if there's no testing standard, if there's no standards or certifications for those manufacturers, I don't know how you can hold them accountable. Again, I would look for manufacturers that participate in the Industrial Internet Consortium where there are best practices and guidelines, partnering with organizations that publish API's through the Open Interconnect Consortium, where there are standards, testing, and guidelines.

AM: My analysis is a little more legalistic and slightly different. Organizations are just starting to fund and create labs where third party objective researches are breaking things to try to figure out what's actually going on in products as shipped. And, that is going to be a game changer when that information gets fed back into the consumer ecosystem. Much the same way that, say, a Consumer Reports rates cars.

On the liability point, there will be liability. There's no way there can't be liability. Right now we're in this weirdly legal limbo, but once you start taking that code and the blue screen of death gets embedded in insulin pumps, in heart monitors, in cars, these devices can kill people. We will see cases, and at that point courts will need to reconcile this aggressive product liability standard with the very permissive software liability standard. Particularly where basic levels of care have not been exercised as embedding and auditing code before it was pushed out to consumers; courts will not have a problem finding the liabilities appropriate especially where physical injury happens as a consequence.

AM: We need that be the final word. Please join me in thanking my amazing co-panelists.

INDUSTRY INITIATIVES PANEL

LEFT TO RIGHT: MODERATOR DR. FERNANDO MAYMI WITH PANELISTS MR. RICK HOWARD, MR. ALEX STAMOS, MR. JIM ROUTH, MR. MARCUS SACHS

Today's moderator is Dr. Fernando Maymí. He's the Deputy Director of the Army Cyber Institute at West Point. In that capacity, he is part of a multi-disciplinary team charged with developing intellectual capital and impactful partnerships that enabled the nation to outmaneuver adversaries in cyberspace. He is also an Assistant Professor of Computer Science in the Department of Electrical Engineer and Computer Science at the U.S. Military Academy where he has taught for the last 12 years, and it's also where he earned his Bachelor's in computer science. He also holds a Master's degree from the Naval Post Graduate School and a Ph.D. from University of Puerto Rico. With that, Dr. Maymí.

DR. FERNANDO MAYMÍ

Thank you. I have two unenviable tasks. The first one is I get to moderate the panel that stands between you and lunch. Not a good place to stand. The second one, and perhaps a more onerous one, is that I'm going to try my best to herd this group that promises to be lively, informative, and entertaining to the audience. So, please cross your fingers for us.

Seriously, we are going to talk about information sharing, and we are fortunate to have on our panel some real luminaries when it comes to sharing information, specifically with security. We have Rick Howard, CSO for Palo Alto Networks, Jim Routh, CSO for Aetna, Marcus Sachs, CSO for the NERC, the North American Electric Reliability Corporation. And last, but not least, Alex Stamos, CSO for Facebook.

First, I want to set the stage real quick. We're going to take a rather liberal definition of IoT. And by IoT, we're going to talk about connected devices, nontraditional computing devices. We are not worried about servers and workstations. We are certainly worried about the things that we normally don't think of as IoT, meaning Fitbits and drones. But also more robust networks like ICS and SCADA. We are going to run the gamut and take a rather liberal perspective on it.

To my second point. Let's start with a soft one, not that you guys need one. Rick, what have you seen, what have you learned in the last couple of years that really should inform how we move forward in terms of information sharing across the entire community?

MR. RICK HOWARD

Thanks Fernando. I just want to give a public announcement for the Army Cyber Institute Cyber Talks. Two talks ago, I had the great privilege to listen to a young Captain Roy Ragsdale give an inspiring presentation regarding the fundamental principles for network defenders. It was very inspiring, and then last summer, I read Elon Musk's biography. He doesn't go after little problems; he goes

INDUSTRY INITIATIVES PANEL

after big, gigantic, hairy problems. When Elon tries to solve those problems, he doesn't try to look at what everybody else does and try to use those solutions, he invents them from scratch, from the ground up. It got me thinking, what are the network defenders' first priorities? If you take everything we do in terms of people, process, and technology, what is it we are trying to do? What is it you are trying to do in your organization?

Here is what I think. We should be preventing material impact to our organizations. Trying to make sure the company doesn't take a big hit. For government organizations, you're trying to make sure you stay functional and do your mission. I think going forward with the information sharing, we are all trying to do is prevent material impact to our organizations.

Information sharing, we're deep believers in this. I think we're a bit of a leader in this, so Facebook operates a service called ThreatExchange, which is a machine-to-machine real time threat sharing platform. We operate it for free for anybody from any industry, and will do so forever. I believe in threat sharing. It's based upon building human relationships, and then trying to come up with systems that build on top of it. At my previous job, we had malware from a nation-state adversary of the United States. That malware was attacking another tech firm that was, obviously, being part of this campaign. Their automated systems had pulled it down, identified it as malware, and automatically uploaded all the IOCs to ThreatExchange. We automatically pulled those down and checked every single NetFlow. One of our admins opened up this Word document, and it called home to one of the IP addresses. We caught it instantly, and automatically turned the port off on her computer, and filed a ticket for somebody to go grab it and do forensics. That could have been a massive multi-week response to a major intrusion that was stopped because we were able to rely upon our partners of the same category of companies that were also being affected. We're very proud of what we're doing and love to chat with people if they want to get on ThreatExchange.

MR. JIM ROUTH

I'm fortunate to be a member of the FS-ISAC, there are 7,500 members, and about 40 percent of them are global. I'm involved with the National Health ISAC, and automatically share IOC information across that network of members through standard STIX and TAXII that's used for the platform. There is a tight group, Circle of Trust we call it, where there are five other companies that I can query any time. We can exchange IOCs that way. The automation that's enabling information sharing today has never been at a higher level. But one of the fundamental things that I've learned is that automation is absolutely wonderful, we welcome it, but most of the actionable data that I receive, which actually prevents breaches comes from the relationships established through forums just like this. I have solid relationships with my fellow panelists that go back over three or four companies, and I still have the same relationship with them. Alex, in your case it might be six or seven companies. We all have a problem holding a steady job for a long period of time.

MR. MARCUS SACHS

In fact, we probably ought to talk about the life cycle of the CSO, because for many of us, particularly the cadets out here, who are thinking about what's life after uniform? It's very short. However, we do have continuous employment, which is always a good thing.

Quick lesson learned about information sharing. I run the Electricity ISAC. It used to be part of the Comm ISAC. I was Vice Chair of that back then in a previous life as we move through these jobs. When we started NERC, the parent organization, was all about voluntary sharing. This was in a world before the 2003 power blackout. The engineers at the power companies were very accustomed to sharing. Post blackout, Congress passed the Energy Policy Act of 2005, and it set forth this thing called the Electric Reliability Organization or ERO, which was then charged with, ultimately, NERC got that mission with creating the CIP Standards. These standards are enforceable. Our organization enforces them. We do compliance, and can fine organizations that fall out of compliance. There is mandatory reporting, no different than in banking; you have to report.

What had happened with the ISAC once this mandatory reporting came in, the amount of voluntary sharing took a nosedive. Because who wants to tell your regulator what's going on for fear that somebody might come in and enforce some violation. Last year, we undertook a separation with ISAC voluntary sharing separated from the rest of NERC that does compliance reporting. We literally built a wall; physically separated the organization's badges from one side of NERC, which will not allow them to get into the ISAC. We separated the electronic systems, codes of conduct. The level of voluntary sharing has gone back up, like it should. The lesson from all this is that information sharing works best amongst those who can do something about it.

I think that we have to get past that. We have to understand to let groups share amongst those who can do something about it. And don't try and insert yourself into that group just for the purposes of monitoring their pain. There are certain groups who can't do anything about it, but they just want to see what's going on, for various reasons. We have to build these private collaboration rooms to let organizations share, and we have to protect that information from eyes that probably don't have any business looking at it.

FM: I'm hearing you say that the power grid is secure.

MS: I think it is. The lights are all on.

RH: I'm hearing you say that the power grid is secure. I would be remiss if I didn't talk about the Cyber Threat Alliance. The one vertical that's been linked to this information sharing game for security vendors. Because we do not want to give you intelligence, we want to sell you intelligence, this is a revenue stream for us, but we've got a group of eight security vendors who decided that's the wrong way to think about the problem. We should not be competing on intelligence; we all have the same intelligence, more or less. We really need to be competing on is product. Use the same intelligence to make our products better – that's what the Cyber Threat Alliance is all about. It's Symantec, and Intel, and Palo Alto Networks, and Fortinet are the core members. But here's the thing, when some vendor comes to you and says we want to sell their products, hear their pitch, and then ask, why aren't you a member of the Cyber Threat Alliance? And watch him stumble through that answer. And then point him my way, and we'll bring him in and help the whole world get safe.

FM: Back to you Marc, the power sector. We all worry about it. What are your thoughts on what's missing and what's the way forward, so that we can all jump on this same bandwagon?

MS: I think what everybody needs to understand, the power industry, and Mark Bristow started talking about this on the previous panel, and there is a physical component to electricity that's often just overlooked. The public likes to think of the grid as a big battery. Something you just turn on, turn off. There's actually a lot of inertial energy that's going on with spinning generators creating electricity. Even if I open a breaker, the spinning part continues, there still is electricity being created. It's got to go somewhere. We'll do load shedding, things like that. The point we all have to remember, the cyber is threat is just like a squirrel. In fact, the number one threat is squirrels in terms of actual loss of power. Now we do not have conferences on how to counter the squirrel threat, or have conferences on how to orient against lightening threat, or wind storms, or other types of perils which is exactly what we see in the power sector and have built resilience in to counter.

Cyber becomes just another one of these potential threats to our grid, mostly at the distribution level. And when we see it, we react to it. We actually have a good track record if you look at decades of running the grid, and we have computer controls, and we do not have any cases yet in the United States and Canada of a single loss of load to a customer due to a cyberattack. Now, there's been mistakes made by operators installing some bad software, but that's different from an external attack. We know what happened in Ukraine in December only affected three substations, and only for a short period of time. The time that it took for an engineer to actually go out and manually reset the breaker.

We have to be careful about the conversation; we are very aware of the cyber dimension, but it's not this gloom and doom with one mouse click away from the entire grid collapsing. There is a great deal of good cyber news out there.

FM: Thank you. I was hoping for doom and gloom and the additional Nightline for tonight. Jim, if we can have your thoughts on how are you looking at leveraging the opportunities of IoT while mitigating the threats?

JR: I appreciate that question, and I have given a lot of thought to this. In terms of what I've come up with in terms of a framework and a solution for the IoT problem, I came up with absolutely nothing. Absolutely zero. I just want to manage expectations here. I don't have a clue as to how to address this problem. But here's one thing I do know, you look back to what happened in the past, and try to predict maybe what's happening in the future. There are some things that might be beneficial. First, every single IoT component I've ever looked at has embedded software. Software is the key to any kind of IoT capability. The good news is we actually have learned a great deal about software security practices today; far better than 10 years ago. Much more mature in terms of the capabilities. There's hope on the horizon in terms of the tools and techniques that we can actually use to develop resilient software.

The next component is not widely known. And that is, when you embed security controls in the software development process, it costs less money. Let me say that again, it costs less money. There is this perception that when we add security controls into the development process that increases cost, and the benefit is the risk mitigation that you get from that. What is true is that it actually costs less money to put security controls into your software development process.

I'll give you some data points just to ponder. First, I run 3,500 developers in our software security program, enterprise-wide across a number of companies. Our defect density is one defect for 10,000 lines of code. One high-risk vulnerability for 10,000 lines of code across the entire enterprise. What that translates into is a $20 million a year cost-avoidance savings as a result of the productivity gain that goes into software development, which is 60 percent. Meaning, 60 percent of every dollar you spent on software development, you get a return in terms of higher productivity. Those numbers are pretty compelling. In order to implement that, you don't have to talk to anybody except your CFO or your CEO, and give them those numbers and tell them you have a potential solution. You never have to mention risk or resiliency; you just have to mention the opportunity to improve your productivity.

We can bake software security capability into the software manufacturing process, and it is a manufacturing process. It's very similar to a car manufacturing process; software security improves the manufacturing process, so it costs less to own and operate that software. The reason that's important is because IoT means everybody that manufactures software has to fundamentally up their game in terms of software resiliency to protect those users of those capabilities, and it's actually economically viable to do so. That's my story, I'm sticking with it. What do you think?

MR. ALEX STAMOS

I totally agree. Building software security into your development lifecycle is dead. There's no place to plug your security team into a development lifecycle other than when the developer's writing the code. There's really no other place. And this is a difficulty for us in that we have a couple more developers than you guys, like in the 4,000 or 5,000 range, and run a continuous integration, continuous deployment environment. You get on a test server, you test it on your local server, you submit it, your code is now started down a path, and it will end up in production automatically, possibly within hours.

To plug into that kind of environment, security testing is pretty much impossible. You have to have static analysis, you have look for areas of the code, which you know there have been security flaws in the past, and you can generate that information automatically. The flip side of this is you can fix your code very, very quickly. Knowing that you are going to make mistakes, instrumenting your system so that you will learn about the mistakes as quickly as possible, and then moving very quickly to fix them. I think it's absolutely the way you have to go. It turns out that you can have pretty crappy software that you can fix rapidly and quickly, and that you can mitigate, as long as you have appropriate instrumentation, and you can still avoid having any actual data breaches, or other impacts to operations.

FM: Speaking of the human adversary, what are your views, I mean, you own Unit 42, what are you seeing in terms of threat, particularly with regard to an increasingly connected world of devices?

RH: By the way, Unit 42 is Palo Alto Networks Threat Intelligence Team. The big change we've seen in the last couple of years are criminals have moved away or at least starting to move away from just basic credit card theft and going to a more painful version of attacks in the crypto space. Where a bad guy from Eastern Europe will come to grandma's computer, encrypt her hard drive and then immediately make a phone call to her and say, "If you want your pictures of your cats and grandchildren back, pay us $500 in bitcoins." They are calling in a different language a grandma and walking them through a bitcoin transaction at $500 a pop. How many people here have actually done a bitcoin transaction?

That's how flexible they are in their backend processes.

They're making it easier to take money out of the system. Just think about what that means in the future with the Internet of Things. They can potentially disable all of those things in your house that makes your life bearable, how much would you pay to get the air conditioning system turned on? "Yes, I'll pay you $500 just turn my air conditioning on, because I'm tired of being uncomfortable."

FM: We can't have a conversation about information sharing without bringing up, at least briefly, CISA, the Cybersecurity Information Sharing Act of 2015. I'm going to throw this over to the panel, please, anybody jump on it.

MS: Before we get on CISA, just real quick about IoT and data and threats. I did want to cover this before we get out of here. It's the data exhaust problem. Briefly, many of us have been looking at IoT and wondering, is it really about the devices and is it about hacking endpoints and taking control? But think about the data that the endpoints creates. When you go on Facebook, which is not IoT, you are voluntarily creating data about yourself; pictures you upload, identifying 'likes', text you type in, things like that. It's being accumulated in some database somewhere. If you're using a Nest device or anything in that sensing the world around you, that information is going somewhere. It's accumulating someplace. If you have an Android or an iPhone, it knows where you are. It's tracking you, and if you have a Google account anywhere, and it's turned on and you're logged in, Google is tracking you for Google Analytics. You're creating this exhaust essentially about yourself. What happens when the bad guys get access to the exhaust? Not just the device, but the information about you and your organization? This trail is no longer just little bit crumbs, but actual buckets of knowledge that you, individually, are accumulating year after year that is somewhere out there? That's almost like a Holy Grail for criminals. Not taking control of the IP connected microphone or the IP connected camera, but all that information about you. That's where I think we need to really begin to think about where is this all going to take us? Now, how does that tie to CISA?

CISA's about information sharing. It's trying to enable a better conversation between the Public and Private sector. I think that it's opened a lot of doors and removed some barriers. This is a long standing Washington problem of throwing barriers regarding information sharing. Congress has been struggling with how you take those barriers off the table to enhance information sharing. Legislation like CISA opens up interesting avenues; if I actually share with the Federal government, be it DoD, DOJ, D- O- fill in the blank, does it become the property of the Federal government to be shared equally amongst all? These are still some barriers we're going to have to work through in spite of CISA.

FM: One final question, because I want to open it up to the floor. The question du jour, if you had a minute with the President, or the next President, what would you say? We'll start with Rick.

RH: We've talked about education and bringing more potential employees into the computer security space. I think what Congress can do is pass a law or make an agency whose job is to bring to the national level these stovepipe organizations who are reaching out and finding young people to be new cybersecurity professionals. There's lots of capture the flag organizations for high schools and colleges. But none of them know about each other. There is no way for commercial outfits to plug into them. I would like someone to take charge of that and make it easy for commercial organizations like us to give them scholarships, let us track and bring them in as interns, and maybe, hire them as employees.

AS: My advice to Congress would be on encryption in security as it relates to law enforcement. I would love to see more strategic thinking on this issue. There is an Energy and Commerce hearing about encryption in law enforcement, and it was a little frustrating. I'm less frustrated about people misusing words. It's easy to be a techy and snarky about well-meaning people who are struggling with a complicated issue that they don't live every day. I'm more frustrated by the lack of strategic discussion in those situations. Law enforcement has a valid problem that they're dealing with, but they are very technical. Decisions are being made based upon one person's phone, in one terrorist attack. That is just one of the many adversaries the United States is going to face over the next several decades. My suggestion to Congress is when you think about encryption, security, and law enforcement, think about what the other players on the board are going to do. We are not the only players on the board, 86% of my users are not American. We have to operate in almost every jurisdiction on the planet. What are those people going to do in response to anything that happens in the US? In my opinion, the United States is the most trusted provider of information technology to the world and it is my opinion that it is in the absolute long-term strategic best interest to the United States to maintain that reputation.

INDUSTRY INITIATIVES PANEL

That is something we should not give away lightly. If we're going to give that away, it needs to be because all of the equities have been measured and weighed, and not just acted on short-term thinking.

JR: I would say to every single government official that will listen: reduce the attack surface. At the end of the day, I only care about one thing: avoiding getting fired, which means avoiding a major breach. To avoid that I have to shrink the attack surface, and that's basic risk management. The easiest way to shrink the entire attack surface in healthcare is to eliminate the social security number as the unique identifier. This is the dumbest thing in the world, does this make any sense at all?

I would say to the President, please stop using social security as a unique identifier. And for all of you, when you go to the doctor and they ask you to fill out that 13 page medical history form, and they ask you for your social security number? Do not put it in there. They will tell you that the insurance company needs it. That's not true. Do not ever give your social security number out when you go to the doctor. The doctor does an outstanding job at providing high quality healthcare services to you. They suck at protecting your information.

MS: Two items for the government, Congress, and President. First one is easy, please protect my information. This is like a Holy Grail. The second is vision. We lack a national strategy in our country, a visionary strategy that tells us where we want to be in a few years or few decades with cyberspace. Ten, twenty, thirty years from now we've got an effort that says we want to walk on Mars. That's really cool and set in motion. Ten, twenty, thirty years from now, what do we want cyberspace to be? Where is that vision? That is what we need from government is that strategic view of where do we want to go. It can start with Congressional funding at a place like West Point, or the other service academies. Post-Civil War, there was a big effort to expand the nation west. We lacked a transportation system and West Point was actively involved in training engineers and actually doing research with other civilian institutions on structural engineering. How about thinking about cyberspace in the same way? If we want to build this thing out, if it's going to be a national asset, why not invest in some of that basic research? Teaching engineers how to engineer cyberspace securely as well as safely. You can start that here and at the other service academies. This is about the military and national security. That is what I would ask Congress and the President. Be a visionary.

FM: Let me open it up for questions. So please, stump our panel.

QUESTIONS & ANSWERS

Q: Gentlemen, there's a question asked earlier if a US flagged ship left a US port and was boarded by China's Navy would it be the government's responsibility to intervene? When we had the North Korea hack, we created a new term cyber-vandalism. What is your sense of where industry is at in terms of the pain threshold, or the red line, so to speak, where they would start flirting with independently taking action?

RH: Well, that's not loaded at all. We're talking about organizations, for the most part, around the world who can't patch their laptops. What I think I hear you advocating for is giving them permission to do more, a lot more, than that. I would say No for most organizations. They don't have the capacity to do that. Stick to defense for most commercial organizations. That said, there is counter-intelligence stuff that could be done. Putting fake networks out, moving bad guys into those fake networks, watching what they're doing. All that stuff is on the table, but if it starts to get it moving into the offensive side, that's a recipe for disaster.

MS: On the law enforcement side, this is an interesting question because in the physical world if somebody steals something there is this kind of concept of taking it back. Should that apply in cyberspace for crime, not nation-state military action, but for crime? Should there be some kind of equivalence in the law that allows a business to employ a badged private sector organization that could recover the goods, much like a repossession company can go after a car, as an example?

JR: I have two thoughts. The first is every time I've seen offensive capability being used there's always a retaliation. I've never seen an example where there hasn't been. So that is something to factor in. Most of us have a lot more to lose than we have to gain through an offensive capability and that's our primary perspective.

Second, there is no clear line in terms of where the government's going to step in, or not in a particular given situation. We saw a situation with 225 attacks on 42 targeted banks occurring over about an 18-month period, and the reality is the government was very clear in telling us, "You're on your own." And what it did is it actually baked in a higher level of resiliency. The reality is we weathered the storm pretty well on our own. And that was probably the right call in terms of judgement. But I don't think it's clear in every given situation, and frankly, I think we're establishing some protocols to help make that more clear.

QUESTIONS & ANSWERS

Q: You can see ransomware on the rise over the last couple of years and it's been associated with virtual currencies. Is this proliferation of ransomware a cost benefit choice that companies are making? What do you see as directions or positive directions related to this problem going forward?

JR: Yes, I've got two thoughts that are somewhat preventative. All of us in major enterprises today have spent the last 15 years automating and making entirely efficient our data replication process for business recovery purposes. And it's nice to see that a security vulnerability in this case, an exploit, can turn all of that obsolete. What we've done is establish something called Clean Copy; we are going back old school, and actually taking time to capture our most critical data, separating it from our network, storing it, and we do that every week. That is purely in the case of where we get ransomware or destructive malware on our systems that percolates through our entire environment. This gives us a way of recovery. It's not elegant, it's not highly automated, but it is something that we did right after the Sony breach, simply thinking this is going to spread. And ransomware is spreading. So those are two things.

MS: Ransomware is a peril like a flood. We prepare for floods and we prepare for fires. You have data storage away from your data center for that reason. Think of ransomware along those same lines. Now there is a computer science part of it that others can work on in terms of solving the computer science, but as business owners, it should be treated as any other peril. You should have backups and data recovery and procedures in place just like you would if it was a natural event.

AS: I was thinking about wearing a hoodie and jeans just to play it up, but I guess I should have. The suit, you saw right through me. On the bitcoin stuff, on cryptocurrencies, certainly they are here to stay. A funny fact, bitcoin has now been more stable than the price of gold for the last 30 days. It is now a more stable place to put your money than to buy gold. As long as there are major countries like China with currency controls, there'll always be enough legitimate transactions to provide cover. Now the flip side is bitcoin is an open ledger system. Every transaction that happens at bitcoin is viewable to everybody in the bitcoin network. I think a lot of people don't understand this. It is not clear whether bitcoins, or the cryptocurrencies, will be as good for these kinds of purposes going forward, because they are much less anonymous in many ways than other kinds of transactions.

CSM (R) RODNEY HARRIS WITH USMA COMMAND SERGEANT MAJOR DAVID CLARK

MR. DON CALLAHAN WITH GEN (R) KEITH ALEXANDER

KEYNOTE PRESENTATION

INTRODUCTION BY DR. PHYLLIS SCHNECK

Good Afternoon. Thank you for being here and thank you for having us. It's a pleasure and honor to be here at West Point and introduce our Secretary of Homeland Security, Mr. Jeh Johnson. I'm going to give a little introduction from my own perspective. I have been working with Secretary Johnson for the past two and half years after I left the private sector to work in the Department of Homeland Security. Secretary Johnson has always told us that cybersecurity is a part of Homeland Security. In my experience, Secretary Johnson has taken the time to learn cybersecurity, to ask all the right questions, to ask the really hard questions of the cyber teams, to drive us to what he calls the unity of effort throughout the Department because we have cybersecurity all over the Department of Homeland Security: Coast Guard, Secret Service, ICE, policy, FEMA, and to the operations center that I run. He has always driven us to excellence.

In 2012, I spoke at a conference similar to JSA with many in this room attending, and I said what if we could bring all the cybersecurity information together at a speed of light. With our agency, partners, FBI, NSA, and under Secretary Johnson's leadership, we did that with the establishment of the National Cybersecurity and Communications Integration Center. Without Secretary Johnson digging in, pushing us, and driving us hard, and learning cybersecurity himself, we would not have been able to issue the binding directives that have literally cleaned up vulnerabilities across the US government. It's been a great honor for me to get to work with Secretary Johnson and with that I welcome him. Thank you!

SECRETARY JEH JOHNSON

Thank you Phyllis! Good afternoon everyone here. It is great for me to be back at West Point. Some of you may know that I served as the General Counsel of the Department of Defense from 2009-2012. I see many of my former clients here. I won't tell you which ones gave me more headaches than the others. I'm also a product of this part of the world. I grew up in the Hudson Valley in a town called Wappingers Falls. I'm a graduate of Roy C. Ketchum High School in Wappingers Falls, New York, in 1975. It's great to be back on this beautiful spot on the Hudson watching an Amtrak train heading North right now across the river. I'm very familiar with this area. Indeed, when I was GC of the Department of Defense, I looked for opportunities to drive up here, because, when I drove up here from Washington, I would always stop at one of my favorite places in the Hudson Valley, which is the top of Bear Mountain, about 5 miles south of here. Those of you who have not been at the top of Bear Mountain, it is one of the most beautiful panoramic places in the Hudson Valley with a view of the City, view of the Bear Mountain Bridge, and a view of the River.

I want to say a few words about the Department of Homeland Security, and what we are doing currently on a number of fronts, and then I will turn to cybersecurity, which is one of our top priorities. As some of you may know, DHS has 22 components; we are the third largest Department of the U.S. Government with approximately 240,000 people and a number of missions: antiterrorism, aviation security, cybersecurity, border security, maritime security, the administration and enforcement of our immigration laws, which is the entire days lecture onto itself, the protection of our national leaders, the detection of chemical biological nuclear threats to the Homeland; response to natural disasters, hurricanes, floods, and tornadoes. As you heard from Dr. Schneck, we are engaged right now in a unity of effort initiative to bring about a more effective and efficient way in which we deliver Homeland Security to the American public, more centralized, more strategic decision making at the Department of Homeland Security headquarters when it comes to budget, acquisition, and HR practices. This is something I announced two years ago; to run an aggressive campaign to revise our acquisition system, HR system, to make processes shorter and more effective. I have built joint task forces modelled after the command structure for border security on the southwest border that brings to bear all the resources of DHS.

We are engaged in an aggressive campaign to raise the level of employee's satisfaction across every level of Homeland Security. I have personally worked alongside numerous members of our workforce in various tasks, and last month I actually put on a TSA uniform and went to BWI and worked alongside our TSO's for about an hour; literally, no one recognized me. No one put the face on the video together with the face in uniform passing the bins, saying have a nice flight! Finally, after about an hour of this, I approached an elderly couple who were on their way to their grandson's wedding in North Carolina, and they had just gone through security. I said to them, hi, I'm Jeh Johnson, do you know who I am? And the husband said, yes, you are Jeh Johnson, you just told me. I added that

I'm the guy who runs Homeland Security. You've ever heard of the show Undercover Boss? They got very excited and wanted to introduce me to their daughter who was down at the gate so there is a great picture of me that went viral (the wife is in a wheelchair) on Twitter—150,000 people saw this including a lot of TSO's who thanked me for working alongside them.

Counter-terrorism remains the cornerstone of our mission. The events of the last several months reinforce this; the attack on our Homeland at San Bernardino, before that Chattanooga, and of course terrorist attacks around the world, in Paris, Belgium and other places. We are doing a number of things on the counter-terrorism front. As many of you know, our military continues to take the fight to the Islamic State, AQ, and the AQ elements of Al-Shabaab. We are doing an excellent job degrading their leadership, and their external capability through partnerships taking back large pieces of territory ISIS once occupied in Iraq and Syria. Our Federal Law Enforcement does in my judgement an excellent job of detecting, investigating, interdicting, and prosecuting terrorist plots here in the Homeland. In this new phase of global terrorist threats, which includes not only terrorist directed attacks, but also terrorists inspired attacks and terrorist enabled attacks. We've had to bring about a whole of government response in the effort. We have enhanced security around Federal buildings across the country.

We are doing a number of things to enhance aviation security on flights and airports here in the United States and at airports overseas. I'm sure a number of you have noticed longer wait times at US airports due in significant part to increased air travel. Twelve months ago, TSA came in contact with about 1.6 million people a day. That number is now up to 2.3 million a day, and we expect it to climb higher during the summer. It's due to increased air travel, but is frankly also due to our efforts to enhance and improve aviation security. We are developing now an aggressive plan to address the longer wait times. My advice to everybody in this room is to sign up for TSA pre-check. It's a great program, and last year we enrolled 1.5 million people, and that number is growing. Please sign up for TSA pre-check and global entry.

We are working more with state and local law enforcement in counter-terrorism efforts. We are on the ground supporting things like active shooter training exercises in large cities like New York, Miami, and even in smaller cities where I attended an active shooter training exercise in Louisville, Kentucky. We are making much more effective use of joint task forces, and fusion centers.

We believe the public has a role in our Homeland Security vigilance and awareness. The "If you see something say something" campaign is more than just a slogan with DHS entering into partnerships with organizations like the NFL, Major League Baseball, and NASCAR to highlight that public awareness and vigilance do make a difference. I announced in December a provision to our National Terrorism Advisory System, which replaced the color-coded system. In this environment of a potential lone wolf attacks, I announced the creation of a Bulletin, which describes current developments or general trends regarding threats of terrorism.

A major centerpiece of our Homeland Security efforts is referred to inside the beltways as CVE, Countering Violent Extremism. We are partnering with communities in helping them counter the Islamic State's social media messaging. I personally met with American Muslim communities in Boston, Minneapolis, Washington, New York, Dearborn, Chicago, Houston, and in California. It is vital that we build bridges to American Muslim communities to encourage them to help each other dissuade somebody headed toward violence. I tell audiences all the time that it's crucial for Homeland Security to maintain a balance in a free and democratic society between basic physical security, and preserve what the American

KEYNOTE PRESENTATION

public cherishes and expects: freedom to travel, freedom to associate, free speech, and freedom of religion–basic civil liberties. Homeland Security always involves striking a balance. Those of us in Homeland Security are guardians of our freedoms as much as our security. As General Alexander and others know, cybersecurity involves striking a balance, between basic cybersecurity and the public's need to connect with the outside world.

You have heard from Dr. Phyllis Schneck who is our Deputy Under Secretary for Cybersecurity and Communications, also here is Dr. Andy Ozment, our Assistant Secretary for Cybersecurity and Communications. We live in an increasingly connected world. There now more devices that can access the Internet on this planet than there are people. And that in five years the number of such devices will be something like 50 billion. At the same time the range of motives and intent and frankly the capability of these bad actors is improving and increasing all the time. Therefore, it is a top priority for me and our President to make tangible improvements inside DHS through the President's Cybersecurity National Action Plan. We are making aggressive strides that we will leave cybersecurity a year from now better than I found it two years ago.

Let me make four points to this audience. First, a piece of good news; we are getting bipartisan support from Congress in our DHS cybersecurity efforts. In late 2014, Congress passed new laws to strengthen the DHS cybersecurity mission with the National Cyber Security Communications Integration Center which Andy runs. This center is one of the critical lines of America's cyber defense. These men and women work around the clock, 24/7, monitoring threats, issuing warnings, sharing information with the private sector, and keeping Americans safe. In 2015, Congress enacted, and the President signed The Cybersecurity Act of 2015. This major piece of legislation establishes DHS as the primary 'portal' for the private sector to share cyber threat information. On March 17, I certified pursuant to schedule that the information sharing is available and open for business; that same day I made a conference call to the Information Sharing and Analysis Center to tell them that our new automated real timing information sharing is up and running. Our goal this year was simply to sign up fifty companies. It looks as though we're on track to far exceed that goal.

Point 2. We are making tangible improvements in securing Federal networks. We are not where we need to be right now, but we are making great strides to get there. Last year, I issued for the first time a Binding Operational Directive (BOD), which requires all federal agencies to patch critical network vulnerabilities within 30 days. Federal departments and agencies responded to that directive aggressively. We identified 363 credible vulnerabilities and 100 were fixed in a very short period of time.

We have accelerated the deployment of EINSTEIN 3A. I gave my folks a deadline of end of last year to make E3A available to every Federal department and agency and we met that goal. E3A has the ability not just monitor and detect intrusions, but to block them as well. E3A has blocked something like one million unwanted intrusions into our Federal System. With E3A, DHS will not only be able to detect malicious traffic targeting federal government networks, but also prevent malicious traffic from harming those networks. This is accomplished through delivering intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating agency networks.

As part of the President's National Cybersecurity Action Plan, we are conducting vulnerability assessments of high value assets; we are in the midst of that project right now in our 2017 budget proposal. We are asking from Congress the ability to triple our Cyber Protection Teams. Some of you may know that DHS along with the Department of Energy and the FBI recently went the Ukraine because of a power failure that affected 200,000 people. We determined the power failure was the result of a cyber-attack, and are now in the midst of educating both US and international critical infrastructure stakeholders about lessons learned.

Point 3. The single most effective thing we can do for cybersecurity is the basic education of the people who use our systems. Basic education about the dangers and vulnerabilities of using our systems. Education, training, and raising awareness goes a long way to solving vulnerabilities. At DHS we are making aggressive efforts to educate our workforce. As many of you know, some of the most devastating sophisticated cyberattacks occur because somebody opened an email they shouldn't have opened. So at DHS, we have emails sent out advertising free Redskins tickets, click here. People click, thinking they won Redskins tickets, and are told to report to a certain room on a Monday morning where instead of receiving free Redskins ticket, they get a cybersecurity alert shirt. It's very effective. Adversaries know human behavior; human naiveté is a critical vulnerability, and so raising awareness through training for people who use our systems can go a long way.

THE SINGLE MOST EFFECTIVE THING WE CAN DO FOR CYBERSECURITY IS THE BASIC EDUCATION OF THE PEOPLE WHO USE OUR SYSTEMS.

Point 4. Everyone in this room recognizes the need for cyber talent in the new generation coming through schools right now. In the federal government we are on a hunt for cyber talent. Through our national collegiate cyber defense challenge which we fund, DHS is seeking people who are interested in serving their country. We have scholarships for people interested in cybersecurity, and the Secretary's Honors Program for cyber student volunteers. We are looking for ways to more aggressively look, identify, and recruit cyber talent.

In conclusion, there is no one single magic bullet for cybersecurity as we all know. My goals in office are to complete the expansion of the E3A, increase companies awareness, and increase companies participation with the DHS. Increasing awareness across our country, and encouraging cyber talent to come and serve our great nation even for just a few years. This must be a shared effort for all of us in government and the private sector. Cybersecurity involves both you and me; those of us in the private sector as well as those of us in government. In my judgement, we are making great progress and are on the right path. Congratulations to all of you who are here for this conference, and let's continue to work together.

Thank you all very much!

THE ROLE OF GOVERNMENT IN CYBERSECURITY

LEFT TO RIGHT: COL J. CARLOS VEGA INTRODUCING MODERATOR, MR. RYAN GILLIS AND PANELISTS GEN (R) KEITH ALEXANDER, DR. ANDY OZMENT, MR. PHIL CELESTINI

MODERATOR ◆ MR. RYAN GILLIS

Vice President of Cybersecurity Strategy and Global Policy for Palo Alto Networks where he is responsible for developing corporate policy, serves as the company's primary interface for global public policy and legislative matters, and leads company participation in various industry associations. In this role, Ryan serves as liaison with government agencies and companies around the world to assist in the development of strategies and operational partnerships to prevent against cybersecurity threats.

GENERAL (RET) KEITH ALEXANDER

Founder and CEO of IronNet Cybersecurity, and was Director of National Security Agency and Commander, U.S. Cyber Command. General Alexander was also just recently named to the President's Commission on Enhancing National Cybersecurity.

DR. ANDY OZMENT

Assistant Secretary for Cybersecurity and Communications of Homeland Security. I have known and worked with Andy for a long time as a Ph.D., cyber operator, worked in the private sector, NSA, and now Department of Homeland Security.

MR. PHIL CELESTINI

FBI Special Agent and right now he is serving in their Cyber Division at Fort Meade.

RG: With that, we turn to the subject of the panel today which is "The Role of Government in Cybersecurity". Let's hear from each one of the panelists where your vision is for "The Role of Government in Cybersecurity?

KA: From my background, the most important thing the government must do is to defend the nation in cyberspace. This is a key role for Department of Justice, specifically the FBI, Law Enforcement, DoD and DHS. You take the recent legislation as a step in the right direction, but it does not imagine an adversary who is dedicated to taking down key critical infrastructure sectors to cause our country harm. If you look at capabilities that are being developed today, you are seeing the evolution of warfare in cyber. Our government and industry must work together if we are going to defend this country. What do we need to do in terms of working together? Consider all the options that are out there and consider all of our missions. Those government missions are to protect the people and protect the nation. Conferences like JSA help develop cooperative strategies. It is beautiful when government and industry collaborate. The country that created the Internet is now coming up with ways of securing it.

AO: I think trust is the fundamental challenge underlying that question. We do have questions of trust that have not been worked, and those are corporate trust. Let me tell you what we are doing at DHS to try to earn that trust as part of that broader inter-agency effort. As General

Alexander said, this is absolutely a team sport, and we cannot do this alone at DHS, or at any other government agency. I'm particularly pleased that we have representatives here of former Department of Defense and current Department of Justice. At DHS, we have been trying to think of an easy way to help people understand our role, and I spend a lot of time now talking to Congress. During my discussions I use a fire fighting analogy. And I view every cyber incident as arson. Just like in the real world, when you have arson you want both the fire fighters and law enforcement involved. The same is true in cyber and responders. We do have instant responders, and you heard from Mark Bristow this morning. We have government instant responders in the US that help companies when they have incidents. But we do that ideally in conjunction with law enforcement. In fact our partnership with the FBI, Secret Service, and Homeland Security investigators has never been better. One of our challenges frankly is to advertise our role because one of our commitments is to keep confidential that we showed at your fire. Part of our work is developing trust in private sectors and keep confidential what we've been told. That is why we struggle to talk about our role and response.

There is another challenge, and DHS spends a great deal of time stopping cyber fires from ever happening in the first place. Think of the equivalent of inspecting smoke alarms or advocating for better building codes. We help companies by promulgating best practices. We endorsed the cybersecurity framework that helps companies large or small better adopt that framework. We share information whether its threat indicators, or whether it's more broad information about what the bad guys are doing. We do much of our work in conjunction with our NSA partners. We are pushing out information provided by NSA (who does not want attribution), or issuing a joint bulletin with the FBI. Any time that we do this, it is a response to incidents. I've heard people today proposing initiatives that we in fact are doing. I do not think we are doing it at a scale we need to do, or with the resources we need to do the mission.

I have been in this position for two years, and have seen four budgets because of the weird way government works. The first three of those budgets went up under 10 percent a year for a mission that was growing enormously in magnitude and importance. The current President's Budget is sitting in front of Congress with an increase to our budget by 30 percent, which I think is actually much more commensurate with the our requirements. When they are actually going to pass that budget? That's a separate question. I do think there is a recognition that we need to invest in cybersecurity, and I tell you that we are going to scale as rapidly as we can to meet that demand. So with that, I'll pause for now and look forward to the next question.

PC: I'm sitting up here in the panel, first of all with Andy, an Assistant Secretary, and the guy next to him whose picture I passed at work every day. But I'll see what I can do to hold my own. I'm Air Force Academy class of '86 'yippy'. The FBI is very focused on the tactical. We do have the ability to act and think strategically, and obviously we have to in order to run programs, but we are focused at the case level. The mission statement of the FBI cyber division is to identify, pursue, and defeat. With the identify piece of the mission, human beings are behind everything we are talking about today. All the routers, cables, bridges, switches, all of it is created and operated at the behest of another human being somewhere in the world. We have to impose costs to our adversaries who will do us harm. We want to help with cyber defense, but we are all about the imposing costs in this equation. The FBI determines who is responsible for doing this, and what can we do to reach out and make them stop.

I have a unique perspective imbedded within NSA and U.S. Cyber Command all day, every day. I get to see the most nightmarish material streaming in over the wires. Our goal is to work with our partners, assist the government, private sector, and local law enforcement and close in on our adversaries; from my perspective they are violating Federal Law all day long. Every time there is unauthorized access to computer systems they are violating 18 U.S. Code Section 1030. Is it possible that someday we actually lay hands on those PLA officers or seven Iranian freelance hackers who are operating on behalf of their respective governments? I have to be open to the possibility; that indictment is in place forever or until they die, or until somebody convinces the Judge and the Grand Jury to recede the issued indictment. What that means for the indicted is that there will never be an opportunity to travel outside of their respective nations without putting themselves at risk of being snatched. In my mind that is imposing a cost. That is where the FBI sees itself in this. We want to be partners, we want to help educate, we want to make sure that you have what you feel you need from the government, and if we can't

THE ROLE OF GOVERNMENT IN CYBERSECURITY

provide the support, we are going to steer you to the right government agency that can provide that information.

RG: Let's come back to the core theme of the conference: Internet of Things and connecting our critical infrastructure to parts of the Internet. The electric grid relies obviously on the interconnectivity. We keep hearing of this Ukrainian attack and how we have worked to drive down some the risk within the United States by applying lessons learned from what happened in Ukraine.

AO: I think for us the Ukrainian incident was a significant step forward in what we do. We have not got all the way there. Let me tell you about the great things we did, and then let me tell you some lessons learned. We recognized first to get some people over there and figure out what happened. We had to get the permission of the Ukrainian government and that took a bit of time. We also had to do this in such a way that my guys did not spend time in Ukrainian jail, because they laid hands on a computer or something of that nature. We got over there about four weeks after the incident, and would like to arrive faster next time. But it was a super valuable experience; we conducted interviews with folks there, and looked at the power distribution where the incident took place. We came back with lessons learned, which were excellent! We will take that information and share with the private sector to better protect ourselves.

We are hitting the road and going to cities across the US having sessions educating audiences on what happened in the Ukraine, and to stop this incident from happening here. It's not just an energy sector incident. Anybody who has a control system will be susceptible to the type of limitation that we saw in the Ukraine. We had three different locations within a thirty minute window, and at those locations attackers took action to shut down the power. The first thing that tells you of course is there is a lot of activity in three different geographical occasions within a very tight timeframe. There was a level of coordination that is very concerning. The bad guys obviously entered those systems months before through phishing emails; reinforcing Secretary Johnson's point that phishing emails are still a huge threat. They moved laterally, obtained legitimate credentials, and when they actually executed the attack they appeared as legitimate users.

I think what is really important is we take this example, and have control systems operators across the US pay attention to this incident. My goal frankly, is to have the CEO's of every company with a control system send an email or call their assistant and say hey, check into this Ukraine thing, are we protected against that? That is the change that I want to drive. With our work with the FBI, and our campaign across the US, I think we are making great strides.

RG: Phil, let's talk a little about engaging with the private sector.

PC: I remember five, six years ago a response by three government agencies to a major financial institution. Each of the agencies showed up, had their own non-disclosure agreement, and according to those NDA's incapable of sharing information. The government is actually capable of learning and evolving. We all collectively got together and started to strategize a way ahead. In the event of a major computer intrusion, what is everyone's respective role? We can't keep moving into each other's lanes and duplication of effort is never a good idea. So we worked through these issues and it's never going to be perfect, but it's pretty damn good right now.

Information comes into the NSA at a very high level of classification. We know this attack is targeting a certain company or certain sector here in the US. How do we get that information to the company? In the past, FBI Agents or other law enforcement would contact the company and advise them they have a pretty big problem in their network and you might want to take a look. We could not tell them much more than that and so it wasn't really a meaningful interaction. Now the NSA/CSS Threat Operations Center actually takes this most highly classified collection and automatically gets it downgraded to an unclassified provision, which provides information to industry in a matter of hours, rather than weeks, or months; this is a major improvement.

RG: General Alexander, could you give us insight into the President's new Commission regarding goals, focus and what you would like to see come out of this initiative?

KA: The Commission is an appointed body. The minutes of the meetings are all written in public law. Our charter has us looking at Federal IT, National Security, and critical infrastructure. This kind of discussion at JSA regarding cyber workforce, Internet of Things, and research & development are all of interest to the Commission. The key issue that the Commission faces is how to produce something meaningful. And I think that's where you all can help. Key issues that the Commission will take on concerns the public and industry. We are going to travel to New York City, Chicago, Dallas, San Francisco, and then back to Washington, D.C. At each visit, we will have a public discussion and look at various sectors. You are all encouraged to send information to the Commission regarding encryption and what you think about information sharing. This will be of great value. What do I hope will come out of this? I hope we can encourage the public-private partnerships. How do we identify some of the problems that are out there, which impedes our nation? Imagine we are a football team trying to win a game. Our Commission's objective is protect our country and way of life. It's not either or, it's both. Everything is on the table, and with the collective wisdom that we have in government and industry we will solve these problems. We need a national vision and people to act as a team.

RG: Phil, you see a lot of trepidation from companies who are afraid that if they called the FBI to get assistance, what they are going to get is police tape put on their front door and not being able to restore their systems.

PC: This question comes up a lot and thankfully most of the time when it does, I'm with somebody from DHS. Who is Cyber 911? Does a company call DHS, FBI, or Secret Service? My message is this, and I can actually say this with a straight face that if you call one you are calling all. We are immediately sharing it through the 24/7 Cyber Watch. It's quite remarkable and a good news story. Now, when your company reports a serious breach, or loss of data, somebody from FBI, DHS, or another law enforcement component is going to show up. When we come to your facility to get on your network, 99 times out of a 100 we are doing so in a consent construct. We ask what's going on, what did you see, ask some further questions about your network and what kind of things are you working on, what do you think they are after, and then we ask if we can take a look? And that's the consent portion of this; we are operating with your consent as the network owners. Based on what we see, we are going to share with our partner's; it may not mean anything to us, but it may mean everything in the world to the guys in the NSA enterprise. So, we're going to ask for your permission to share that information. We are not going to put out a Press Release. Every time that I'm aware of in the past three years where it's been revealed that the FBI is conducting a cyber investigation of a company, it came from either inside the company, or someone connected to the company. It does not come from the FBI or the DHS. If that is one of the underlying fears behind not wanting to pick up the phone and call and talk to the government, please let me alleviate your concerns.

RG: General Alexander, could you talk from your government and private sector experience about the application of lessons learned from DoD?

KA: I think the biggest difference is how you look at the network. How you look at achieving objectives in cyberspace, which may be one of different objectives an adversary would want to take. In cyberwar, what are the steps and strategies that you want to take to keep an adversary from entering your network? You see what Russia has done to Estonia, to Georgia, to Ukraine, and you see what Iran did to Saudi Arabia. Terrorists are getting increased capabilities. In the next five years you will see a massive cyberattack in the US.

GEN (R) KEITH ALEXANDER ADDRESSING JSA AUDIENCE

PANEL DISCUSSION

CLOSING REMARKS

INTRODUCTION OF CONGRESSMAN MIKE POMPEO

Congressman Mike Pompeo is a 3rd term congressman from the 4th District of Kansas. He is a 1986 West Point graduate who has served as a cavalry officer before the fall of the Berlin Wall and served with the 2nd Squadron, 7th Cavalry in the Fourth Infantry Division. After graduating from Harvard Law School, he founded Thayer Aerospace before becoming President of Sentry International. Mr. Pompeo serves on the House Committee on Energy and Commerce and the House Permanent Select Committee on Intelligence. Please welcome Congressman Pompeo.

CONGRESSMAN MIKE POMPEO

Thanks for the kind introduction. It's great to be here! Lieutenant General Caslen wouldn't admit this but he is largely responsible for my career. When I was a plebe 29 years ago, Captain Caslen was my cadet officer in Company A.

I called my son who works software in New York City for a Silicon Valley based company, and told him I was coming here to speak to the JSA, and he said Dad, what the heck do you know about cyber? The answer is that I know a little bit about cyber as a result of my work experience.

When General Alexander asked me to speak, I decided we would find places that I actually did know something about. After searching for a topic, we decided that I'll share with you my five years experience working on cyber issues in Congress. I could talk for hours about the absence of cyber knowledge on Capitol Hill regarding the very issues talked about today. You have talented people in Congress working diligently to try and help address your problems, challenges and opportunities that we've all talked about today. I have been here for most of the conference. I actually heard nine, maybe thirteen criticisms of Congress today, and the great thing about speaking last is that I can address them.

I'm in my 3rd term in Congress, I represent Wichita Kansas, and I'm a conservative Republican. I will share my views, talk about the issues that I deal with on the Intelligence Committee, and the Energy and Commerce Committee. I'm talking today not as a professional, but as a citizen and taxpayer. I want to discuss who is going to pay the freight for some of these things? We talk about security and privacy, but often forget profit. I want to talk about three things. The American political discourse surrounding cyber issues, how I have experienced it, and how my colleagues on Capitol Hill have experienced it. I'll talk on how we all have a role in making sure we discuss the American cybersecurity infrastructure, and if we do not talk about it in the right way, we will destroy it, while we all try to fix it. Language matters; when you go out and speak on FOX News you do not have nine-hours that we had today. Then, I want to talk about where as a member of Congress, how I see these cyber threats evolving and where you can help.

General Alexander talked about how people come into government, I promise you I will not be serving in Congress for forty years. I intend to perform my function for a moment in time and serve the people of Kansas and America. I have to begin by giving credit to the institution that I am serving, and how industry and government can work together. I want to talk about Article 1 and the folks who have this constitutional duty to draft laws as citizens and taxpayers, and how we talk about this is in a way to achieve the objectives that we all share. This brings us to Edward Snowden and the time he became a traitor and stole billions of pages of documents from the US government, and yet you have members of Congress talking about him as if he performed a public service that I find both inaccurate and disgusting. From the perspective of our JSA summit, I find it deeply at odds with what we are all trying to achieve. I watched some of my colleagues go on television news to say the NSA is listening to your phone calls and reading your emails. If members of Congress were doing their jobs they would have known better. We can all have disputes about the collection process, but we ought not to strike the people who are trying keep us all safe from evil.

I will tell you that shortly after Mr. Snowden was invited to speak at South by Southwest. The venue was sponsored by companies sitting in this room. I wrote a letter that they have constitutional right to bring whoever they want to speak on any topic that they want under the First Amendment. What would merit this major cyber and software conference to support Mr. Snowden's message and have their logos on stage? They have sanctioned the type of behavior in which he engaged. We talked today at this conference about building trust to convince them the government is working to keep their network safe and to keep bad guys out of the system and prevent incidents just like the Snowden case.

We are about to have the same fight again. This one is more important. You know the provisions in Section 702 of the Foreign Intelligence Surveillance Act. It is essentially the core program that forms intelligence around the world, and in its absence you will all be materially less safe, and I assure you our active duty troops would be materially less safe. I've watched the forces array and gear up for a fight with each sides taking maximum positions. If we are going to have an important robust debate about cyber issues, about intelligence collection issues, about data collection, and the use of that data involving the private sector and the government, we have to be candid and speak honestly. Today, some folks talked about the battle between Apple and their broken iPhone. I took a day and read everything that has been written. I watched the FBI make their case, and watched Apple take their position. They can't possibly have met—right! You think about Apple's position. Apple's position was at no time can the government force us to take any action. I remember going to law school a long time ago, and we talked about the Fourth Amendment and seeking consent.

I listened to folks today and the conversation has covered a wide range of topics. I called my doctor, and he is taking my Social Security number off my health records. Folks at the JSA summit have commented that Congress does not have a strategic vision. I think that the government does not have a strategic vision, and this an enormously fair criticism and indeed it may be too kind to this institution. It is difficult for an elected official to develop a strategic vision in a world with cyber moving so fast. You should know that the place for this vision is not sitting in the cubicle some place in Washington, D.C.

I remember working to develop a piece of cyber legislation on intelligence sharing, and was the designated liaison tomy class of 2010; ninety Republicans who came to Congress under the Tea Party. Most of them were like me; I ran a machine shop before coming to Congress. We haven't changed machinery technology material since the early 1950's. It's a fast moving world, and Congress cannot by their very nature, continue to keep up. You have no additional duties, tomorrow someone will want to talk to me about national parks, and the day after a huge project for the Corps of Engineers in my district. You must understand that Congress wants to get to the right place, but theyneed enormous assistance to do it. When they see some industry folks talk about a subject that is not productive, they turn away, and are inclined to do something that would harm all of us and not just in industry. We saw your response to this issue, which would generate legislation of enormous restrictions and enormous mandates. Needless to say, that is not the best way to legislate. If the trust does not exist today, there is no building that trust in moments of crisis.

Last stop; we are spending an awful lot of money today, and I don't mean to be too cynical, but if you are an agency and trying to figure out how to expand your budget, you create a cyber section. It's trendy, new, and everybody wants one. You have to help us identify the means to effectively ensure we have a cyber infrastructure that works today, next week and a decade from now. We have a greatdeal of resource duplication; it may have made sense at the time the money was identified and put in place, but is no longer needed. If we can do those things, if we can find the space to work together and talk about the cyber challenges in an intellectual way, we would be more likely as members of Congress executing legislation where you can go run your business and make money, which is what I hope for you. And that you will be able get privacy into profit in a way that would keep us all safe.

Before I got on the plane yesterday, I got a note to see the Intelligence Committee to receive a briefing on a cyber incident. Very seldom do these attacks have more than 5 digits to the left of the decimal place; often it's only 4. On some occasions there is no cost. We can and must get to the right place for our Soldiers, Sailors, Airmen, Marines, and industry. Our GDP depends on it, and as I look at this JSA audience, you can help me achieve these goals. We need to get the law right, and then go execute this alongside you to keep America free, secure, and prosperous.

Thank you very much for letting me be here today, God bless you!

COLONEL J. CARLOS VEGA

This concludes our formal portion of the ceremonies.

JSA BIOGRAPHIES

LIEUTENANT GENERAL ROBERT L. CASLEN, JR., HOST

Lieutenant General Robert L. Caslen, Jr. became the 59th Superintendent of the U.S. Military Academy at West Point on July 17, 2013. Lieutenant General Caslen graduated from the U.S. Military Academy in 1975. He earned master's degrees from Long Island University and Kansas State University. Previous to this assignment, Lt. Gen. Caslen served as the Chief of the Office of Security Cooperation Iraq. Lieutenant General Caslen's prior deployments and assignments include serving as the commander of the Combined Arms Center at Fort Leavenworth, KS., the command that oversees the Command and General Staff College and 17 other schools, centers, and training programs located throughout the United States; commanding general of the 25th Infantry Division (Light) and commanding general of the Multi-National Division-North during Operation Iraqi Freedom; Commandant of Cadets for the U.S. Military Academy; Deputy Director for the War on Terrorism, J-5, The Joint Staff; Assistant Division Commander (maneuver), 3rd Infantry Division (Mechanized); Chief of Staff, 10th Mountain Division (Light); Chief of Staff, Combined Joint Task Force Mountain during Operation Enduring Freedom; Commander, 2nd Brigade, 101st Airborne Division (Air Assault); Chief of Staff, 101st Airborne Division (Air Assault); Senior Brigade C2 Observer/Controller, Operations Group, Joint Readiness Training Center; Commander, 1st Battalion, 14th Infantry, 25th Infantry Division (Light); Executive Officer to the Deputy Commander in Haiti during Operation Uphold Democracy; J-3 in Honduras for Joint Task Force Bravo; Brigade Operations Officer, 3rd Brigade, 101st Airborne Division (Air Assault); Executive Officer, 2nd Battalion, 187th Infantry, 101st Airborne Division (Air Assault) during Operations Desert Shield/Desert Storm.

COLONEL ANDREW O. HALL, CO-CHAIR

Colonel Andy Hall is the Director of the Army Cyber Institute. He studied Computer Science at West Point, Applied Mathematics at the Naval Postgraduate School, and Operations Research at the Robert H. Smith School of Business at the University of Maryland. He has served on the Army Staff, Joint Staff, and MNC-I/XVIIIth ABC Staff deployed to Iraq. He is a Cyber officer and was instrumental in creating the Army's newest branch.

MR. MARK D. MCLAUGHLIN, CO-CHAIR

Mark D. McLaughlin Chairman, is Chairman, President and CEO of Palo Alto Networks. In August of 2011 and became Chairman of the Board in 2012. Before coming to Palo Alto Networks, Mark served as President and CEO of Verisign. Prior to that, he held a number of key positions at Verisign including serving as Chief Operating Officer, Executive Vice President of Products and Marketing, and head of the company's Naming Services business. Prior to Verisign, he was the Vice President of Sales and Business Development for Signio, a leading Internet payment company. Before joining Signio, he was the Vice President of Business Development for Gemplus, the world's leading smart-card company. Previous to Gemplus, he also served as General Counsel of Caere Corporation and practiced law as an attorney with Cooley Godward Kronish LLP. President Barack Obama appointed Mark to serve on the National Security Telecommunications Advisory Committee (NSTAC) in January, 2011. In 2014, President Obama appointed Mark to the position of Chairman of the NSTAC. He received his J.D., Magna cum Laude, from Seattle University School of Law and his B.S. Degree from the United States Military Academy at West Point. He served as an attack helicopter pilot in the U.S. Army and earned his Airborne Wings.

LIEUTENANT GENERAL EDWARD C. CARDON

Lieutenant General Edward C. Cardon, Commander, U.S. Army Cyber Command and Second Army. Lieutenant General Edward C. Cardon was born in Texas, raised in California and was commissioned as an Engineer Officer from the United States Military Academy in 1982. His company grade assignments include: Platoon Leader and Battalion Maintenance Officer with the 17th Engineer Battalion (Combat), 2nd Armored Division, Fort Hood, Texas; Training Officer with the 130th Engineer Brigade, V Corps; Brigade Engineer for 3rd Brigade, 3rd Armored Division; Company Commander, C Company, 23rd Engineer Battalion, 3rd Armored Division; Staff Officer and Engineer Company Trainer for the Live Fire Team, Operations Group, National Training Center; and Instructor, United States Army Engineer School. After graduation from the Naval Command and Staff College, he served as the Assistant Division Engineer, 3rd Infantry Division (Mechanized); Executive Officer, 82nd Engineer Battalion, 1st Infantry Division (Mechanized); Staff Geographic Officer for Land Forces Central Europe, NATO; Chief Geographic Officer, IFOR/SFOR Bosnia-Herzegovina; Battalion Commander of the 588th Engineer Battalion, 4th Infantry Division (1998-2000); and as Special Assistant (Strategy) for the Army Chief of Staff, Pentagon (2000-2002).

SECRETARY JEH JOHNSON

The Honorable Secretary Jeh Charles Johnson was sworn in on December 23, 2013 as the fourth Secretary of Homeland Security. Prior to joining DHS, Secretary Johnson served as General Counsel for the Department of Defense, where he was part of the senior management team and led the more than 10,000 military and civilian lawyers across the Department. As General Counsel of the Defense Department, Secretary Johnson oversaw the development of the legal aspects of many of our nation's counter terrorism policies, spearheaded reforms to the military commissions system at Guantanamo Bay in 2009, and co-authored the 250-page report that paved the way for the repeal of "Don't Ask, Don't Tell" in 2010. Secretary Johnson's career has included extensive service in national security, law enforcement, and as an attorney in private corporate law practice. Secretary Johnson was General Counsel of the Department of the Air Force from 1998 to 2001, and he served as an Assistant U.S. Attorney for the Southern District of New York from 1989 to 1991.

MR. RICHARD LEDGETT

Mr. Richard (Rick) Ledgett serves as the Deputy Director and senior civilian leader of the National Security Agency. In this capacity he acts as the Agency's chief operating officer, responsible for guiding and directing studies, operations and policy.

Mr. Ledgett began his NSA career in 1988 and has served in operational, management, and technical leadership positions at the branch, division, office, and group levels. From 2012 to 2013 he was the Director of the NSA/CSS Threat Operations Center, responsible for round-the-clock cryptologic activities to discover and counter adversary cyber efforts. Prior to NTOC he served in several positions from 2010 to 2012 in the Office of the Director of National Intelligence in both the collection and cyber mission areas. He was the first National Intelligence Manager for Cyber, serving as principal advisor to the Directorof National Intelligence on all cyber matters, leading development of the Unified Intelligence Strategy for Cyber, and coordinating cyber activities across the Intelligence Community (IC). Previous positions at NSA include Deputy Director for Analysis and Production (2009-2010), Deputy Director for Data Acquisition (2006-2009), Assistant Deputy Director for Data Acquisition (2005-2006), and Chief, NSA/CSS Pacific (2002-2005). He also served in a joint IC operational activity, and as an instructor and course developer at the National Cryptologic School. Mr. Ledgett spent nearly 11 years in the U.S. Army as a SIGINTer and, between the Army and NSA, has completed 6 field tours.

GENERAL RAYMOND T. ODIERNO, USA, RETIRED

General Raymond T. Odierno became the 38th Chief of Staff of the US Army. He is Senior Advisor to the Chairman, CEO, and Operating Committee, JP MorganChase. Gen. Odierno culminated his military career as the 38th Chief of Staff of the United States Army from 7 September 2011 to 14 August 2015. A native of Rockaway, New Jersey, Gen. Odierno attended the United States Military Academy at West Point, graduating in 1976 with a commission in Field Artillery. With more than 39 years of service, he commanded units at every echelon, from platoon to theater, with duty in Germany, Albania, Kuwait, Iraq, and the United States. From December 2006 to February 2008, he served as the Commanding General, Multi-National Corps-Iraq (III Corps), the operational commander of the surge of forces Later, he served as the Commanding General, Multi-National Force-Iraq and subsequently United States Forces-Iraq, from September 2008 until September 2010. From October 2010 until August 2011, he was the Commander of United States Joint Forces Command. During his tenure as Army Chief of Staff, Gen. Odierno was influential in the development and activation of US Army Cyber Command and the Army Cyber Institute at West Point.

CONGRESSMAN MIKE POMPEO

Congressman Mike Pompeo is a 3rd term congressman from the 4th District. As a teenager, he enrolled at the United States Military Academy at West Point and graduated first in his class in 1986. He then served as a cavalry officer patrolling the Iron Curtain before the fall of the Berlin Wall. He also served with the 2nd Squadron, 7th Cavalry in the forth Infantry Division. After active duty, Mike graduated from Harvard Law School and was an editor of the Harvard Law Review. Mike later returned to his mother's family roots in South Central Kansas and founded Thayer Aerospace, where he served as CEO for more than a decade providing components for commercial and military aircraft. He then became President of Sentry International, an oilfield equipment manufacturing, distribution, and service company.

JSA BIOGRAPHIES - PANELISTS

GENERAL KEITH ALEXANDER, USA, RETIRED

Founder and CEO of IronNet Cybersecurity, is one of the foremost authorities on cybersecurity in the world. A four-star Army general, GEN Alexander was previously the highest-ranked military official of USCYBERCOM, NSA/CSS, where he led these DoD agencies during the conflicts in Afghanistan and Iraq when attempted cyber attacks against the U.S. were on the rise. In recognition of cyber's increasing importance, President Barack Obama and Defense Secretary Robert Gates appointed GEN Alexander as the first commander of USCYBERCOM, a newly created military command charged with defending the nation's security in cyberspace against sophisticated cyber threats to businesses and government operations in an increasingly interconnected world.

LIEUTENANT COMMANDER JOSEPH BENIN

Upon graduating with a bachelor's degree in Electrical Engineering with High Honors from the United States Coast Guard Academy (USCGA) in 2001, LCDR Joseph Benin served as a student engineer and the Electrical and Electronics Officer aboard the polar ice breaker USCGC HEALY (WAGB-20). He holds Masters Degrees in Electrical and Computer Engineering (ECE) and Information Security (INFS) with a PublicPolicy minor and a Doctorate of Philosophy in ECE from the Georgia Institute of Technology (go Yellow Jackets!). He joined the USCGA Faculty in 2005 and was selected as a member of the Permanent Commissioned Teaching Staff (PCTS) the same year. LCDR Benin is a registered Professional Engineer.

MR. MARK BRISTOW

Chief for Incident Response and Management for the Industrial Control Systems Cyber Incident Response Team (ICS-CERT) at the National Cybersecurity and Communications Integration Center (NCCIC) within the DHS. Mark has been with ICS-CERT, and its predecessor organization the control system security program (CSSP) since 2008. Mark has worked previously conducting assessments and penetration tests of industrial control systems equipment in multiple sectors with a focus on electric power generation, transmission and distribution. Mark has a bachelor's degree in Computer Engineering from Pennsylvania State University.

MR. PHIL CELESTINI

Veteran Special Agent of the Federal Bureau of Investigation who has served in a wide variety of field division and headquarters assignments. Mr. Celestini is currently assigned to the FBI's Cyber Division, stationed at Fort Meade, Maryland as the Senior Executive FBI Liaison to the National Security Agency and U.S. Cyber Command. Mr. Celestini received his Bachelor of Science degree from the United States Air Force Academy in 1986, and also holds a Master of Science in Public Safety Leadership. Prior to entering the FBI, Mr. Celestini served our nation in the United States Air Force as an Intelligence Operations Officer, followed by a brief career as Acting Director of Security at the Centers for Disease Control and Prevention in Atlanta, Georgia.

MAJOR MICHAEL V. CHIARAMONTE

Assistant Professor of Computer Science at the United States Air Force Academy in Colorado Springs, Colorado. He is responsible for course development and execution in a variety of disciplines to include Operations Research, Cyber Security and Computer Science. Currently he is responsible for directing the Cyber Warfare Fundamentals and Computer Simulation courses. He also teaches Network Security and conducts research into cyberspace security and education topics.

MR. RYAN GILLIS

Vice President of Cybersecurity Strategy and Global Policy for Palo Alto Networks where he is responsible for developing corporate policy, serves as the company's primary interface for global public policy and legislative matters, and leads company participation in various industry associations. In this role, Ryan serves as a liaison with government agencies and companies around the world to assist in the development of strategies and operational partnerships to prevent against cybersecurity threats.

MR. RICK HOWARD

CSO for Palo Alto Networks where he is responsible for the company's internal security program, the oversight of the Palo Alto Networks Threat Intelligence Team and the development of thought leadership for the cyber security community. His prior jobs include the CISO for TASC, the GM of iDefense and the SOC Director at Counterpane. He served in the U.S. Army for 23 years and spent the last two years of his career running the Army's CERT. Rick holds a Master of Computer Science degree from the Naval Postgraduate School and an engineering degree from the U.S. Military Academy. He taught computer science at the Military Academy and contributed as an executive editor to two books: "Cyber Fraud: Tactics, Techniques and Procedures" and "Cyber Security Essentials."

LIEUTENANT COLONEL MIKE LANHAM

Lieutenant Colonel Mike Lanham received his ROTC commission as an Infantry officer from North Carolina State University in December 1992. He became a Functional Area 53—Information Systems Management office in 2003. He has served in numerous deployments to Macedonia, Boznia-Herzegovina, Sierria Leone, Liberia, and Kuwait. His military assignments included duty with 2-15IN, 3rd ID (Mech) (Schweinfurt, Germany) and Special Operations Command Europe (Stuttgart, Germany) as well as with the 1st BDE and 1-327IN, 101st Airborne Division (Air Assault) (Fort Campbell, Kentucky). He has also served as faculty at USMA, in various staff positions with USSTRACOM, Joint Functional Component Command (JFCC)-Integrated Missile Defense (IMD), JFCC-Network Warfare (JFCC-NW), USARCENT, and USASMDC/ ARSTRAT/ ARFORCYBER. His current research interests revolve around finishing his dissertation in "Rapid Mission Assurance Assessment via Socio-Technical Modeling and Simulation."

DR. ANDREA M. MATWYSHYN

A legal academic studying technology innovation and its policy implications, particularly corporate information security regulation and consumer privacy. She is currently a full professor of law and professor of computer science at Northeastern University, a faculty affiliate of the Center for Internet and Society at Stanford Law School, and a visiting research collaborator at the Center for Information Technology Policy at Princeton University, where she was the Microsoft Visiting Professor during 2014-15. She is a US-UK Fulbright Commission Cyber Security Scholar award recipient in 2016-2017.

DR. FERNANDO MAYMI

Deputy Director of the Army Cyber Institute at West Point and an Assistant Professor in the Department of Electrical Engineering and Computer Science. Dr. Maymí has over 25 years of experience as a leader in information systems security. He has authored and taught dozens of cyber security courses for academic and professional audiences and is co-author of 3 patents. He holds a Ph.D. in Computer and Information Sciences and Engineering from the University of Puerto Rico

MR. SCOTT A. MONTGOMERY

Vice President and chief technical strategist for the Intel Security Group at Intel Corporation. He manages the worldwide team of chief technology officers who lead the group's various business units and is responsible for advancing technical innovation in Intel's security solutions. Montgomery has dedicated his career to information security and privacy software development, gaining a breadth of expertise that spans endpoint protection, firewalls, intrusion prevention, encryption, vulnerability scanners, network visibility tools, mail and Web gateways, authentication, and embedded systems. He joined the Intel organization in 2011 with the acquisition of McAfee Inc., now a wholly owned subsidiary that operates as the Intel Security Group.

DR. ANDY OZMENT

Working in cybersecurity for almost twenty years as an operator, programmer, policymaker, and executive in both the government and private sector. As the Assistant Secretary for Cybersecurity and Communications at the Department of Homeland Security, he is charged with protecting the government against cyber attacks and helping the private sector protects itself. His organization helps its customers by responding to incidents, sharing information, developing and promulgating best practices, and increasing our nation's cybersecurity capacity.

PROFESSOR STEPHANIE PELL

Assistant Professor and Cyber Ethics Fellow at West Point's Army Cyber Institute (ACI) and teaches Cyber Ethics in the Department of English and Philosophy. She writes about privacy, surveillance and national security law and policy. Prior to joining West Point's faculty, Stephanie served as Counsel to the House Judiciary Committee and was a federal prosecutor for over fourteen years. Stephanie received her undergraduate, master's and law degrees from UNC Chapel Hill.

MR. JIM ROUTH

Aetna Chief Information Security Officer and leads the Global Information Security function for Aetna. He is the Chairman of the National Health ISAC and a Board Member of the FS-ISAC. He was formerly the Global Head of Application & Mobile Security for JP Morgan Chase. Prior to that he was the CISO for KPMG, DTCC and American Express and has over 30 years of experience in information technology and information security as a practitioner. He is the Information Security Executive of the Year winner for the Northeast in 2009 and the Information Security Executive of the Year in 2014 in North America for Healthcare. He has published several white papers including the FS-ISAC 3rd Party Software Security Controls paper and leads several cross functional information security working groups.

MR. MARCUS SACHS

Senior Vice President and Chief Security Officer of the North American Electric Reliability Corporation in Washington, D.C. where he is responsible for the oversight of the Electricity Information Sharing and Analysis Center (E-ISAC), and for directing security risk assessment and mitigation initiatives to protect critical electricity infrastructure across North America. He also leads day-to-day coordination with governmental agencies and stakeholders regarding security matters, including analysis, response and dissemination of critical information regarding security threats and events.

DR. EDWARD SOBIESK

Director of the Education and Force Support Division for the Army Cyber Institute at West Point and an Associate Professor in the Department of Electrical Engineering and Computer Science. Dr. Sobiesk spent 28 years in the U.S. Army, retiring as a colonel, and he has almost two decades of experience as an educator, leader, and practitioner within the Cyber Domain. He has taught over 15 different computer science and information technology courses and has directed three different computing programs at West Point; he has run a 200 person computer support directorate for an intelligence command; and he has over 30 invited or refereed academic publications. Dr. Sobiesk holds a Ph.D. in Computer and Information Sciences from the University of Minnesota. His research interests include online privacy and usable security, computer science & information technology education, and emerging technologies.

CAPTAIN PAUL TORTORA, USN, RETIRED

CAPT Paul Tortora, USN, Ret., is currently the Director of the Center for Cyber Security Studies and the first Chair of the new Cyber Science Department at the United States Naval Academy. Paul recently retired from the Navy following a 26-year active duty career originally as a Nuclear Submarine Officer and then as a Naval Intelligence Officer. During his active service he served and deployed on two nuclear fast attack submarines, two amphibious assault ships, and a nuclear aircraft carrier, conducting various peacetime and combat operations across the globe. His ashore assignments included Director of Training at the Navy and Marine Corps Intelligence Training Center, on the staff of the Director of Naval Intelligence, as Naval Aide and Intelligence Officer to the Secretary of the Navy, and with the Office of the Director of National Intelligence.

COLONEL J. CARLOS VEGA

COL Vega is a Cyber Officer, Senior Army Aviator and the Director of Outreach for the ACI. He has served in multiple leadership roles in the Army; Commander (CEO), CIO–Logistics for US Army Forces in South Korea, and multiple roles with the XVIII Airborne Corps (CISO, CTO), culminating as the Chief of Cyber Operations in the emerging cyber discipline and domain. COL Vega earned BA and MS completed the resident portion of a Ph.D. (ABD) from the Naval Postgraduate School in Monterey, CA.

ARMY CYBER INSTITUTE (ACI)

VISION

To develop intellectual capital and impactful partnerships that enable the nation to outmaneuver our adversaries in cyberspace.

MISSION

The ACI is a national resource for research, outreach, and education in the cyber domain, engaging Army, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations.

ACI LEADERSHIP

Colonel Andrew Hall
Director and Assistant Professor

Dr. Fernando Maymi
Deputy Director and Assistant Professor

Master Sergeant Jeffrey Morris
Sergeant Major and Assistant Professor

CIVILIAN ADVISORS

Lieutenant General (Ret) Rhett Hernandez
USMA Cyber Chair

Marshal N. Carter
Chairman, NYSE Group, Inc.

Neal Creighton
CEO, CounterTack, Inc.

George Cybenko
Dorothy and Walter Gramm
Professor of Engineering, Dartmouth College

Major General (Ret) John Davis
Vice President, Federal Chief Security Officer,
Palo Alto Networks

Brigadier General (Ret) Jeffery G. Smith, Jr.
Dean of Faculty, Virginia Military Institute

Vincent Viola
Chairman and CEO, Virtu Financial, NY

MILITARY ADVISOR

Lieutenant General Edward C. Cardon
Commander, United States Army Cyber Command

JSA CYBER SECURITY SUMMIT

ACI

Colonel J. Carlos Vega
Director of JSA

Lieutenant Colonel Glenn Robertson
Program Committee Chair

Major Terence Kelley
Public Affairs Officer

PALO ALTO NETWORKS

Rick Howard
Chief Security Officer

Ryan Gillis
Vice President, Cybersecurity Strategy
and Global Policy

Major General (Ret) John Davis
Vice President, Federal Chief Security Officer

Susan Stover
Senior Field Marketing Manager

UNITED STATES MILITARY ACADEMY
WEST POINT.

UPCOMING CYBER EVENT

CYCON U.S. OCT 21-23 2016

The inaugural U.S. based International Conference on Cyber Conflict will take place 21-23 October 2016 in Washington D.C. Focusing on a theme of Protecting the Future. CyCon U.S. is organized by the Army Cyber Institute at West Point, in collaboration with the NATO Cooperative Cyber Defense Center of Excellence.

JSA
JOINT SERVICE ACADEMY
CYBER SECURITY SUMMIT

2016 JSA CYBER SECURITY SUMMIT

EVENT CO-HOST paloalto NETWORKS

COMMENTARY ◆ KEYNOTES ◆ PANEL DISCUSSIONS

SYNCHRONIZED SECURITY

PUBLIC ◆ PRIVATE PARTNERSHIPS IN CYBERSPACE

THE ARMY CYBER INSTITUTE AT WEST POINT