4-1-2015

No. 9 - Cybersecurity and National Defense: Building a Public-Private Partnership

Rebecca H. White
University of Georgia School of Law

C. Donald Johnson
University of Georgia School of Law

Loch K. Johnson
University of Georgia

Quentin E. Hodgson
United States, Office of the Secretary of Defense

Jamil Jaffer
George Mason University Law School

See next page for additional authors

Authors
Rebecca H. White, C. Donald Johnson, Loch K. Johnson, Quentin E. Hodgson, Jamil Jaffer, Clete D. Johnson, Victoria Woodbine, Timothy L. Meyer, Adam Golodner, Barry Hensley, Andrea Matwyshyn, and Jacob Olcott

Occasional Papers

Dean Rusk Center

University of Georgia School of Law

Number 9

Cybersecurity and National Defense: Building a Public-Private Partnership

Panel 1 – The National Security Threat

Panel 2 – The Private Sector Role in Addressing Cybersecurity Risks

Lunchtime Address – The FCC's 'New Paradigm' for Communications Security in the Internet Era, *Clete D. Johnson, Chief Counsel for Cybersecurity, Federal Communications Commission*

NUMBER 9 SPRING 2015

For more information about the Dean Rusk Center,
please visit us at: **www.law.uga.edu/dean-rusk-center**

Cybersecurity and National Defense: Building a Public-Private Partnership

Organized and sponsored by the Dean Rusk Center for International Law and Policy, *Cybersecurity and National Defense: Building a Public-Private Partnership* was a daylong conference exploring issues related to the national security dimensions of cyber attacks as well as the role of the private sector in addressing cybersecurity risks. The overarching theme was the scope of public-private collaboration in addressing cybersecurity risks and the potential for future cooperation between government and the private sector. Clete D. Johnson, Chief Counsel for Cybersecurity at the Federal Communications Commission gave a lunchtime address on the FCC's approach to communications security in the Internet era. The transcript of the conference proceedings has been edited for publication with the consent of the speakers.

Edited by: Laura Tate Kagel, Assistant Director, Dean Rusk Center for International Law and Policy, University of Georgia School of Law

Published by: The Dean Rusk Center (Athens, GA)

The Dean Rusk Center for International Law and Policy

The Dean Rusk Center was established in 1977 to expand the scope of research, teaching, and service in international law and policy in order to increase understanding of international issues, provide a sound basis for foreign policy decision-making, and contribute solutions to global problems. Today the Center serves as a nucleus for collaboration between University of Georgia School of Law faculty and students, the law school community, and diverse international partners on foreign and transnational legal and policy matters.

In fulfillment of its mission to globalize legal education at the University of Georgia, every year the Rusk Center the Center invites scholars from abroad to engage in collaborative research with faculty and to teach short courses that enhance the law school's educational offerings. In addition to faculty exchange programs with foreign universities, the Rusk Center administers highly praised summer programs in Beijing and Shanghai, and Brussels and Geneva. The Global Internship Program with placements in thirty-five countries around the world provides another excellent opportunity to gain international experience.

An important function of the Rusk Center is to provide a forum for the exchange of ideas about important international legal and policy matters. Every spring Georgia Law's international faculty hosts a colloquium series on timely topics in the field of international law. With the goal of engaging a broad audience on matters of global significance, the Center sponsors conferences and lectures with high-level policy makers, diplomats, scholars, and practitioners. The Rusk Center also offers guidance and support to international student organizations, including the *Georgia Journal of International and Comparative Law*, and frequently collaborates with them on organizing conferences and lectures.

Through its public service and outreach programs, the Rusk Center influences policy regionally and on a global scale. It has provided research and counsel to the Georgia governor's office on international trade issues since its inception, most recently by participating in the establishment of a trade office in China. In 2008, the Center's director, C. Donald Johnson, a former ambassador in the Office of the United States Trade Representative, met with President George W. Bush and his senior trade officials at the White House to advise them on current trade initiatives. Over the past sixteen years, the Center's renowned International Judicial Training Program (IJTP) has trained over twelve hundred foreign judges and court personnel and provided models for concrete judicial reforms in participating countries.

Finally, Rusk Center publications, such as this Occasional Papers series, disseminate the results of work done at the Center, including conference proceedings on diverse themes.

Further information on the Dean Rusk Center for International Law and Policy is available at:
www.law.uga.edu/dean-rusk-center

Cybersecurity and National Defense: Building a Public-Private Partnership

TABLE OF CONTENTS

Cybersecurity and National Defense: Building a Public-Private Partnership

March 31, 2014
Welcome and Introduction

Rebecca H. White, Dean and J. Alton Hosch Professor of Law,
University of Georgia School of Law
C. Donald Johnson, Director, Dean Rusk Center for International Law and Policy,
University of Georgia School of Law

REBECCA H. WHITE: My name is Rebecca White, and I'm the dean of the University of Georgia School of Law, and it's a real pleasure to welcome you here this morning. A special thank-you to our panelists. We have such an impressive group. It's a real pleasure to welcome Clete Johnson back to the law school—a real stand-out while he was here, and he's continued that in Washington. We're very proud of you, Clete, and glad to have you back. We're also very grateful for our partners at SPIA and Dr. Johnson; thank you so much for being here. And I really want to say a special thank-you to the Rusk Center, particularly Ambassador Don Johnson and his staff for the work that they've done to bring this group together. It's an important topic. We're so glad so many of you are here. We have about seventy people registered that will be coming in and out during the day, and we also are taping the proceedings. So, again, thank you so much to each of you, for being here and Don—to you and your staff for the work that brought us here.

Athens is a beautiful place. For those of you who have not been here before, I hope you'll have the opportunity to spend some time in Athens. We have a beautiful day for you today, and it's truly a charming college town, so I hope you have the chance to wander up there. And I hope you also have some time to look around our law school. It's one of the finest law schools in the country, one of the top public law schools in the country. We're very proud of our students and the work that we do. And so, we hope that you will take the opportunity to make yourself at home. Wander around. If you have any questions, just stop someone. They'll be happy to help you, and again, welcome and enjoy your day.

Thank you.

C. DONALD "DON" JOHNSON: Well, thank you very much Dean White. I can't tell you how important it is to have a very strong and supportive dean for what we do here at the Rusk Center in all of our international programs. I always like to start with just a brief welcome on behalf of the Rusk Center and to tell you just a little about what the Rusk Center is. The Dean Rusk Center for International Law and Policy was created in 1977 in honor of one of our professors, Dean Rusk, who also served as secretary of state for eight years under Presidents Kennedy and Johnson. We were fortunate to have him come here afterwards from the State Department, where he taught for nearly a quarter of a century. He was a great mentor to students, including myself, a great colleague to faculty members, and just a very important part of the community here.

The Rusk Center was formed . . . and I'll say that Dean Rusk was a very modest guy; he didn't want the center to be named after him. Some people in the audience knew him, and he didn't much like this building being named after him, but we forced it on him. And the idea was to expand the scope of international education, promote research in the field of law and influence policy in the international arena, which, of course, was a burgeoning field during that early 70's period. And, since that time, we've tried to fulfill the mission in a number of different ways.

One way, of course, is through the educational programs that we have — bringing in visiting scholars from all over the world, who spend a lot of time here studying U.S. law and international law, and foreign professors who teach short courses in some areas that we don't otherwise cover. And our students participate in any number of programs, including the LL.M. program, but also our study abroad programs, in Oxford — we have a semester-long program there, and we have two highly praised summer programs; one is in Shanghai and Beijing at two great universities there. We have a program that was started in 1973, shortly after Rusk came here, studying EU law in Brussels, and we've expanded it to Geneva — studying international trade law. Those two programs have been popular. We also have internships all over the world, literally in — how many countries, Maria, thirty . . . fifty?

MARÍA GIMÉNEZ: Thirty-five.

DON JOHNSON: Thirty-five countries. There have been a number of years where we have had at least a third or 25 percent of the first-year class participating in these programs. So, you can see that the international programs are one of the draws for this university and the law school. We also have a strong public outreach through the Rusk Center. Since the inception, we've been highly involved with the Georgia Department of Industry and Trade, now the Department of Economic Development. We helped find an office for them in China and we work with them on a number of international trade issues.

We are also called from time to time to Washington to help with the USTR on trade issues and a number of other issues like that. We have a highly-praised International

Judicial Training Program that helps not only our foreign judges and friends learn about U.S. law and administration of justice, but also helps fund programs like these.

Finally, and perhaps equally as important, is the forum for the expression of ideas like the one that we're having today. Next week, we'll have a professor from York University. He's going to be talking on the subject of Iran and human rights there. And then we've got a conference that we'll do with the *Georgia Journal of International and Comparative Law* in about two weeks on the role of corporations in international governance.

Last year, we did a conference on Cuba. I mention that because we have just published the proceedings in our Occasional Papers series. We will be doing the same for this program. So, you'll all get a chance to review your remarks and revise or extend them. "The Cuban Embargo: Policy Outlook After Fifty Years" was a very interesting program, as you might imagine. We had the Chief of the Cuban Interests Section, Ambassador Cabañas from Washington, come down and speak in that program and that drew a lot of discussion from the community. It was very interesting, and that's the kind of thing that we're trying to do today.

Of course, the leadership here doesn't do it alone. We have a lot of very strong support—Dr. Laura Kagel, with whom many of the speakers have been in touch, and Kay Vaughn, our office manager, and María Giménez, our associate director, who are heavily involved, as well as students. We have Eric Heath. Many of you met him last night, and Kelly Wegel — very helpful in putting these programs together. We always try to bring sort of an interagency or interdisciplinary approach to this, and that's the reason today we are joined by the School of Public and International Affairs; they are co-sponsoring this event.

We were very happy to have Dr. Loch Johnson, an old friend of mine — no relation, but an old friend and one of the most eminent professors, really, in the Southeast. You know, our football team hasn't done so well in the Southeastern Conference in the last couple of years, but Dr. Johnson was named the most influential professor in the SEC. So, we can hold his honor up at times when our football team is not doing so great.

Dr. Johnson is a national expert on intelligence and national security. He has written hundreds of articles that have appeared in the New York Times, the Washington Post, and countless other journals. And he has just published his twenty-ninth book. He was a former staffer on the Senate Intelligence Committee back during the Frank Church days — a very interesting time. He also served as staff director in the House Intelligence Committee. So, he's had an illustrious career, and he's a great professor — one of the most popular as well as the most substantive. We are very happy to have him here with us today. And I have to say, too, that he was one of the founders of the School of Public and International Affairs.

In the first panel we have everybody sitting up here for purposes of the discussion, but Loch will be introducing the speakers. We'll have each person speak for about

ten to fifteen minutes and then we'll have a joint discussion and take questions from the floor. Also, I want to mention that we're having a lunch here afterwards, and I've imposed on Clete Johnson on this panel, who does happen to be related to me, to give an overview of the mission of the FCC on cybersecurity and to talk about what their plans are for the near future. So, with that, I'll turn it over to Dr. Johnson, and thanks again for being with us. Thank you.

Cybersecurity and National Defense: Building a Public-Private Partnership

Panel 1 - The National Security Threat

Moderator: *Loch K. Johnson*
Panelists: *Quentin E. Hodgson, Jamil N. Jaffer, Clete D. Johnson, Victoria Woodbine*

LOCH K. JOHNSON: Thank you Ambassador Johnson. I appreciate your very kind introduction—thank you. Of those twenty-nine books, I think my mother is the only one who bought any of them. I see three of my students out in the audience who were making an F in my class and now are getting an A. Well, as Ambassador Johnson mentioned, I'm only going to introduce the first panel and later on you'll hear an introduction of the second panel. Let me be brief in these introductions to leave more time for the speakers. On my immediate right here is Quentin Hodgson, and he is the chief of staff for cyber policy in the Office of the Undersecretary of Defense.

And then to my immediate left is Jamil Jaffer, who currently serves as a senior Senate staffer and as an adjunct professor of law and director of the Homeland and National Security Law Program at the George Mason University Law School as well as adjunct professor at the Elliot School of International Affairs at George Washington University. All of that means he never sleeps, I think.

And then over to my right is Clete D. Johnson and as was mentioned earlier, we're not related, but he's certainly one of my best friends, and I've known him since he was on the Harvard University football team and knocking down Yalies right and left. He also went through this law school; he was one of the best students we've ever had around here. He's currently chief counsel for cybersecurity in the Public Safety and Homeland Security Bureau of the Federal Communications Commission.

And last, but certainly not least, is Victoria Woodbine, who is cyber policy lead in the Foreign and Security Policy Group of the British Embassy in Washington—a position she's held since September of 2012. We are going to have ten to fifteen minutes for each panelist, then fifteen minutes of dialogue among us, and then we'll be opening it up. And I'd like to start, if I may, with Quentin.

QUENTIN E. HODGSON: Thank you, and I want to extend a thank-you to Don Johnson and Kay Vaughn and the entire team here for having me down. They originally invited my boss, Eric Rosenbach, who is currently serving in an acting position with one of the longest titles in government, so I won't belabor and/or bore you with that, but I know he is sorry he couldn't be here with you, and I'm glad I could take the opportunity to come down. I think he would have really been excited to be here at a law school because he loves to use the Socratic method when he's speaking in public, which means that you can never quote him on anything because he's getting you to say the stuff that he would want to say if he wasn't being recorded.

I'm going to try to limit my remarks, especially since Secretary of Defense Hagel stole most of my thunder on Friday and already gave most of this talk at the retirement ceremony for General Keith Alexander, who, as you probably know, is concluding over ten years as director of NSA, the National Security Agency — the longest serving director we've ever had, as well as having served as the first commander of U.S. Cyber Command as well as the predecessor organizations, an incredible individual in many respects. Also, apparently he was the roommate of a guy named Marty [Martin E.] Dempsey, who happens to be the chairman of the Joint Chiefs of Staff right now — so someone who has deep roots and has been able to really highlight for us the threats that we see in cyberspace and has been, I think, one of the most prescient people in government thinking about this issue — not just from the perspective of what the Department of Defense needs to do but also what the United States government needs to do. So, I commend to you any of the number of speeches he's made in public, to read those, to go back and look at Secretary Hagel's comments on Friday, particularly as he talked about how we think about the employment of cyber capabilities in the defense of the United States.

What I will do is just take a few minutes to talk about what we're doing at the Department of Defense, what we're doing with other departments and agencies, and a few thoughts on topics of the day. I think one of the first things to remember, of course, is that cyberspace, which we like to think of as an operational domain like any other — like air, sea and land as well as space — is unique because it is a man-made environment. But that means it has both logical as well as physical manifestations, and both of those manifestations have real implications for how we think about policy. So, a lot of people will think about cyberspace as this amorphous thing that doesn't really exist anywhere, but there are servers and switches–and we have somebody who used to work for CISCO that can tell us all about that–that reside in physical areas. People own them, people operate them.

They're largely owned and operated by private sector companies and individuals, which means that when we think about the things that we might have to do to defend ourselves, to defend our networks and so forth against threats in cyberspace, there are a lot of complicating factors that you have to think through. It's not just the issue of a missile that is being launched at us by an adversary state. It's coming from that state; it's crossing over an ocean and potentially threatening us or one of our partners. It's

something where a threat can spread throughout a network and impact hundreds of individuals, corporations, countries worldwide.

One of the things I think it's also important to state is that, as we think about the way we operate in cyberspace, we're certainly not trying to, although we've been accused of this a lot, militarize cyberspace–that somehow the United States is using this as an opportunity to impose its will or to be reckless in cyberspace.

As the secretary [of defense] talked about on Friday, we really try to take a very deliberative approach to it. And I know many people external to government think that in some respects these new things happen sort of willy-nilly and people are off doing crazy things, but if you've ever been in the process, and I know the man to my left has been . . . he can tell you just as well as I can, nothing is done quickly in government. Nothing is done without hundreds of people having put eyes on those things. And so, they do go through legal review. They do go through policy reviews, and all of these things are brought together through the NSA's staff process, and so forth.

But the important thing is that — from a DOD perspective — we have to be ready to defend and to operate, so that we can do what we need to do for the country. And that is the reason why we're setting up this new cyber mission force that's aligned across the three primary missions of Cyber Command, the first being defending DOD's networks. And so, the point here is that if DOD can't do its job because its networks are infiltrated and are not functioning, then we're no good to anybody else. Actually, when you look at the bulk of the 6,000 personnel that we're putting into this mission force over the next few years, the 133 teams that we're setting up — the majority of those people will be doing this kind of work. What is that work? That work is assessing our networks. It's doing hunting on our networks to see if we can actively find adversaries on our own networks. It's doing remediation in real time. It's tracking what we can see in terms of the potential vulnerabilities in our networks. And we're doing that not because we're worried about the networks themselves but because we see the networks as just as critical to how the department does operations as any plane, ship, or operations center.

The second piece is providing support to our combatant commands. Every combatant commander–and we have nine of them currently–is tasked with certain missions, and they have to think now about what role cyberspace is going to play in their ability to achieve those missions. If my role is to defend against certain threats, I also have to think about what those threats might be if they come in cyberspace, but also what kind of effects I might want to bring to bear in cyberspace that can contribute to achieving strategic ends. What this is really about, right now, is just doing what combatant commands do, which is plan, and that's something that the Department of Defense always does against a wide array of threats. That doesn't mean that we want them to happen. It doesn't mean that we expect them necessarily to happen, but they are of such consequence or potential consequence to us and our allies that it bears being forward leading and forward thinking and thinking through what those things would be.

Finally, the third piece of this–and although it's one of the smaller pieces of the mission force, it's probably the one that's gotten the most attention–is talking about defending the nation against strategic attacks in cyberspace. That's thinking about what potential adversaries may be out there who would target us through cyberspace to do significant damage against us, against critical infrastructure — those kinds of things. And I'll talk a little bit about some of the considerations regarding that in a little bit. But I think it's important to realize that this is something that . . . again, it's about a defensive measure, but really the Department of Defense's role in this is to be very much adversary focused.

We're not here to sit on government, on private sector networks. We're not going to be sending out DOD teams to work at PEPCO or whatever your local power company is or sitting in Goldman Sachs' financial center or something like that. That's not DOD's job. Our job is to understand what the adversary may be doing, or the potential adversary, and to be postured to respond and, if necessary, preempt any kind of attack that may be coming our way. So, those are the main lines of operation that we're pursuing in the department. It's just underway in terms of standing up this mission force.

We will have the mission force fully stood up in 2016. There'll be ongoing training and so forth that has to happen, and that's not even considering the broad array of people who are doing the normal day-to-day operations of our networks. So, those teams . . . those people . . . the 6,000 I talked about are really one layer that we have in the department. And then you have your sys admins, your IT departments and all that. They're still going to be doing their work, but this is really about becoming much more aggressive in how we deal with the problem from our perspective.

The other piece is the support that we provide to other departments and agencies, particularly the Department of Homeland Security. That is the lead federal agency for implementation of presidential guidance when it comes to protection of critical infrastructure. And that role is really: How can we provide support where it makes the most sense, as well as working with our own sector, the defense industrial base, and how do we shore up their defenses and provide threat intelligence that we need? How can we provide a way for them to share information amongst themselves?

We have programs to do that, to share analysis that we may have done, both at the classified and the unclassified level as well as in putting our money where our mouth is and implementing things that we're also asking the private sector to look at, such as the NIST cybersecurity framework. So, the Department of Defense is adopting that framework; we're going to implement that framework. And we're going to move forward and try to work as much as we can to help improve the framework because, even as the folks at NIST will tell you, it was the first shot and they're going to keep going back and thinking about how it can be improved. And certainly we're open to those efforts as well.

Finally, we definitely want to partner with industry and not just our traditional partners — your Lockheed Martins, your General Dynamics, your Boeings — but also those people who are doing innovative work, including the technology side of things, so new ways of doing non-signature based network intrusion detection or doing work on how you assess certain risk, people who are thinking about different operational models. And that's something where the Department of Defense — I'll be honest — has not been the best at reaching out to non-traditional partners, but it's something that we're actively working on. In fact, I'm going to be accompanying the DOD chief information officer to Silicon Valley in a couple of weeks as we do more outreach to the private sector, to everyone from the largest companies to the small garage folks who are getting started with just $100,000 in investing, and we're trying to think about how we can onboard those technologies or processes in a better way.

I can't guarantee you success in the near term, given how large and bureaucratic the Department of Defense is, but it's certainly something that we're focused on. Another piece, of course, is the partnerships that we have with our allies and partners overseas, whom I could not forget — certainly not since Victoria [Woodbine]'s here--and thank you for being here--but because it is an important part of what we do and how we think about conducting operations and so forth in the future.

Given the large footprint that the United States has overseas and certainly from a Department of Defense perspective, we have to be working with our partners in all the regions where we exist to make sure that the infrastructure we rely on and they rely on is protected to best effect, but also that in those cases, particularly with our closest allies, that we're able to operate together in a combined fashion and understand how each other works. We each have different systems of operation, different legal implications, different policy considerations, but the more we can do in advance to really understand and exercise together and come together and work on these concepts, the better off we'll be when we come to the point where we may have to operate in cyberspace together.

The final thing, I guess, is that you have to talk about Edward Snowden at some point in these proceedings. It's no doubt that the revelations, the things that he has released to the public, have had a significant impact on the United States in terms of our diplomatic relations, also to a certain extent our operational relations. And, no doubt, there probably has been some impact in terms of the private sector, where you read about [how] companies are now no longer asked to bid on contracts overseas because they are seen as American companies who are in cahoots with the NSA and so forth. This is a process where we will have to work through and rebuild some of those relations as we move along.

As you know, the president issued new guidance on signals intelligence back in January. Some guy named Dick Clarke was involved in doing some good work to think about how we address very real needs that the United States government has to collect

intelligence but also to consider privacy, to consider what impact it has when we're thinking about particular targets of those intelligence nets. And that's something that, I think, although it didn't happen the way that we would have wanted it to, certainly has opened up the conversation in a way that is healthy to a certain extent.

That's something that we're endeavoring to work on very closely with our partners at NSA as well as elsewhere — to make sure that as we go through and think about the kinds of programs we have in the intelligence community, that they're serving the U.S. national interest, but in the broader context: not just, "Can we collect it?" but "Is it smart to collect it and is it something that actually feeds into protecting American citizens as well as our allies and partners?"

A lot of the time — and I'll just close with this — a lot of the time, when we talk about cyberspace, there's lots of doom and gloom. I just want to get back to the piece about critical infrastructure. You know, you'll hear people talk about the zero-day exploits, gray and black markets and how people are constantly scanning critical infrastructure. I think it's a very important thing that we need to track, but I think it's also very important to understand, from at least the Department of Defense perspective: systemic failure of these kinds of systems is not an easy thing to do. And so we have to really be very cautious about how we think about these kinds of threats. There are certainly threats to a power substation, for instance, that can come through cyberspace, but does that mean the entire system will go down? Probably not. In fact, given where I live–my local company is PEPCO, one of the most hated companies in America — and one thing they've gotten very good at is not having a functioning system that they are able to get back up and running again, and we manage to live through that.

On the other hand, if somebody was to target, for instance, the power generation side of things, not the distribution side of things, GE, for instance, does not have large-scale gas turbines just sitting on a shelf. It doesn't make sense for them to do that. That's the case where, if somebody could use a cyber attack to disable a large swath of those kinds of machines, to kind of go "stucksnet" on them, to coin a phrase, that could have a significant impact to the United States. But we have to understand that that's something that for the most part, is only within the reach of very few nation-states, and we think that's still the case.

There may be some very talented individuals out there, but understanding the complexity of these systems and that there are redundancies in these systems, we should note a word of caution: we have to be prepared to address these threats, but we shouldn't be slaves to the doom and gloom all the time and should understand what's real and what's not real when it comes to these risks. So, with that, I'll conclude my remarks and thank you.

LOCH K. JOHNSON: Quentin, thank you so much for getting us off to a great start. Now let me turn to our next speaker, Jamil Jaffer.

JAMIL N. JAFFER: Thank you Dr. Johnson. Well, I'll actually pick up right where Quentin left off, and I think this is the important thing to talk about when you're talking about the national security threat that faces our nation in cyberspace. And that is a sort of notion of a Pearl Harbor-style attack and these day-to-day cybersecurity risks that our nation, both the government and the private sector, faces. And a lot of people spend a lot of time talking about the Pearl Harbor scenario — what happens when the power grid goes down, what happens when the banking system goes down.

As Quentin points out, that's a possibility, but it's one that we focus on to our detriment. And it's one that we have to account for, one we have to prepare for and be ready to deal with. But there's a larger problem going on day-to-day, a nation-state-driven problem that is much more present and much more threatening to our economic viability. And that is the constant day-in and day-out, walking out the back door of every major U.S. company of core intellectual property. And so, we know today . . . it has now been sort of publicly discussed: the very fact that there are major nation-states, including China, that are targeting not only the U.S. government. That's sort of standard that we expect that we, like a nation-state, go to collect intelligence from our opponents around the world, and they collect intelligence on us. That's an understood sort of concept, whether it's surveillance . . . putting aside all the controversy that Edward Snowden has created with his disclosures, other nation-states know that we collect intelligence on them, and they collect intelligence on us — that's just part of the game.

What's different today though in cyberspace is the fact that at least one nation that's been publicly discussed and others that haven't been — China in the case of the one that has been publicly discussed — is not only targeting the government for collection, but it is, at a corporate national level, targeting American private sector corporations, stealing our core intellectual property — the very thing that drives the American economy and makes us the most innovative, most diverse, most successful economy in the world today — and taking it and transferring it to Chinese corporations in the private sector, both the public and private space. In China that distinction is blended, where the government provides a tremendous amount of support to their industry, both in the form of stolen IP and in the form of low-interest or no-interest loans to help them fund these efforts.

And so, what we see is a very odd situation where a nation-state is engaged in an effort to take private sector intellectual property, convert it to both public and private use there, thereby undermining our ability to compete in the global marketplace. And what makes it a particularly hard challenge is: What is the U.S. government going to do about it? How does the U.S. government respond to that threat? For years we knew this was a fact and had a hard time to even talk about it publicly because the way we knew was through intelligence accesses and the like.

Dare I say, by the way, that all of my remarks are my own thoughts and not those of my current or former bosses, so I don't get any of them in any trouble, and I don't get myself fired. But we've known this for a long time. We've known about this threat that both China and other nation-states pose to the U.S. private sector as well as the U.S.

government, but it's been hard for us to talk about it. And we've finally now realized 1) the threat is such that we need to talk about it and 2) the government can't do the protection of the private sector itself.

The vast majority of the Internet and the connected networks out there are owned and operated by the private sector. The U.S. government simply has no insight into those networks. No matter what you hear about the U.S. government's capabilities in signals intelligence and in cyberspace, the reality is that we can't, nor do we want to be, nor do our laws permit us to, be on every network at all times to know what's going on. It's not something that the American people want. It's not something the government wants to do, nor is it something we have the capability to do. Hence, the question becomes: How can the government work with the private sector to enable the private sector to better defend itself? And how do private sector companies work with each other internally to defend themselves from this very threat?

A lot of people think that one of the best ways to achieve that goal is to have the government intervene in the market and say, "Look — the private sector is not doing what it needs to do to protect itself. We need to tell them how to do it, right? Here are some regulations. Here are some laws. Here's how you need to accommodate yourself to this new reality of nation-states threatening you and your core intellectual property and your systems, either to avoid a Pearl Harbor-style attack or to avoid this walking out the back door of your intellectual property." That, I think, is the discussion that was had over the last couple of years, and it has faded into the background in large part because industry has shown a huge resistance to having government-imposed regulations and laws and for good reason. Industry and the U.S. private sector are very innovative and oftentimes the government regulation in places where there is not a market failure can stifle innovation rather than embolden it.

The question becomes: How do you determine whether there's a market failure here, or not, in this industry? There can be no doubt that industry could, and perhaps should, be better protected against cyber threats, particularly in the nation-state space. But the question is: Why is it not? And I would posit that the reason that industry is not as well positioned today to defend itself is because industry fundamentally doesn't understand the threat it faces. It's only recently, in the last year or two, that we've begun, as a government, talking about the very real threat that industry faces from nation-states which have very high-end capabilities and both the capability and the desire to go into these companies. So, it's only recently that companies have begun coming around to the realization that the IP is walking out the back door, and there is potential for a Pearl Harbor or lesser attack on their networks.

And even today I think everyone would admit — whether you're in industry or the government — that the government doesn't tell industry enough about what it knows. So, the government knows a lot about the zero-days that might come up against them. They know a lot about what the threat looks like. And they have a very hard time talking about it to companies, either at an unclassified or even at a highly-classified level. It's only when things get to a really hot boil that the government will be willing

to part with its deepest, darkest sort of most sensitive intelligence collection and even then it will only tell industries absolutely what they need to know in order to deal with that immediate threat. And that's something that fundamentally has to change. And I think the government's on its way there. I think that General [Keith B.] Alexander has made changes while he was at NSA, and I'm hoping that Admiral [Michael] Rogers will continue those changes, too, to think through how best to work with industry. But it's not simply government working with industry, because it will be a great thing if we can get to a place where we can pass some sort of information-sharing legislation that allows the government to share with industry what it knows is a threat.

But the reality is that today — without the government having a sense for what industry is seeing on the 98 percent, or 95 or 96 percent, of networks that it owns and operates — it's hard for the government to know where to focus its collection activities. For instance, today we know about the Chinese cyber actors coming up against our networks. So, it's easy for us to target that person and try to go after his system and figure out what he or she is doing. We know for a fact that sitting right next to that person, very likely, is another hacker — government-funded — going after the U.S. private sector, but we don't see that person, because we're not on the private sector networks looking for that. Until industry has the ability and the desire and the willingness to share with the government what they're seeing, it's hard for the government to turn around and say, "We're going to go try to target that person to see if we can figure out what they're doing, too, in order to provide back to industry the best capabilities the U.S. government has at its disposal." And so, that's one thing . . . it's sort of freeing up that information sharing gap between public and private and creating that trust between the government and private sector to share that kind of information.

But, second, and perhaps even more important, is the lack of trust within the private sector — the inability of private industry actors to communicate with one another the threats they're seeing. And there are a lot of reasons for that. There are regulatory reasons, there are competitive reasons, and there's just an inherent sense of, "It's hard for me to tell the guy next door what I'm doing." Now, the truth is that at the systems administrator level this happens all the time. Systems administrators of major corporations all the time will call each other up and say, "Hey, I'm seeing this on my network. Are you seeing it?" And the reason that relationship works is because they trust each other. They know that the other sys admin is not going to, you know, screw them over competitively. They do worry at the corporate level, however. If general counsel were to know about this kind of conversation going on, they'd probably be tamping it down and saying, "Look, you can't be talking to, you know, the sys admin over at our competitor because who knows if he tells his CEO what's going to happen to us competitively."

So, the question becomes: How do you create trust within the private sector to ensure that this sharing happens? And I would posit in that space the way to do this is to think about a model in which the private sector does it for itself, where a set of entities, cybersecurity consulting practices or companies, grow up that have a profit motive

driven to sharing information. These private-sector, profit-driven companies actually build the very trust that's necessary to share their information. So, I think there are opportunities here.

The financial services industry has realized that it is at the core of its need to survive to share this information. So, they're doing a good job. The rest of the community could do better. I think we're on the verge of seeing these models evolve to where the private sector will get better at sharing internally. I think that eventually, over time, we'll see the government get to a place where it is more comfortable sharing highly-classified intelligence with private sector entities who can help provide protection to the private space, and industry will realize that using the government's capability to collect intelligence will benefit them because then the government can pass back to them better or more refined intelligence about the people going up against them.

And so, I'm hopeful; I think we're at a moment where the large regulatory notion is starting to fade into the background. We're talking about these now voluntary frameworks, like the NIST framework, the good work that the FCC is looking at doing. As regulation starts to fade away as a big bugaboo, I think there's an opportunity here to build trust both between the government and industry and within industry. And so, I'm hopeful, but I guess we'll see what happens.

LOCH K. JOHNSON: Thank you very much. As I thought about what he was saying, it made me think about some work I've been doing on counterintelligence, and I find that the intelligence community has not been very good at sharing information with industry across the board, not only in cyberspace but against human attacks and other problems. So, it's an important area. Let me turn to Clete next, if I may.

CLETE D. JOHNSON: Let me start by thanking everybody for being here and thanking my dad and former mentors and professors for organizing this. It's a fun homecoming. It's the first official event–unless you count a Georgia football game as an official event–that I've been to at the law school since I graduated ten years ago, and it's great to be with so many people that have been fighting in the trenches together on these cybersecurity issues over the past several years.

So, to pick up on what Quentin [Hodgson] and Jamil [Jaffer] discussed, I'd like to briefly place this threat and how we deal with it in the context of the broad context of the past five hundred years of strategic security. We're in an academic setting, so we can get a little bit wonky about this challenge, and then narrow in on how we might address the need to create a truly new paradigm of necessary public-private collaboration and, as Jamil said, a growing consensus about what needs to be done.

This consensus is still growing, but even as of now, it's a deep and broad consensus about how we as a society — not how we as a government, but how we as a society, public and private, from citizen up to the highest levels of government address this challenge. Because, in many ways, it is different from other security challenges we

have faced in the past. With that backdrop, I'll telescope back about five hundred years to the beginning of our changing strategic security environment that has for previous centuries been built on territorial integrity and sovereignty and government control and security within borders.

The Peace of Westphalia — all these friends and colleagues have heard me say this a million times, have rolled their eyes, but we're at an academic conference now, so we can really get into all that context. The Peace of Westphalia in 1648 ended the Thirty Years' War, and for the first time it established a legal and political concept of territorial integrity and sovereignty. And what that meant in practice vis-à-vis security considerations is that governments were sovereign over the territory of their defined borders and the government–security services, armies, and in some cases navies, and other security services–would protect their citizenry within those defined borders.

Fast forwarding to 9/11, after the Cold War ended and a number of states started to disintegrate, transnational threats started to develop or accelerate. We encountered a new principle of security that didn't fit neatly into this Westphalian context. We had transnational, non-state actors, who were a band of individuals that were not affiliated with any state and infiltrated our defenses, such as they were at that time, and posed a real threat to us as a nation-state. There had been terrorism for, you know, hundreds, if not thousands, of years, but this was the first time that a band of individuals not representing any state had posed a real threat to a global superpower. And I think that was an introduction to really a new era.

Still, even in that terrorism setting, the response required a government-centric defense. Counterterrorism is always going to be a government-centric defense because it's going to rely on government intelligence, government law enforcement and then, in some cases, government military action. The cyber threats that we face take that non-state or not necessarily state-based threat one step further past the Westphalian construct. Even though nation-states are largely at the heart of a number of the problems, as Jamil [Jaffer] noted, cyber threats take that one step further because the people who are attacking in cyberspace don't have to be physically within our borders.

Cyberspace is largely a borderless domain. I say "largely" because you can quibble with that legally, and there are some attempts to balkanize the Internet but, broadly speaking, the Internet is a virtual global commons without borders or even geographical distance. Somebody sitting in Eastern Europe can reach out to us here in Athens without physically moving. He can, for instance, reach out to the refrigeration vendor of Target and get into Target's network via that refrigeration vendor in Pennsylvania without moving from his keyboard in Eastern Europe. And so it largely renders borders altogether irrelevant.

The other component of it is that these cyber threats to our country come directly to the company or citizen or, in some cases, the government entity that's being attacked. This is fundamentally different from the past. Previously, if a nation-state was under a threat, the attackers had to basically get through our army to do harm to our society.

And, in a lot of ways, the security services acted as a proxy for our country to fight our enemies. Now the country is directly exposed, via the Internet, to the bad actors, wherever they are in the world.

And so, the question is: What do we do about that? Because, as Jamil said, this is not a threat that can be addressed by government action alone. Even if we wanted to — which we don't–and even if it were legally permissible — which it isn't--the government cannot put its arms around our country in a Westphalian border-centric protective stance and defend the country from its cyber enemies. It's just not possible and won't happen. And even if we tried to do that, it wouldn't work. The Internet and networks are too big and diffuse. It's just not a possibility.

And likewise companies can't defend themselves alone. In a similar way that a company can't defend itself from an intercontinental ballistic missile, neither can it defend itself alone from a rising superpower putting the heft of its nation-state and its entire government structure and economy behind trying to steal an R&D development or IP from that company's servers. So, it requires a new paradigm of private sector-driven, public-private collaboration. And that's the new paradigm that we've all been working on in various ways over the years, and I'll talk a little bit more at lunch about how this applies legally in the FCC setting.

Now I'm going to pivot to a focus on the last five years of policy discourse because now we have arrived at that consensus, finally, after lots of fighting and arguing, including among ourselves, about the best way to do this. There is now a general consensus that it has to be this private sector-driven, public-private collaboration. And I'll just briefly walk through how we got there, because we were not there when Jake [Jacob Olcott] was a new staffer on the House Homeland Security Committee in — what? — 2005, 2006? Jake was probably one of about a handful of people in the government outside NSA who had ever thought about cybersecurity outside of the NSA with regard to cyber policy, and we've come a long way from there since then. I'll talk about this from the Senate perspective. Jamil [Jaffer] was modest; he was personally involved in an extraordinarily important legislative effort in the House that actually passed a bipartisan bill that would allow more information sharing.

But just to walk through how things developed in the Senate, — because I think the Senate debate was really a crucible for the development of this consensus for public-private collaboration--back in 2006, 2007, again, very few people in the policy community had thought through what to do about cybersecurity. And at that time my former boss, Jay Rockefeller [John D. Rockefeller IV], who was the vice chair and then in 2007 the chairman of the Senate Intelligence Committee, got a briefing from the Director of National Intelligence, Mike McConnell, who at that time was George Bush's DNI and had a very close relationship with Rockefeller. So, Rockefeller would tell you he is not a technical expert on how precisely digital communications threaten our national security, but he does know when somebody who knows what they're talking about is speaking the truth. And I think a number of these senators got a briefing from DNI McConnell back in the 2006/'07 timeframe that I think, frankly,

scared the living daylights out of them about what could happen to our country, and as Jamil said, what is happening to our country today on a day-to-day slow bleed basis.

And so, he determined that he wanted to do something about it. In 2008, he began the transition from serving as chairman of the Intelligence Committee to chairman of the Commerce Committee, which are both very important committees dealing with cybersecurity. On the Intelligence Committee, Rockefeller had overseen the beginning of the implementation of the first major policy effort on cybersecurity that was initiated by President George W. Bush. And that was called CNCI — the Comprehensive National Cybersecurity Initiative. It had a whole host of provisions, but its thrust was–and it was important to start here–its thrust was a defense and intelligence-oriented approach to how we grapple with this problem.

And Rockefeller wanted to take that one step further and, particularly as he moved into the Commerce Committee leadership, to make this more of a private sector-oriented, private sector-driven process. And so, when he was transitioning around Thanksgiving, Christmastime, January of late 2008, early '09, he pulled together a couple of his staff, including myself, his Commerce Committee staff director Ellen Doneski, and his top Intelligence Committee cyber staffer, a guy named Sameer Bhalotra, who later went over to the White House and helped shepherd this process from the National Security Council. Rockefeller pulled us together and basically said, "Put together a draft bill. I want to do something that is big and meaningful, and I want it to be intelligence-based, but most importantly, I want it to deal with the issues that companies that we oversee and drive in the Commerce Committee, telecommunication companies in particular but also tech and Internet companies, are concerned with. I want this to be very meaningful."

So, we picked up a timely report that had just been put out, and we sat with a blank sheet of paper in a lonely compartmented facility in the Senate Intelligence Committee offices. This was a report that Jake had helped author. In December 2008, the Center for Strategic and International Studies had put together a bipartisan report with Jake's boss, Representative Jim Langevin. He and a conservative Republican from Texas, Mike McCaul, had put together a series of recommendations for the 44th president — whether that would be John McCain or Barack Obama — about what the next president should do with regard to cybersecurity policy. So, we picked up that report and started taking notes, put down a whole host of ideas. A few months later the Rockefeller-Snowe Cybersecurity Act of 2009 was introduced. Senator Olympia Snowe was the Republican from Maine who, like Rockefeller, was a member of both the Intelligence and Commerce Committees.

We put forth that bill and quickly realized that we had a lot of good ideas in there and also a lot of ideas that, shall we say, needed refining, as Adam Golodner pointed out to me on a number of occasions. We spent the next year working out the kinks on that and perfecting language and a year later, in early 2010, we reported a bill out of the Commerce Committee unanimously. That bill had two basic pillars. It had a whole host of things about research and development and education and a lot of other

important things that aren't controversial, but it had two crucial pillars. First was an information-sharing piece along the lines of what Jamil talked about earlier that would increase cyber information sharing between and among private sector and government entities. And second, and this was the most difficult piece, it included a market-driven standards and best practices development process that would be facilitated by the Department of Commerce's National Institute of Standards and Technology (NIST).

Some of you may have heard of the Cybersecurity Framework that NIST rolled out in February of this year, and there's a direct line between that original Rockefeller-Snowe legislation and the NIST framework that's now a reality. NIST is a somewhat unknown, but very dynamic, group of scientists, including Nobel laureates, and it is the world standard of metrology and standards. How do you measure things? How do you create standards that can be measured against? That's what NIST does. And the Rockefeller-Snowe bill would give NIST the responsibility to facilitate this private sector-driven process on cybersecurity standards. The bill went out of the Commerce Committee unanimously.

That same year Senators Joe Lieberman and Susan Collins, who were the chair and ranking member of the Senate Homeland Security Committee, put out a bill from their committee that was very Department of Homeland Security-centric and very prescriptive, regulatory-centric. And they also got that bill out of their committee. Then a few months later, in early 2011 . . . I mentioned Sameer Bhalotra, our Intelligence Committee colleague, whom we've all worked with very closely . . . by that time, Sameer had left the Intelligence Committee and was the senior director, the first senior director, for cybersecurity at the White House on the National Security Council. He shepherded this big interagency effort, borrowing from the Rockefeller-Snowe principles of a private sector-driven standards process, putting that into the Lieberman-Collins structure of a DHS-oriented structure, and then the administration put out its own legislative proposal.

For the next year, we tried to merge all of these things together. By this time, Jake had come from House Homeland Security to Senator Rockefeller's staff, and Jake was Rockefeller's lead counsel on these issues sitting in the Commerce Committee, and we spent a lot of awful late nights and weekends trying to merge these two bills together. And they were not a good match, because Rockefeller-Snowe was inherently private sector-driven, and Lieberman-Collins was inherently sort of regulatory and DHS-oriented.

But to make a very long story somewhat shorter, we finally came to something that we thought was at least a start. On the Rockefeller-Snowe side, we knew that this merged bill needed to be improved to come back closer to that private sector-driven process. And we took it to the Senate floor in the summer of 2012, which was probably, to get back to world history, the worst time in world history to try to pass a bill that looked a little bit like a regulatory bill. This is after the Tea Party had arisen; we were in the middle of presidential politics; and we heard a lot about: "This is an election year. You can't do anything important in an election year." I would

try to remind people that the Civil Rights Act was passed in an election year, 1964, welfare reform in 1996, normalized trade relations with China in 2000, overhauling the Intelligence Community in 2004, and the FISA Amendments Act in 2008, all those were presidential election years, controversial issues that became law. But it was not to be in this election year. And–we were all talking about this last night--I think it's largely because neither the government nor the private sector really knew how to speak this new language of: How do we create this new paradigm of private sector-driven, public-private collaboration?

And so, I would say, in a biased fashion, the Rockefeller-Snowe approach was trying to address the issue from this new paradigm perspective. A lot of the players in the private sector (not all–and I'll note Adam [Golodner] and CISCO took a very enlightened approach to this), but also lots of stakeholders in the government, could only kind of talk about these things in the old way. The private sector wanted to keep the government out and keep regulation away, and the government talked about it in terms of requirements and regulation.

And so, in the midst of that election year, we never could get to this sweet spot that we're in now, even though we tried and tried and tried, and I won't go into the details of all of the compromises that were right there in front of us, if only more of the players had been willing to say, "Yes, let's try to get there. Let's find a workable compromise." It was an election year, and it bogged down. But the good thing is that it moved the discourse to where we are now, and soon after the bill in the Senate was filibustered, the president issued an executive order that basically encapsulated the principles that we were trying to get to legislatively. It started to do more information sharing, and it created this process of a NIST-facilitated private sector-driven standards process. And that's where we are now. It's a new consensus and that's what I think the government and the private sector alike are seeking to implement.

LOCH K. JOHNSON: Clete, thank you so much.

In this rather hostile, uncertain world that we live in, certainly some of our best friends are in the U.K., and I'd add to that New Zealand, Canada and Australia. So, we're very pleased to have a representative from that part of the world — Victoria.

VICTORIA WOODBINE: Thank you very much. I was just going to start with a little bit of history, and it's not anywhere near as sophisticated as Clete's reference to the Treaty of Westphalia. When I found out I was coming to the University of Georgia, my Google searching came up with the Georgia Bulldogs, and I hadn't realized that English bulldogs would have gone extinct had they not been a) exported to the U.S. or b) saved by a breeder called John Johnson. So, another Johnson. Thank you very much for the opportunity to offer a British perspective today and for saving the English bulldogs.

I'm going to talk a little bit about my role in the British Embassy in D.C. I'm focused purely on cyber policy, and I think that's really indicative of how important the

U.K. considers the U.S. as a partner and also how much is going on in the States on cyber policy. I work very closely with the Administration, mainly the White House, State Department, Department of Homeland Security, colleagues in Congress, and then the think tanks and academia. And my role is really about monitoring all the policy developments in the States and how that maps with the U.K., and how we can collaborate more and realign our assets a little bit more. Today I will just give a quick run-through of the key tenets of the U.K. cybersecurity strategy with a focus on public-private partnership.

Our efforts kicked off in 2010. We were given about a billion dollars' worth of funding in what was then a very fiscally restrained environment. Also that year, our national security strategy designated cyber as a tier one threat, alongside counterterrorism, military interventions, natural hazards and disasters. So, again indicative of how important cyber is in the U.K.

The first strategy was launched in 2011, and we took pains to look through both a security and economic lens and put in place a number of mechanisms to really drive a collaborative effort between government and the private sector. The four key objectives in our strategy: First it's about making the U.K. one of the safest places to do business, so improving awareness, risk management, corporate governance, tackling cyber crime. Second, making the U.K. more resilient to cyber attacks, so really enhancing our national capability to deter and defeat those high-end threats and improving our protection of our national infrastructure. Third is about our international work, so, all of the bilateral and multilateral relationships we have to help make sure that cyberspace is open, vibrant and stable. And underpinning all of that is the work on skills, capabilities and enhancing our knowledge, so ensuring we have a future pipeline of talent to really take forward these objectives.

A little bit more on that first objective: Our efforts are focused on ensuring cyber is integral to good business and ensuring that government interventions develop those right market structures for industry and the sector to drive itself. So, our approach is very liberal, market-based, and we're trying to avoid legislation. We think regulation is just too blunt an instrument to use at this time in this sector and this complex theater. We're more interested in putting in place mechanisms for the market to drive growth.

We've made progress on cyber exports. By promoting the U.K. as a more attractive place to do business, we're securing more IP-rich business based in U.K. headquarters. We're promoting exports, but with that very important crucial human rights element attached to it. We're also seizing on business opportunities, making cyber a facet of bigger infrastructure projects and really using the U.K.'s enhanced cybersecurity as a market differentiator. Similar to some of the other initiatives that have taken place in the U.S., we've done a lot of work on outreach to business and raising awareness. So, pretty much every U.K. company has cyber now as a key part of its corporate governance and board discussions.

But we're moving on to: How do CEOs, boards, customers, investors not only know about it but ask the right questions and put in place the right mitigation strategies? We have a lot of work going on with our top U.K. audit houses. Every single one of our FTSE350, e.g. Fortune 500 companies in the U.K., has undergone a complete cyber risk audit. That was really useful in both discussing cyber risk directly with the CEO and figuring out, per sector, best practice and vulnerabilities. The companies which took part in that initiative were provided with a confidential set of conclusions so they could assess themselves against their peers. And also, our Department of Business in the U.K. was provided with an aggregated and anonymised report to use as a basis to make the correct policy and government interventions, with full understanding of the private sector's best practice and vulnerabilities.

We've also had a Regulator Summit in the U.K. The regulators of all of our key critical infrastructure sectors came together with senior officials from our intelligence and government agencies. They publicly signed a communiqué which said that they would consider cybersecurity more seriously and look to do more information sharing — a real genuine public sign of commitment that our regulators in the U.K. would be prioritizing cyber as an issue.

We also realized that companies who do invest in cyber want to be able to make money from the investments they're making. So, similar to the NIST framework that Clete mentioned earlier, we're doing some work in the U.K. where we're coming up with a basic cyber hygiene standard. Companies can really demonstrate that they're taking cyber seriously by getting this badge of, "We've audited ourselves, and we know that we're up to that baseline standard of minimal controls and how to implement them." And on the law enforcement side, we're really taking pains to decrease levels of cyber crime in the U.K. We've tripled the number of police we have working on this, and we've got an entirely new cyber law enforcement unit to pursue convictions and disruption.

The second objective in our strategy is focused on resilience, defending our national infrastructure and ensuring that we have the capabilities that we need. A key piece of that is incident management. In the U.K., we hosted the Olympics in 2012, and that was a real example of government and industry working together in a time of heightened cyber threats where we successfully averted genuine attacks. And that was great for lessons learned, so we can now streamline and improve upon that for national cyber incident response.

GCHQ is our equivalent of NSA in the U.K. We've invested a lot of money in them and that's about better analyzing hostile attacks. An enhanced understanding of the threat will help us prioritize our defensive efforts, but also help industry keep pace with the growing volumes and the growing sophistication of threats in the U.K.

We have a cyber information-sharing partnership, so that's government and industry co-located together, conducting real-time threat information sharing. It's a little bit

different from the set-up in the U.S. where each sector has its own ISAC. In the U.K. we're all co-located and we've found that has really worked, and cross-sector pollination of the threat-sharing is an added benefit. And as part of that information sharing partnership, we also have fusion cells — intel agencies, and law enforcement– co-located to give an extra added overlay of information.

Our third objective is the international angle, again, very much focused on national security but at the same time economic security — protecting innovation, economic growth and also, in tandem, social benefits. So, everything we do in the U.K., all three of those, are conducted in parallel. We're doing a lot of work on promoting norms of behavior and what construes acceptable behavior in cyberspace. By having that dialogue, we hope that, should there be an escalation of conflict in cyberspace, there would be the mechanisms in place to have a mature conversation about how to de-escalate.

And Internet governance — another key piece of that international work, especially, at the moment, post-NSA revelations. There's a lot more of an international dialogue about government control of the Internet. We're absolutely opposed to that. It's all about the multi-stakeholder approach — industry, government, and civil society working together to manage the Internet.

The last objective: focusing on cyber skills, outreach awareness. We're quite conscious that a public awareness program is quite difficult. You want to reach as many people as you can. The last effort we had reached four million people, but it's hard to get the balance right. You want to elucidate the threats to the general public but equally you don't want to put them off. So, again it's about promoting that right balance of social benefits versus national security.

And then, in our education system, we've made numerous interventions. We've changed the curriculum in university courses and in school courses. We've put in place funding for a number of Ph.D.'s. We've got eleven Cyber Centers of Excellence now, but we're also conscious that those are long-term efforts. So, in the next few years, we're looking at apprenticeships into government, into private sector, into the intelligence agencies — things like professional certificates so we can minimize that gap and ensure that we've got the knowledge and the capability we need to really boost that pipeline of future talent.

I think, in conclusion, the crucial aspect of this is partnerships. The partnership with industry, partnership with government, partnership with academia but also that international angle as well. Again, I would just like to thank my U.S. colleagues for all the support and the strength of the U.K.-U.S. relationship in general.

LOCH K. JOHNSON: I want to make sure that we have about fifteen minutes, so we can have interaction with the audience, but let's take about five minutes to see if any of the panelists would like to add anything quickly or ask questions of one another. So, the floor is open to this immediate group here.

BARRY HENSLEY: I have one specific question. You mentioned the Department of Defense's role was to actually do hunting engagements or friendly forces on the network for yourself. How about your supply chain, defense industrial base–so obviously critical to your technology growth–the compromises that happen there? Are you going to extend that friendly forces hunting engagement to that community as well?

QUENTIN E. HODGSON: Not directly. You know, that's something where there's certainly a lot of scope for the private sector to step forward on that and actually, when we think about hunting, for instance, it's a very exciting sounding term, but what it's really about is having people who know your network best actually look at it and see what it's doing and look through logs in as much as real time. And this is also partly why having us go out and do things on private sector networks really doesn't work: because we don't know your networks the way you know your networks. So, it's really about getting the folks who know it best, who understand operationally what you're trying to accomplish, to be actively searching for those kinds of anomalies on the system and so forth.

Where we are working most closely, we have several programs. One of them is the Defense Industrial Based Cybersecurity Information Assurance Program, which has over a hundred partners as members. Now, just as scale, clear defense contractors are several thousand, so we're looking to ramp that up. But that hundred represents something on the order of 80 percent of our acquisition buy. So, it obviously has the largest ones.

But the supply chain is a significant issue that we're addressing from a lot of different areas. One is the threat piece of it–do we understand that? And in some cases, though, that's a difficult question because for a prime to even know who all is on that supply chain and how it changes over time–it's not something that stays constant–is a really important issue.

The other piece is also a lot of work we're doing with private sector partners on things like software assurance, and I'm not an expert in that field, but it's something where [we're] trying to understand: Where is your code coming from? What kind of testing and evaluation has it gone through? What kind of verification and compliance? Especially nowadays because the urge is sort of, you know, scrum and all this other stuff, where it's just "get the product in a faster and faster cycle," which invariably means that any kind of inherent vulnerability or exploitable code is just going to get buried as you keep metastasizing it through the system.

But there are ways to address that. There are some innovative companies who have found ways that you can actually do real-time evaluation of your code, particularly open source code, to make sure that you're tracking that. We have had some folks in Congress who've tried to be very "helpful" on this front. And, in some cases . . .you know, Clete talked about some not-so-fully-baked ideas, and we have seen some. And I'm not saying that the legislative branch is the only place where not-fully-baked

ideas come from, but we have seen some efforts to try to impose that sort of more Westphalian approach to things, which says, "If you know that this is coming from someplace, you can no longer do business with that country," or something like that. Well, you can't do that in this modern age, so I think we have to think about better ways to approach that.

LOCH K. JOHNSON: Mr. Olcott.

JACOB OLCOTT: I have a question. You know, sort of from the audience perspective, there's always an underlying question about the market and whether the market is actually broken or is working when it comes to cybersecurity. And this is often discussed in the context of, "Do we need additional regulation for companies to do better or do the right thing, or can the market be better incentivized to produce different reactions?" And I'm curious — from Jamil's and Clete's perspective — do you think the market is broken when it comes to cybersecurity or is it working the way that it should be? What's the government's role in realigning the market to the extent that it's broken?

LOCH K. JOHNSON: Let's hear from Jamil; then we'll go to Clete.

JAMIL N. JAFFER: Sure. You know, I think the market is not broken. I think that the market is functioning perfectly well, but the problem is that the market doesn't have full information today. And so, a market is going to only make its decisions based on the information inputs that it has today, and the fact is the government knows a lot about the threat facing industry, that it is, for whatever reason–whether for sources or method reasons or for bureaucratic reasons or other reasons–it's incapable or unwilling to share robustly with industry. And, as a result, there's an information gap that we know exists. There are things that you knew when you were in the government, Jake, and you and I, Clete (you being in the government now), know about the threat facing industry today at a strategic level that the government has simply not been able to translate well to industry. And, as a result, there's this gap.

So when the government gets frustrated and says, "Look, the private sector is not doing enough. They don't protect their systems well enough, as well as we think they ought to," I can tell you one reason why — it's very simple. They don't know what you know, and if you were to share with them what you know, perhaps the market might make different decisions.

I'm not going to say that is an end-all, be-all solution to the problem, but certainly one, I would say, where you've got to close that information gap to see what the market will do in response to information and then decide whether there is still a market failure that needs to be addressed. There may very well be a market failure . . . the government needs to step in . . . a tragedy of the commons or some other market, you know, incapability to deal with this fact. But the reality is that today we know there's been an information gap.

So, to step in with the regulatory or legal measures that impose a change in the market, I think, is unwise at a time when you know the market is incapable of functioning in the way that you would expect it to do, because it lacks information. And so, I think it's incumbent upon the government to figure out a way to undo this information sharing problem, at least at some level, before it steps in with the regulatory stick or the legal stick. And so, that's where I think, yes, the market functions, but only as well as it can with the information it has.

LOCH K. JOHNSON: Although I might note that sometimes it's the private sector that is frightened of the government and doesn't want to cooperate because they're fearful the government may intervene in some way. Clete?

CLETE D. JOHNSON: I will begin by agreeing 100 percent with Jamil, and I think that there is so much more information, of two kinds, that would be valuable to share. One type is tactical threat information–the digits, the signatures that the government is seeing in some of its collection or otherwise that are real-time threats. And the other type is the general trend information about, "Here's what we're seeing coming from this threat vector or this bad actor and here are some things you could do about it." This is where Jamil played a central role in trying to build a statutory approach to clarifying some of these issues that would allow for more sharing in that way. What I would add though is that I don't think it covers the problem to say that that's the only element of the lack of information or lack of situational awareness, because I think this lack of information is one part, but only one part, of a lack of risk management situational awareness among companies.

Now, a lot of companies in the tech sector, the financial sector, the telecommunications sector, no doubt, are playing at the A-plus level with regard to cybersecurity. But companies across the board, including big sophisticated companies like Target that have very sophisticated cybersecurity practices, are not fully managing the risk that the people in their IT departments and their chief security officers are aware of. In a lot of cases, we could add more threat information and more trend information, and that would certainly boost the company's capabilities, but alongside that threat and trend information gap there's a huge gap between the technical people who run the networks in a company and the C-suite boardroom folks who deal with enterprise risk management, corporate risk.

You know, the CEO will pay a lot more attention to what his CFO is saying about financial risk, or to what other elements of the company are saying about reputational risk or other operational risk — traditional business risk issues — than the CEO listens to what the CSO is saying about the threats to the company's network. They see that as something the IT department should fix, so "Let's pay more money to get the IT department to fix this cybersecurity issue." And that's just not the way it works.

It's really a fundamental risk management issue I think over the past couple of years. For a whole host of reasons, including more awareness of the threat, including this policy discourse we have been discussing, and including pro-active action by companies,

these issues have begun to trickle into the board room, and they are becoming a living and breathing part of how companies govern themselves. And so, I think the trajectory is unmistakably positive, but we've got a long way to go, and there are a lot of CEOs out there who have just realized in the past year or two that information security risks are fundamental enterprise risk issues that they need to manage as an executive.

LOCH K. JOHNSON: Thank you Clete. Why don't we open up the floor now to our distinguished visitors? And, Gary, let's start with you. Gary, would you mind telling us who you are?

AUDIENCE MEMBER: Gary Bertsch. I'm a retired faculty member, former founding director of the Center for International Trade and Security and now retired, working on some of these issues in a more private kind of way through a group called TradeSecure. Don — good conference and good panel participants. I'm concerned though that maybe we haven't talked this morning, at least not enough, about the global context in which U.S. behavior in cyber espionage, both government and private, is being played out.

This is a global issue, and the United States, in many parts of the world, is viewed as a big part of the problem. Recent revelations about NSA and other involvement . . . just two weeks ago, there were the articles in the press that talked, after years of accusing Huawei of penetrating U.S. cybersecurity, about the fact that NSA had been doing for years to Huawei exactly what we were accusing them of doing. And, I don't think that it's in our interest to overlook our role in all of this — the U.S. government role.

Often, we hear comments coming out of Congress and elsewhere in the U.S. government that appear very hypocritical and sanctimonious. I think we have to admit this. So, my question to the panel is: Is the U.S. government, and are the efforts that you're involved in, sensitive to what we're doing and how it's viewed by other countries, and how this is going to have to fit into global solutions?

LOCH K. JOHNSON: Not everyone at once.

VICTORIA WOODBINE: I'll interject a little bit with a slight international focus. So — absolutely — the U.S. government is completely cognizant of the current environment in which they're working post-surveillance. It was mentioned earlier that it has had an effect on diplomatic relations and on industry. I think the steps that the government has taken — the President's speeches, the bilateral engagement . . . there have been a lot of meetings behind closed doors, and there are nuances with the approach and with the way in which you deal with different countries and partners. I mean, China, for example: the State Department has a very sophisticated and mature cyber working group with Beijing. And there, within that, each side can bring to the table issues and concerns they have. So, this is being discussed. And, with a slight note of caution, the press reporting on it isn't always an accurate version of the messaging

coming out. I'm supportive of U.S. government efforts--the issue is being taken into hand and these broader perspectives are being addressed in the best way in which they can.

Similarly in the U.K., you know, we're in that same boat. And I think actually it ties into broader cyber issues in the fact that–maybe a slightly esoteric point–but the announcement two weeks ago about the Department of Commerce and the IANA functions within Internet governance. There's a big conference coming up in Brazil in three weeks' time which President Dilma Rousseff, following the revelations, called together the global community to talk about Internet governance, cyber issues, and surveillance. And the U.S. government has made a fairly big, bold concession in offering up functions of this contract to ICANN, who help run the Internet, and that is a true example of a multi-stakeholder governance which we support. My point is that there are a number of strands of work going on. It's not just all about what you see in the press.

LOCH K. JOHNSON: [unintelligible] Yes, then we'll come to you.

JACOB OLCOTT: I think the answer is "no," that the U.S. government does not do a very good job of evaluating equities when it comes to considering intelligence interests versus business interests. You know, right now, I think that the intelligence function has an oversized role in the U.S. government, and that our intelligence collection capabilities and policies are really overwhelming any of the business priorities that we have as a nation.

So, that's a really significant issue, and you see that play out in a lot of different ways. I mean, if you believe that NSA manipulated the encryption standards to benefit our intelligence capabilities, if you're on the business side of things, you're saying, "Why are we doing that? You know, that's not really helping us internationally." From an intelligence standpoint, you see very clearly why we're doing that. So, I think one of the challenges that our government faces today is that the intelligence community has a very strong . . . maybe a much stronger representation at the table than the business community does.

The other issue is that, when it comes to whether it's a Huawei issue or, as Vicky [Victoria Woodbine] was saying, another instance where there has been pubic reporting of a particular exploit, that information is often erroneously reported, or there's some nuance to it that is not really adequately reflected. So, for instance, the United States does not exploit other companies' networks to provide that same information to U.S. companies. We don't engage in economic espionage for the purposes of benefiting our own companies, whereas other countries do. Well, that's a really important distinction, but a lot of other countries don't really recognize that distinction. They see the U.S. as a monolith and that we're exploiting things just for the sake of exploiting things. And we often lose that distinction in talking about these things publicly, and it makes us look like everybody else, but I think there are a number of different problems.

LOCH K. JOHNSON: Okay, let's hear from Quentin briefly, and then we'll have time for one more question.

QUENTIN E. HODGSON: First of all, I wanted to thank Victoria. She's got a great second career as a White House spokesperson actually. So, I appreciate your intervention. I would say . . . obviously, I'm not going to comment on particular revelations and whether they're actually accurate or not. I think the comment about what you read in the newspapers versus what might actually be the truth is an important one to foot stomp, and that's not just an excuse. But having worked in this field, you recognize how disparate sometimes the public debate is versus what's actually going on. I think the other point that Jacob [Olcott] was just making is a very good one as well, which is that there are some important distinctions in terms of what kinds of activities we engage in.

The third one I would say is: because the United States is still the preeminent economic . . . certainly military power, we are held to very high standards. We hold ourselves to very high standards. There are a lot of countries, quite frankly, which engage in rhetoric and are completely lying to you about what they're really doing. We only do that occasionally. So, please don't quote me on that. But the point is that I think what this has reinforced is the need for us to hold ourselves to a much higher standard—not just to say that we are like any other country—that we do have certain founding beliefs that still endure that we need to hold true to. Otherwise, then I think we do lose ourselves.

And then, finally, there's just the factor of . . . I disagree a little bit. I think there is a lot of debate about what makes sense from an intelligence perspective versus what's good for American business, versus what's important from a diplomatic perspective versus what's important from an operational perspective. And just to illustrate the point: there are a lot of people within the Department of Defense who would love to go out and do things operationally that we do not let them do, because it makes perfect sense from an operational perspective but makes absolutely no sense from a strategic and policy perspective.

LOCH K. JOHNSON: On those rare occasions we mislead other people, we do keep our fingers crossed behind our backs.

AUDIENCE MEMBER: William Foster from Emory's Goizueta Business School. I've been looking at . . . starting in 1995 for OSD . . . looking at U.S.-China cyber relations. I think it's very clear that the U.S., China, and Russia are in a cyber war, and we need to be honest about it. I think, according to Mike Cognato, who was the State Department representative in Guangdong [Guangdong Province, China], that there was no evidence that any Guangdong company used intellectual property gained by the Internet in Guangdong. And so, in fact . . . I believe that we will be in a cyber war for the next fifteen to twenty years with Russia and China. I think we should move into deterrence, but as those of you who have studied deterrence . . . it's good to be clear and honest about [the fact] that we're actually in a deterrence relationship. We need to

admit the truth of our relationship with Russia and China, and I think that's the way forward to world peace.

LOCH K. JOHNSON: I'll take that as more as a statement than a question. Is there another question. Tyler?

AUDIENCE MEMBER: Thank you. I've really enjoyed the discussion so far. I'm actually a senior undergraduate student in SPIA. I had Dr. Johnson last year. This is sort of directed at Ms. Woodbine and the panel in general, but you mentioned the four-point policy that the U.K. is doing with relation to cybersecurity. What have you seen as far as the results of the policy you guys have implemented as far as how successful you've been in bridging the gap between the market and the government, as far as the sharing of information? And, in regard to the panel in general, it seems like a lot of the ideas that Ms. Woodbine mentioned could translate well in regard to solving a lot of the problems you guys have talked about and bridging that gap, the information gap. Do you see a cross-pollination between the U.K. and the U.S. in kind of sharing strategies in the future, or currently?

LOCH K. JOHNSON: Victoria?

VICTORIA WOODBINE: On our cyber information-sharing partnership I think we are a little bit more fortunate in the U.K. in that our legal framework makes it a touch easier, and we have a slightly less litigious environment in the U.K. And we're also a little bit smaller, so it's easier to build up these relationships of trust where, as Jamil [Jaffer] mentioned earlier, [you have] the kind of sys admin calling sys admin. Our cyber information sharing partnership is up to about 300 or 400 companies and all of our critical national infrastructure sectors are represented. So, I think they see real benefit in not only their unique protection, but it helps drive enhanced cybersecurity down the supply chain, and the companies know they're getting the benefit of broader collective situational awareness.

We're probably also a little bit more fortunate that GCHQ is non-military. So, the huge mass of cyber threat information comes from GCHQ and is shared around all of the U.K. government departments and U.K. companies. We don't have the same set-up with the role of DHS, the role of Justice, the role of DOD and how those different constructs work. So, being a little bit biased, I'd like to think we've been successful at that. What was the second half of your question? It was information sharing and . . . ?

AUDIENCE MEMBER: The second part of the question was more for the panel. You mentioned the cross-pollination in your own country, but it seems like a lot of the strategies . . . like, the U.S. bureaucratically and otherwise functions a lot differently than the U.K. I mean, how that [works with] maybe the implementation or kind of bridging of similar strategies into the U.S.

VICTORIA WOODBINE: I would say it's an overarching point, pretty much, the fundamental platform and baseline of what the U.K. and the U.S. do on cyber, and

the strategy and the objectives are pretty much completely aligned. There are just nuanced approaches about the way that our authorities and legalities work and the U.K. government's relationship with industry versus the U.S. government's relationship with industry, but that's the reason for my post in the embassy — bringing it together even more if I can.

ADAM GOLODNER: One thing I note is that this is a global issue. So, at the time that the U.S. and the U.K. are dealing with this issue, the European Commission is dealing with this issue for the European Union and actually has a piece of legislation, which is in the Parliament, which takes a very different view than the U.S. view. It takes a much more regulatory approach with regard to critical infrastructure sectors in all twenty-eight member states. India is making its way through a working group recommendation that will probably, at the end of the day, propose a pretty regulatory approach towards critical infrastructure in India. China has taken an approach with a multi-level protection scheme which is quite regulatory down to very small entities in China.

And so, I think one of the challenges that everyone has to work through is that, although we see the same sets of issues, threats of a global nature, we're really coming at these issue sets in very different ways that are reflective of our own political structures, our own sets of history, and our own values. And this is a real challenge.

VICTORIA WOODBINE: I was going to say we're lobbying against that regulation in the EU.

ADAM GOLODNER: But, as you know, there are many countries in the EU that are much more regulatory than the U.K., and are in a different place. And so, this is particularly complex. I do agree with the panel that we've sort of reached, through lots of blood on the floor, a consensus in the U.S. for going forward that is based on a voluntary approach. My own view is very much market-driven, innovation-driven and quite concerned about regulatory approaches, which I think will stifle innovation and, at the end of the day, make you less secure. And if you have that view, there is a real need to socialize the benefits of that view globally. So, this is a real global issue; right now not all countries are in the same place, but we need to rationalize this because it is a global network.

LOCH K. JOHNSON: Thank you, Adam. What a wonderful panel this has been. Thank you so much.

Cybersecurity and National Defense: Building a Public-Private Partnership

Panel 2 - The Private Sector Role in Addressing Cybersecurity Risks

Moderator: *Timothy L. Meyer*
Panelists: *Adam Golodner, Colonel (Ret.) Barry Hensley, Andrea M. Matwyshyn, Jacob Olcott*

TIMOTHY L. MEYER: Alright. Well, thank you all for being here. We are ready to start our second panel, which is entitled "The Private Sector Role in Addressing Cybersecurity Risks." We have a very distinguished panel here. I'm just going to briefly identify them, although you have their information in the program, and then we're going to get started. We're going to proceed in the order in which the panelists are listed in the program. To my left, we have Adam Golodner from Kaye Scholer—it's a correction to the program. We're then going to turn to Colonel Barry Hensley from Dell SecureWorks, then to Andrea Matwyshyn from the University of Pennsylvania, and then finally to Jacob Olcott from Good Harbor Security Risk Management. And, with that, we'll turn to Adam to start us off.

ADAM GOLODNER: Thanks Tim. I appreciate it and really appreciate the opportunity to be here at the Rusk Center. This is really a terrific day, a terrific bunch of panelists and audience participants. Thank you, and thank you to Ambassador Johnson for spearheading this. By the way, to the correction to the program: I have started at the Kaye Scholer law firm in the last three weeks. So, I'm so happy to be here at a school of law and for all of you who are in the School of Law or associated with the School of Law, you can do cyber law . . . such a thing exists. So, hopefully there are bright futures for all of you who are in law school and thinking about cyber and what your future might look like. These are really tough issue sets and over the next couple of years people will spend a fair amount of time helping to scope out the rules of the road.

I want to talk really about three things today, which I just find to be interesting. I think that they are topic sets which very well fit the kinds of issues that the Rusk Center might focus on. They are broad based, global issues that need a lot of thought and I believe are critically important to the future of the global interoperable network. So, here are three issues: Internet governance, where there is a very hot issue right now, and Victoria has talked a little about that already. Standards and the technical standards

of the Internet and why they're important, what's happening in standards now, and some work actually that Tim Meyer here at the Center is focused on, like the WTO. And the last is what people have been talking about — the rules of the road for cyber going forward. I think these three issues are fundamental, and things we just need to get right. So, let me just sketch them out a little bit. Maybe it's food for thought for you, and maybe some of the other panelists, all of whom could talk about these issues as well as I could. We'll get a discussion going with you and the participants in the audience.

This Internet governance issue is at an inflection point. The Internet is a network of networks around the world that, over time, has allowed a governance structure embodied in ICANN — that is fair to characterize as a multi-stakeholder framework. Which really means that the governance is not government owned and run, but other people have a voice — civil society, engineers and as well as government. But it is not government "run." This is quite different from the traditional "telephone" regulatory construct, where you had plain old telephone service which grew up in a regulated environment, both within nation-states and then on a global level through sets of rules that were put together by the International Telecommunications Union, or ITU, a subsidiary of the UN, a governmental regulatory body. In some sense, the Internet governance, through ICANN, is bottom-up, and the telephone system, through the ITU is top-down.

The global discussion now is: What's the future of Internet governance? Is it going to remain bottom-up or are governments going to step in and regulate it, top-down. Under the ITU, government model, where decisions are made in a multilateral government run context, all the traditional regulatory effects and incentives, like regulations arbitrage, and log-rolling, can and do occur. These are not the stuff of innovation, technical and economic efficiency. Under old style regulation countries can engage in cost shifting, cross-subsidization, and other sub-optimal economic and political activity that would have profound impacts on new technology and business models. The Internet, through nongovernmental governance, has avoided most of the effects of old-style regulation, and most commentators believe this has been critical to its growth and innovation.

The Internet, of course, grew up and became fundamentally important. And even before the Snowden revelations, we had the situation where some countries were saying, "Hmm . . . we're sovereign." We should "control" this Internet. And what is this ICANN thing? We don't understand what that is, but some countries said, "We should 'own' it, 'control' it, so we want to create our own rules."

The issue came to head at a ITU WSIS meeting in December 2012 in Doha. China, Russia, and a couple of other states said essentially,"We want to move control of the Internet into the ITU." And most of the Western world said, "Sorry, we want to keep an innovative, global interoperable (and we think better) method for securing the Internet in the context of the ICANN and an Internet-based model." A clash was born. At Doha, the world essentially split, with about eighty-five countries saying (this is an oversimplification): "Yes, we should have more control by governments

over the Internet through the ITU." And about fifty-five countries—most of the West and others — saying, "We disagree; we want to continue to drive innovation through ICANN and in a non-governmental way."

This open split created a little tremor through people that care about the Internet or what the future of the Internet looks like. And the issue isn't resolved. In fact it's red-hot. And it's going to continue in ITU meetings at the end of 2014 and then into the future. But, this isn't just a government issue. Everyone who cares about the Internet should care about this issue. In some sense the .com of today may not look like the .com of tomorrow, depending on how this turns out. Now, I have a very strong feeling this should stay in ICANN, this should be innovation-driven. This should be "best idea wins" on technical standards, and we shouldn't have governments imposing rules that are going to stifle innovation — my own view. To clarify the road forward, the U.S. the U.K., Europe and others have been talking about "doubling-down on the multi-stakeholder approach through ICANN–showing why the future of innovation-driven, interoperable, open and secure networks rests with the multi-stakeholder, non-governmental approach,

Security has been key in this debate and is also meaningful to the developing world. So, two weeks ago, as Victoria [Woodbine] noted, the U.S. government said: We're going to transition some aspects of Internet governance more deeply into the multi-stakeholder framework, into ICANN, and going to work with developing countries on building capacity so they understand that a move to the ITU would not necessarily meet their development and security goals. That process is underway, and at the end of the transition, there must be a clean path forward for assurance of the security of the network, through the governance of the Key Signing Key for root servers and other issues.

For people who care about the Internet this is a seminal issue for the future of the Internet and an interoperable and innovative network. I think it's the kind of issue that everyone here might think about. I think it's the kind of issue that the Rusk Center might put some cycles against because it's at an inflection point. The choice in some sense is binary–ICANN or the ITU. So, take that as you will. That was issue number one.

The second issue is more technical, about standards. The Internet has grown up through technical standards that were industry-led and voluntary, through bodies like the Internet Engineering Task Force (IETF) and IEEE, which are literally comprised of men and women discussing and debating the best ideas to build out the underlying standards of the Internet. This is how the Internet community built upon the Internet Protocol, IPv4, IPv6, Wi-Fi, and lots of other technical standards. And because interoperability is so important . . . to get a packet from one place in the world to a packet in the other place in the world 1) The piece-parts have to speak the same language, so that packets can 2) find the most efficient path; and 3) get there securely. The technical pieces of the Internet need to be able to speak the same underlying standards, and innovate on top of those base standards, in order to

communicate, whether it's voice, video or data. And in standards there is a corollary to what's happening in the ITU versus ICANN in the context of Internet governance. In standards, the issue is the continuation of global interoperable industry LED standards vs. domestic nation-state control specific standards. Many countries, under the guise of security, are promoting domestic (non-international) standards, which are leading to a Balkanization of the Internet.

If countries pull inward and force non-international, domestic standards, we won't have the global interoperable language of the Internet anymore. Take encryption, for example. If I talked French, and you only talked English, and we couldn't use hand signals, we couldn't really communicate. And with encryption, when you're sending encrypted messages, unless you can talk the same language, you can't talk at all. So, "Good Bank" in New York couldn't talk to the "Good Bank" office in Beijing if the fundamental language they were speaking were different. And so from a global commerce perspective, and from an interoperability perspective, this would be a non-trivial problem. A problem with current use cases.

Now, another intersection with the Rusk Center and the work that Tim has been doing is: How do you ensure global interoperability? And it turns out we do have some ways of policing this, and it's an economic tool. It turns out that under the World Trade Organization rules–and 160 countries or so have joined the World Trade Organization–there are Technical Barriers to Trade Agreement that say you must use international standards unless you have a very good reason not to, and just because you don't want to, or because you want to drive domestic production, are not good reasons. And there have been a series of discussions where domestic standards have been pushed back based on the concept that you should use these international standards under the WTO. Therefore, the WTO helps foster an interoperable global Internet, and enforcing the use of international, as opposed to nation-specific, standards is a key tool and principle in Internet law and policy today.

Now, what this means is that by having a way of dealing with this as an economic matter, we now have moved the discussion—some say a fight—over what the security of the Internet looks like to some of the international standards bodies. This creates the second part of this issue. If the discussion moves to the standards bodies, they matter. Now, just like in the ICANN-ITU tussle, some standard bodies are industry driven (IETF/IEEE) and some are government-run (ITU/ISO). The Internet has thrived under the IETF/IEEE model, but some parties pushing their technical security standards are also now looking to the government-run standards bodies as they think they can do better there. So another fight is on.

So, I'll note that as the second issue for the Rusk Center to think about: How do we preserve the fundamental nature of the Internet as innovation-driven, as interoperable, based on international standards, when international standards bodies are substantially different? And are we using the right tools to police that from a global perspective? That was issue two.

The third is what everyone, I think, has been talking about for a number of years: How do we define rules of road or the conduct that's acceptable by nation–states for cyber? And this one is really, really tough. In the discussion we had before about intellectual property, Jamil was talking about the very serious issue of intellectual property being stolen by nation-states or actors closely associated with nation-states that are used for commercial purposes. We need to find ways to come to agreements on fundamental issues like that. We haven't actually been able to get there on issues like whether commercial use of national-state stolen intellectual property is acceptable nation-state activity. The U.S. is clear that it is not acceptable. But not everyone seems to agree. There are some countries which are not as forward leaning as the U.S. would like them to be about laying down some of the basic rules of the road.

Other rules of the road which have been in the news recently are: How should countries treat the zero-days exploits, for example–their own use of zero-days, the collection of zero-days, where we also need, on the other side of the cyber discussion, to protect critical infrastructure and to protect systems by fixing all vulnerabilities? Can we think about rules of the road — thinking out two, three, five, ten, twenty years — that we can actually get to a place that we can assure that we're going to have an Internet which isn't taken apart in times of stress.

So, these rules of the road are really important . . . and the third issue I put on the plate for the Rusk Center. And these three issues: Internet governance; standards and the global methodologies for policing those standards; and these rules of the road, I think, are vitally important.

TIMOTHY L. MEYER: Thank you Adam. That was great. And we're going to be very busy here it sounds like. Colonel Hensley?

BARRY HENSLEY: [Remarks are off the record.]

TIMOTHY L. MEYER: Alright. Great. Thank you. Andrea — we'll turn to you now.

ANDREA M. MATWYSHYN: First, I'd like to thank the organizers for inviting me to speak here today, and it's a privilege to be with you all. I'm Andrea Matwyshyn. I teach at the University of Pennsylvania in the Wharton School, however, I am a law professor and a developmental psychologist. My perspective is going to be a little different — more of a bottom-up perspective on these issues — and probably better understood in the context of my own background. I started practicing law in 1999 as a corporate attorney, and I was representing multinationals and start-ups as they began to struggle with data security/information security issues. After that, I started my work as an academic, and I've been writing on these issues for over a decade. I've also been embedded in both the business community that is trying to address these challenges of corporate governance relating to information integrity and security, as well as the technology end of this: the information security research community and

informal hacker community in the U.S. And I should use this as a moment to disclaim: I'm also currently serving as the Federal Trade Commission's senior policy advisor on privacy and security, and anything that I say is not attributable to the Federal Trade Commission. These are my opinions as an academic, so please don't attribute anything I say to the FTC.

The look of this set of data security issues from the bottom up is sometimes slightly different from the top-down view that we've heard a bit about today, though certainly there are overlapping themes. The first point I'd like to share with you is to highlight a bifurcated shift that explains why information security policy presents challenges for both national defense and private sector innovation policy simultaneously. On the one hand, from a national defense perspective, we see the increased privatization of national information security defense, partially driven by practical realities of network management and the fact that much, though not all, of the elite talent in information security tends to lie in the private sector.

On the other hand, we also see an expansion of military targets to directly include private sector entities and citizens. So, the types of targets that are now potentially vulnerable to foreign attack directly include consumers–regular citizens within our borders — and that's arguably new. Particularly with the rise of non-state actors, groups of potential attackers don't necessarily map onto our traditional notions of the attackers usually contemplated as part of national security and corporate risk management planning. In particular, the lone individual attacker has greater access than ever before because of the interconnected nature of technology.

This dynamic means that we must evolve — and this is my second point — in the process by which we learn. Learning in information security needs to happen on three different levels: on the level of consumers, the levels of corporations, and on the level of governments. Consumers are now at a point where they need to be empowered to better guard themselves. For example, consumers' learning needs to be expanded to understand that the medical devices that they are implanting in their bodies may have code integrity problems and may be compromised by an attacker remotely through the Internet. That means that consumers, when they're choosing which medical device to implant in themselves, should be asking good questions about information security. They should be researching the histories of vulnerabilities and the security behavior of the companies that manufacture the products they are selecting. Certainly having government help with that information sharing process is a piece of this consumer learning challenge. There is a very basic consumer education piece that must happen for us to maintain a functioning, trusted, technology-driven society.

The next piece of evolving learning processes involves corporate learning. Some companies have been deeply engaged with high-level information security risk management since the '90s and some have been disclosing vulnerabilities that are material in their securities filings since the early 2000's. However, some others have not. So, there is a notable lack of homogeneity in corporate information security disclosure practices across various companies even in the same industry, and this

deficit is not sector specific. There's divergence, even within sectors, with some companies erroneously choosing not to disclose potentially material vulnerabilities. And that is part of the challenge here — that there are cases where companies receive vulnerability reports that they do not act on or disclose. This is an important part of the puzzle: when we are at the point where information risk can be gamed for the benefit of one party over another, we have yet another important element to consider in this panoply of moving pieces around information security.

The last piece of evolving learning relates to government. The traditional top-down approach of government is a piece of this, but it's important to also recognize the bottom-up forces at work here. Trying to dovetail both of those approaches is a challenge, because superior information security threat information does not necessarily always reside with the government.

In each of these three pieces of our society, we face challenges not only in information security learning, but also in applying that learning and trying to translate knowledge for the other members of the information security ecosystem. For example, I spend a lot of time embedded with the information security research community, a community that is formalized to different degrees in different parts. There's a movement to professionalize that industry — maybe somewhat modeled on what we as attorneys have or what doctors have built. They're still working through this, and it is a comparatively new industry that's trying to form and self-govern. In many cases, these security professionals feel left out of our policy conversation. They feel that their technical insights and their voices are not adequately filtering into the organs of government and into the conversations around broader questions at the intersection of technology and citizen safety. The translation of the way that these security professionals talk about information security issues to the way that policy people talk about these issues, and the way that other constituencies that are interested here, including C-Suite people, talk about these issues–that translation triangle is, from my perspective, one of the most formidable challenges that we face as policy people and scholars embedded in this community.

Viewing these questions as innovation policy questions requires multilateral cooperation from each piece of this puzzle and engaging with the reality that vulnerabilities come in two flavors that impact both government entities and companies on the one hand, as well as, obviously, the consumer base on the other. In the first instance, you have vulnerabilities that are widely known, that can be relatively easily remediated. That's our first step — to fix those known problems where the information about mitigation is already available, and it's simply about reaching for that information and creating process-based ways inside enterprises, inside our entities, to address them on an ongoing basis. Many entities lack these basic processes to address known vulnerabilities, and the vast majority of security problems arise from known vulnerabilities.

The second flavor of vulnerabilities is the truly new, unforeseen vulnerabilities and exploits: zero-day exploits which some smart person–whether that person is an individual or whether that person is working for government or working for some other

non-state actor–uncovers. How does that new threat best get processed by companies, by governments and what impact is there on consumers and citizens? So, those are two different challenges, and we still haven't fixed the low-hanging fruit problems of the known vulnerability piece. And so, from my perspective, this is a great place for us to work to coordinate our efforts around the known vulnerabilities.

Increasingly, from the bottom-up perspective, consumers are also becoming concerned with these questions. The Federal Trade Commission has had over fifty enforcement actions on data security questions. We're moving toward a world where there's going to be accountability not only through these mechanisms but through tort law and through civil liability. You have that private sector conversation that's going to also come into this broader question of information control and information security.

Software liability is likely to arise within the next few years as we see the Internet of Things and the technology-enabled ubiquity of products that can directly harm consumers in physical space with their code. As those types of harms start to become more prevalent, we're going to see litigation arise, and we're going to see the private sector fight out some of these issues. It won't necessarily even be consumer-focused litigation: companies are starting to engage in information security litigation against other companies because they perceive there to be cost transference happening. Some companies are acting as good actors and engaging in best information security practices in handling their risk, while some other companies may not be choosing to allocate adequate resources, time and energy to fighting those information security battles. Yet, data loss impacts both because they are business partners. This results in a private sector debate, sometimes in the form of litigation, over where that type of cost allocation and risk is appropriately allocated. You'll see more action in this space in the future.

These private sector dynamics play into this broader picture on the national level of the way that we think about these policy questions around information security. States have also been very active with state data breach notifications statutes — helping to get information into the market to allow the market to process information about management of risk and information integrity. We're at a very early stage of this field of information security, particularly as a legal discipline, and in crafting a policy nationally that dovetails all of these innovation policy concerns with the reality of the national security challenges that we're going to face in the next ten years. I'll conclude there and leave time for questions.

TIMOTHY L. MEYER: Alright. Thank you very much. Jacob?

JACOB OLCOTT: I think I might be able to just pick up on that and wrap us up here, too. One of the things I just want to touch on is that we're sort of thinking about the public-private relationship here, and the fact is: it is so complicated. We've been here for a couple of hours now. There are so many different nuances to these relationships. There are so many different relationships, period. One of the things that I want to do is just kind of make a statement that it is impossible to identify any sort of unifying

theory of public-private partnerships or relationships, in part because there are so many different types of relationships that the government has with the private sector. You know, there are times that the U.S. government wants to help the private sector. There are times when the U.S. government wants to punish the private sector. There are times when the U.S. government wants to incentivize the private sector.

And so, just kind of thinking about the different interactions that the government and private sector have with respect to cybersecurity, I think it's important to keep in mind and recognize that it's an evolving relationship and that there is no sort of current unifying theory out there. I was actually . . . if I can just say one quick thing . . . I have a sort of short list of things that I want to talk about. But something that Vicky [Woodbine] said kind of stuck with me. You know, we always talk about creating a trust relationship between the government and the private sector — you hear that a lot. In some ways, that's great, you want that; you want that when it comes to information sharing, for instance. You want to create a trusting relationship between the holders of security vulnerability information within the federal government and the recipients within the private sector.

On the other hand, you know, when it comes to contractual relationships that the government has with private actors, I don't know if we really want the same type of trust relationship. You know, from the government perspective, you want your contractors to be concerned about violating the terms of your contract, because if they're not, then they might not act appropriately in securing your stuff. So, I'm going to kind of dive into about a dozen sorts of different relationships that the government and the private sector have. But I just think it's kind of important to recognize that there's a lot of nuance to each of these things and that we don't necessarily want to just encourage trust here. We want to also create thoughts about liability, because that's an important driver for private sector behavior, too.

So, here's my short list: There are about twelve different relationships–I'm going to just kind of tick through each one of these, give you maybe a little vignette, and then we can get into our questions here–twelve different types of relationships regarding how the U.S. government and the private sector work together today. Again, this is evolving. There's direct information sharing. So the classic example there is the Department of Defense and the defense industrial base. A few years ago, the Department of Defense was very concerned about all of the intellectual property theft and the government secret theft that was occurring within defense industrial base companies. They created a relationship, a mechanism to directly share signatures with defense industrial base companies, sort of the top twenty or so, and that is sort of currently being expanded. So, for number one the government has this kind of direct information sharing exchange with the private sector.

Second thing: The government and the private sector sometimes work together on joint criminal investigations for law enforcement. In kind of a really interesting development, Microsoft has been working extensively with the Department of Justice to take down botnets. And this is something that Microsoft has really sort of initiated

on its own, and then they kind of eventually dragged in DOJ in this, but this is an example of a public-private partnership between law enforcement and one particular private sector company to combat the threat of botnets.

Another relationship that the government and private sector have: the government provides voluntary assessments for private sector companies that are interested in receiving them from the Department of Homeland Security, for instance. So if you're a critical infrastructure company today and you want the Department of Homeland Security to come in and do an assessment of your network, you can have them do that.

Another relationship out there is that the government sometimes funds the private sector to develop standards in particularly hard areas where the government doesn't have all the solutions. One example of that is that the Department of Defense is currently funding a group called the Open Group to develop supply-chain security standards. And the Open Group is comprised of private sector actors who sort of get together and assess the challenges when it comes to supply-chain risk management and propose standards eventually that the government will consider.

Number five: sometimes the government has actually recommended that companies use other private sector companies to respond to breaches. Has everybody heard of the company Mandiant? At least one person. This is a bit of an exaggeration but Mandiant is the company that it is today in large part because the FBI kept on recommending that companies use Mandiant to respond to incidents. The FBI was getting tired of going door-to-door to all these compromised companies out there and saying, "We've found all this, you know, all this evidence that, you know, malicious actors are inside your system. You need to do something about it."

Inevitably the company would say, "Okay, so what should I do about it?" The FBI, not wanting to kind of walk with them over and over and over again about "Well, this is what you need to do," said, "We think you should just hire Mandiant, because they know what they're doing." And seven years later, Mandiant is now a billion dollar company that responds to breaches, not only here in the U.S. but also internationally. So, that has been an example of the government actually sort of propping up a private sector company in order to do work on its behalf.

The government punishes companies when it comes to cybersecurity. I worked on an investigation when I was with the Homeland Security Committee in the House . . . an example of a private sector contractor, Unisys, that the Department of Homeland Security had been paying to protect its networks, and we found about a dozen intrusion detection systems sitting in a closet somewhere. When intrusion detection systems are sitting in a closet, they are not being used to stop the bad guys from infiltrating your network. The Department of Homeland Security kicked Unisys off of the contract. So, punishment--that's another way.

The government oftentimes creates or facilitates private information sharing. We talked about the financial services — ISAC — the Information Sharing and Analysis

Centers. These kinds of centers exist through all different kinds of sectors, whether it's the financial, chemical, or energy sector. So, this is another relationship that the government and the private sector have created with one another.

Sometimes the government has created standards with the private sector that the government enforces. And in that example, the North American Electric Reliability Corporation (NERC) actually writes cybersecurity standards for the industry, which are then enforced by the government. Sometimes the government creates standards without private sector involvement. The Nuclear Regulatory Commission writes its own standards. There's very little private sector involvement in that, but the private sector is being made to implement those standards.

Sometimes the government creates voluntary standards with the private sector, but there is no enforcement. And that's the NIST framework, an example of a public-private partnership with the government facilitating conversations with members of the private sector and industry to develop a series of standards that are voluntary; they are not enforceable.

Sometimes the government works with the private sector on education awareness. The national counterintelligence executive has convened meetings all over the country to provide information to private sector actors about counterintelligence threats. And, just the same, the government is working with the insurance companies right now to try to promote the idea and concept of cybersecurity insurance. So, this is another example of how the government, not through a particular requirement or liability or incentive, is actually facilitating conversations and discussions around the country to promote private sector action on the insurance market.

And a final way that the government and private sector work together is with training. Whether it's DHS or other government agencies, there is a sort of a famous national exercise called Cyber Storm that the government creates that would bring all different kinds of private sector actors to the table, and they sort of facilitate this talk about cyber Pearl Harbors. So, that's another example of how the government and the private sector work together on these partnerships.

The bottom line is that the government and the private sector have many, many different types of relationships, and when we're talking about building a partnership, we're not just trying to build partnerships with one particular group of private sector actors or one particular . . . you know, we don't want to just build relationships with technical folks. We want to build relationships with business folks and executives and others, but there are so many different types of relationships that are out there today. That is something to keep in mind when we think about what the next generation of relationships might look like. There's a lot out there that we can build on today.

TIMOTHY L. MEYER: Alright. Thank you very much. So, we have a good amount of time here for questions. I'm first going to actually look to people sitting up here,

particularly members of the first panel, to see whether there are any questions, whether the government has any questions for the private sector. Yes?

CLETE D. JOHNSON: This is a question for everybody, but just picking up on Jake [Olcott]'s last point, and to push back a bit on the notion that there's not a unifying theory–and I think I agree with Jake's point, but just to explore that a little bit more–could you argue that the unifying theory is that cybersecurity is not a problem to be solved but instead a risk to be managed? That it will be here forever, like the flu, like a cold, and then take more an epidemiological approach? And that, therefore, any organization, whether it's a government organization or a company, has to manage the risk by governance, by insurance, by a whole host of other risk management tools that apply across every other risk? Is that something that could help get us not necessarily to a unifying theory but to something that is a conceptual approach to cybersecurity that works no matter what your enterprise is?

BARRY HENSLEY: Where I struggle in that discussion, having been involved in lots of breaches last year of various organizations across all verticals, is those companies — whose risk are they assuming, right? So, it's my patient data that was lost, but they made a decision not to report because they couldn't prove the fact that the data was exfiltrated, but we knew for sure that they had been breached. We knew who the threat actors were. We knew what their tactic, techniques and procedures are. They took the data, but that organization, on their own, took the risk to say, "I didn't need to disclose that." Or, on the financial side, where my wife's credit card data got stolen months ago, but the report didn't come across until the bank got in touch with a retailer and said, "Hey, there's very strange charges on her credit card," — forced that retailer to now disclose. That's where I struggle is in that . . . I think risk is the key to this discussion, but ultimately who forces that company to ensure the right risk is taken for me as the end user?

ADAM GOLODNER: I agree with that, and I guess I'd add a little bit. I might even propose a unifying theory. My unifying theory is that for most of the government/private sector relationship, the interests of the private sector and government substantially align. That is my unifying theory. And that doesn't mean that it's perfect, but it means that fundamentally, their interests are the same. And I don't think that in public policy debates that's always the case. And, from the private sector perspective, no one wants their core service to stop functioning. No one wants to lose the trust of their customers or their partners or their suppliers. No one wants to really hurt some other actor within the marketplace. There are some tougher interests to align. The tougher piece is the intersection of espionage/war and commercial interests. An issue that deserves its own session.

Now here's a research question I would raise, one which Jamil talked a bit about this morning, as well as Clete. Is there market failure in cyber? In general I think not. But there may be a delta between what the market will drive as a result of rational market behavior, and a national security need of a country. That is the market, even if it brings a reasonable and rational result may not fully extend to what the national

security establishment thinks it needs. Usually if there is this delta in national security, governments build aircraft carriers and bombers. And perhaps that's what's happening now with cyber. But the impacts on the commercial sector need to be considered, and internationalized. There has been so little work about what that delta really looks like that I myself am very cautious about jumping to that next conclusion about what one might call a market failure, particularly in light of, I think Jamil [Jaffer]'s very good point, lack of full information within the marketplace for a variety of reasons. And I, myself, would rather work on the actual economics than go to the presumption about knowing what the delta is between what the market's driving and what the national security may need, particularly because of the innovation points and because I think you could really do significant damage to the future.

ANDREA M. MATWYSHYN: I'll offer a potential parallel. For me, infosec is much like accounting. You have to stay on top of it constantly or you're going to end up with lost assets. It's a process-based approach that needs to be maintained on an ongoing basis with regular auditing — not only internally but also externally — to make sure that something isn't falling through the cracks or just missed by the smart people already looking at it. So, vigilance and process-based solutions on a regular basis are definitely the way to go here, I think.

ADAM GOLODNER: One more thing, Jake, and I think, Clete, you and I had this discussion in the Senate at one point: the cyber issue is so multi-faceted — it's fraud, it's crime, it's espionage, it's war — and you can't solve those with one government response. So, I think we have to be very, very careful about asking what we are concerned about with each of those and then what tools are in the toolbox from a governmental perspective.

But as a general matter, people tend to munge them together. And, of course, we add to this because we just say "cyber," right? But in my mind, each of these is really substantially different and the people who care about crime — their job isn't really to care about war. The people who care about war — their job isn't really to care about crime. Now, some of the methods are the same, so that makes things a little bit difficult, but the fundamental pieces of government that have cared about those different things, which are so traditional, really are different pieces of government, and there are traditional tools to deal with each of those — even globally. They're just really hard, globally, but they're there, I think, but this is for the Rusk Center to work on.

But I think that traditionally, we've got the Law of the Sea Treaty, we've had the WTO, we have the U.N. Conventions and my sense is these are categories of paths forward we can look at. So, I think being very specific about what problem you're trying to solve with a particular policy response is really important.

JACOB OLCOTT: Well, I guess I was just going to say that the challenge, again just sort of bumping it back up to the 30,000 foot view here, the challenge that we have is that we've talked about disclosure a lot and the importance of enforcing

disclosure. So, most people, at this point, think that it is an important job for the U.S. government to enforce disclosure of cybersecurity incidents, whether there are incidents impacting, personally identifiable information, which is a state government issue, whether it's material losses of intellectual property or trade secrets, which is an SEC, sort of federal level, issue. And all I'm suggesting is that sometimes enforcing those laws, while important, can also present challenges for the public-private sector relationship, because the same people who are trying to enforce those laws are really irritating the general counsels within those organizations, right?

The IT staffs within those same organizations are trying to work hand-in-hand with the government on this public-private sector information exchange. So, those IT guys are trying to get the technical information from the government. We've all been hearing a lot about the importance of information sharing, and so the only thing that I would say is that sometimes we can all be sort of working towards the same issue, which is improved cybersecurity, but different organizations have different responsibilities to enforce laws or to promote information sharing or things like that. And so it can kind of muddle this whole public-private partnership idea.

JAMIL N. JAFFER: I mean, it's not just irritating the general counsels though, right? It's actually creating very real financial and reputational risk, right? The fact that you're being forced to disclose these breaches, while we may all think it seems obvious and critically important to our own identities, and, you know, sort of in the networks, it's very real and very concrete in a way that cyber risk may be harder to measure and the C-Suite . . . they get that when they're being forced to disclose a breach, that's going to cost them money in their bottom line. That's going to cost Target some reputational damage. People are going to be less likely to use their credit cards there and, over time, that maybe peters itself out, but it's a very real risk that's got to be managed. And so, you know, I think you're absolutely right that the government sort of coming at it from both angles. It's very hard to build trust when you're both trying to regulate and share information and sort of be the good shepherd while also carrying the stick and the carrot. It's hard to do.

TIMOTHY L. MEYER: Are there questions from the floor? Yes, sir.

AUDIENCE MEMBER: Again, William Foster from Emory University. For the past couple of years, I've had a debate with FS-ISAC as to whether threat sharing should be done just within the United States or whether the real challenge is to do threat sharing with the Chinese banking community and with the Russian [unintelligible] presidency. And I think one of the things that we haven't talked much about is the importance of Track 2 processes. So, right now there are debates between Emory and the Chinese Academy of Science and the Russian Academy of Science about threat sharing that could never happen at a government-to-government level.

VICTORIA WOODBINE: It is happening at the government-to-government level as part of diplomatic dialogues and other exchanges, and an important part of that is

information sharing. So, there is some; it's in the very embryonic stages, but in certain relationships sharing threat indicators is happening.

AUDIENCE MEMBER: [unintelligible]

VICTORIA WOODBINE: But you have to start somewhere.

QUENTIN E. HODGSON: If I could just jump in on that as well. We have pursued Track 1, Track 1.5, Track 2 dialogues, certainly with the Chinese, also with the Russians and various other countries, on these issues. In fact, the National Science Foundation also is engaged in this with the Chinese. So, we don't lack for people talking to each other. Sometimes we struggle a little bit with getting the right people from the other side to engage in that dialogue. Talking to a country and saying, "We would really like to have you bring to the table people who represent your intelligence and your military communities," the response we get is: "Well, we don't have an equivalent of your Cyber Com, so we can't . . . we don't have that." And we know that's not true, but it's something where at least we're continuing to engage in that conversation.

Certainly, cyber has been a significant topic between the United States and China at all levels right up to the presidential level, and I think that's good, because the main thing we're most concerned about there, among many things from our perspective, certainly in DOD, is ensuring that we don't have a miscalculation or a misunderstanding about what people are really doing and what's happening. And given the volume of activity in cyberspace, there is a significant risk that that could happen.

One of the things you talk about in cyberspace is that the difference between infiltration of a network to be able to get information out of it and infiltration of a network to do serious damage is really just a question of what's the last keystroke that you initiate. That's a little bit oversimplified, but still, from a perspective of trying to understand what somebody is doing when they're in your network, it's very difficult to figure that out. And that's one of the reasons why we have to maintain these dialogues: to point out where we have various concerns, to try to have those competency building measures moving forward.

AUDIENCE MEMBER: Ken Parris with TradeSecure. I'd be interested to hear from a number of the panelists. What proportion of cybersecurity attacks are lapses in best practices of standard operating procedures, and what proportion are the safe-cracking, where somebody is actually going in and breaking the network? And, in the spirit of closing the information gap, what are the statistics the government has versus the private sector on those?

QUENTIN E. HODGSON: Well, I'll jump in a little bit. We talk about the growing sophistication and volume in cyber attacks, and attack is probably a bad word because we mix our lexicon, but when you look at the number of times that people have successfully been able to infiltrate a network, I would say roughly speaking — don't

quote this specific number — 90 percent of the time they're using tried and tested techniques that have worked for over ten years. The fact that sequel injection is still something that people are able to do is mind-boggling, because it's actually an easy thing to fix, but it goes back to: What kind of verification are you doing on the code?

I also think I mentioned this to somebody in the hall outside: We do a really poor job of training people on awareness and techniques when it comes to cybersecurity, and I'm not talking about system administrators. I'm talking about, you know, stupid me, the user. There's a Level 8 problem, you know, user error. The thing is that the way we approach the training for this is as sort of an obligation. Tick the block, do it once a year for an hour, and then you're done. And that's not the way people learn. You have to articulate and work on understanding the threat, making sure that people recognize what a spearfishing attack looks like.

There's an interesting study, I think, a British . . . I think the University of Bradford looked at the ability of people to recognize what was legitimate email versus illegitimate email. And I'm not sure of the exact numbers, but roughly half the time people identified as illegitimate that which was legitimate, and they identified as legitimate half the time that which was illegitimate. So, it's not an easy task, but at least giving people the sense of what to look for . . . . Don't click on tiny URLs, actually look at the whole URL that you're faced with. Know that, just generally, your friend is probably not lost in Ukraine with no credit cards and needing $10,000 to get home. That literally happened to a friend of mine, and I had to send her a Facebook message saying, "I'm pretty sure that you're not in Ukraine, but could you just confirm this?" because she didn't know that somebody had hacked into her account.

BARRY HENSLEY: [Remarks are off the record.]

JACOB OLCOTT: Can I just add one thing to this conversation? As more of the Fortune 500 becomes more sophisticated, it's the third-party risk, the vendor risk, that's really becoming much more elevated for those companies. So, you know, if you look at the Target case, as discussed earlier, it was an issue of the bad guys breaking the Target HVAC vendor and then accessing the Target network through that vendor. By the way, does anybody think that that sounds really sophisticated? Does that sound really sophisticated to anybody? I mean, you'd be surprised. I asked a lot of people; most people would say, "Oh, my God, that seems like . . . that's the most sophisticated thing I've ever heard." But, at the end of the day, it's a vendor risk management issue. You don't want your HVAC vendor to be able to get access to your 100 or 500 million credit card numbers. That's not rocket science, right?

So, anyway, the bottom line is that the attackers are shifting more towards the vendors and other third parties, law firms, consulting firms, other actors, or other vendors who have access to your sensitive information. And that's become the shift. So, now companies are trying to figure out: How do I manage vendor risk? How do I make sure that I know what's happening on their networks and what they're doing with my

information? And that's really sparked a big . . . there are a lot of lawyers who are reviewing contracts right now for that, too.

AUDIENCE MEMBER: Sort of bouncing off of that, I feel like we've talked a lot about government relations with cybersecurity between governments and companies and the private industry and foreign entities, companies using, for example, the Chinese government to get better information for the Chinese companies from the U.S. government and U.S. companies. Where are we, at this point, on increasing awareness or increasing cybersecurity between companies? I feel like that's something we haven't talked about too much.

BARRY HENSLEY: [Remarks are off the record.]

ANDREA M. MATWYSHYN: I'll just follow up on that. Much of the security research community is wedded to each other through interpersonal relationships. So, there are trusted individuals who deal with other trusted individuals. And that's partially why this professionalization movement within the infosec industry is important, because it's a way to try to operationalize the broadening of those trust relationships and implement a bit of homogeneity through standards of conduct — the way that we have in other professions that have had a longer period of time to evolve.

JAMIL N. JAFFER: Yeah. I think the challenge though, of course, in both these scenarios is that when you expand the group, and you don't have this, "I don't know that that person over there is not going to screw me," or "I don't know whether to trust them." You've got to find a way to make these things replicable over time. One way may be professionalization. One way may be connecting these various networks of trusted groups here, trusted groups there. But I think, fundamentally, what you've got to do is figure out a construct, a sharing construct which takes advantage of sort of private sector incentives. How do you ensure that the market and the profit motive can drive trust? I'm a fundamental believer that there is a market here to be created for creating this trust between companies, that you can find a third party who will guarantee the trust, who will ensure that I'm the center point of the transaction between three or four of you, right? And the way that you know you can trust that person is because I trust that person and you trust me. And why do you trust me? Because my profit motive is driven by the fact that I've got to maintain that trust between you and that trust with them — otherwise I lose business.

Fundamentally, I think there is a construct here that can work. The hard part is getting there. But once you're there, and these trust relationships can be built, you can make them replicable and faster [. . .], pick up the phone or send an email to the group and actually just share the data in real time if you've got a few . . . two or three or four or eight or ten center points that other market players trust as their methodology sharing.

BARRY HENSLEY: It's interesting you mention that. When I was at the Department of Defense, we had something called the Computer Network Defense Service Provider,

where the Department of Defense would actually certify the services — Army, Navy, Air Force, Marines to now be a CNDSP for others, as an example, and it facilitated that trust relationship. Well, today we're the computer network defense service provider, SecureWorks for 3800 customers around the world. We host annual meetings, actually our global client forum is next week. Well, specifically those customers will come in and they have a trust with each other because we're their common bond as a security provider, which has been interesting.

CLETE D. JOHNSON: I completely agree with everything that everybody said and Jamil [Jaffer]'s point about building automated trust mechanisms where computers can trust each other and companies can trust that information shared is secure and not disclosed, etc. But I would add that beyond the notion of trust, there's a second level that I think is really important, and that's what reasonable expectations are with regard to both information sharing, but also best practices. So, just like when we drive down the road, we don't "trust" the other driver. I don't know the other driver in the street, I don't "trust" him, but I can reasonably expect that he's going to stay on his side of the road and I'm going to stay on my side of the road. We both know how this system works. We know what the expectations are. This is a different, lower level of trust: trusting the system, based on reasonable expectations.

That doesn't presently exist in a mature way in the cybersecurity ecosystem. It's developing. I think this NIST framework provides a common language of expectation that can at least begin the process of developing this system of trust and expectation. You know, if Target is contracting with an HVAC vendor, they can at least have some articulated expectations--or, eventually, maybe unarticulated implicit expectations– about what all the players in the system can reasonably expect of the other players with regard to what cybersecurity level they're playing at.

And it may be that the HVAC vendor says, "You know what? I don't need that level of security in this area, that area, the other area to be a profitable business." In which case, Target could say, "Okay, well then you should focus on that sector. We need to get somebody who's playing at a higher level." But I think in this case . . . and this gets back to Ken [Parris]'s question about best practices . . . in almost every case, you could either prevent an exploitation, or make it much harder by doing something a little bit better somewhere along the way — usually it's in retrospect. But until we have this common language of expectation, we won't be able to do the risk management or the contractual demands or, eventually, tort liability enforcement of how you police these best practices.

JACOB OLCOTT: This is actually why I think today is just a very fascinating time in cyber risk management because the liability issues are so significant. It is such an important driver for every business, whether it fully appreciates it or not. Sometimes we would joke that it would have been a lot easier if we had just passed a bill years ago that would have clearly established what the standard of care is for the private sector, but that didn't happen. There is no bill out there. There's no specific legislation

that kind of dictates what a standard of care is. And so, across all of these different industries, whether you're an energy company, whether you're a hotel business, there are all of these different standards of care. And the interesting thing is that any time that there is a breach . . . for instance, Target is now facing eighty class action lawsuits . . . that's a lot of lawsuits. And so, what that is going to teach us about the evolution of the standard of care that companies like Target will have to meet in the future is actually one of these really important drivers in getting this whole cyber risk management thing right.

BARRY HENSLEY: [Remarks are off the record.]

JACOB OLCOTT: That's a great question.

CLETE D. JOHNSON: I can't wait to hear Adam's follow-up.

JACOB OLCOTT: I want Adam to put his Cisco hat back on. This is a great question. I think you're already seeing a new trend in recent years where the end users are starting to demand more from the software vendors themselves. For many, many years, there was not this demand for securely developed software. That has been changing, and it will continue to change when end users are on the hook for vulnerabilities that are exploited by the software manufacturers who create them.

Another interesting case from Target that will play out in the weeks ahead is that, in one of the lawsuits, a company called Trustwave, which provided the payment card industry data security assessment for Target is now being sued because they certified that Target was compliant with the payment card industry standards. I think this is going to be a really fascinating legal development. Can a company . . . can an auditing and assessing firm be held liable for certifying that a company has successfully passed an audit or assessment but, in fact, was eventually breached? So kind of stay tuned for this litigation because the success or failure of that case is going to have really, really big implications for other software vendors, other auditors. You know, the Big Four are going to look at this and say, "Are we going to get in this game or get out of this game?"

ADAM GOLODNER: I guess, to my way of thinking, all of this is actually quite traditional. And so, the Congress had a fundamental choice . . . Congress and other people. You could try to have a regulatory approach to all these issue sets. If you did, most people were rightly quite concerned about impacts on innovation which, at the end of the day, is probably the most important tool for getting ahead of the cyber problem. If you regulated here, you risked throwing the baby out with the bath water. There is that, plus a general political aversion to more regulation. But most of the cyber issues are the kinds of issues that common law has dealt with forever. There were some people who argued for new special liabilities for software, which failed because of predictable adverse impacts on innovation, but in general, as in most use cases, the common law continues to apply.

TIMOTHY L. MEYER: I would just add an accounting point. One of the issues that happened in the securities context as lawsuits have moved towards auditors is that auditors are actually . . . there are jurisdictional problems because the auditors are often organized as networks themselves and oftentimes the auditing is being done offshore by an entity that doesn't actually have a direct connection to jurisdiction where the lawsuit is being filed. I'm more familiar with this in a securities context, but if you saw that sort of move happen . . . I mean, it is done partially for liability reasons because if you can evade jurisdiction, you can functionally evade liability.

We have time for one more question.

DON JOHNSON: I've got just a brief question. I want to ask Jake [Olcott] this question, because I understand you've been working on disclosures for purposes of the SEC requirements. Just wondering if you could speak to that just a little bit. What are the issues involved in that?

JACOB OLCOTT: I'll try to be brief about this. Back in 2011, the Securities and Exchange Commission issued guidance to publicly traded companies about their obligations to disclose two things in the cybersecurity context. One is material cyber risk and the other is material cyber incidents. "Material" in the SEC context means things that are important . . . information that's important for the average investor to know before making an investment decision.

What the SEC did was take eighty years of law requiring the disclosure of material information, right? This is back in the 1934 Securities Act. There was this requirement that companies–publicly traded companies–disclose material information to their investors. And what the SEC did in 2011 was apply that law in the cybersecurity context. And so what they've done is that they've spelled out a lot of different scenarios where a publicly traded company should be disclosing incidents to their investors. And those incidents look like the loss of material intellectual property or trade secrets, the loss of a material amount of personally identifiable information or other sorts of sensitive health information, the material disruption of operations over a period of time. So, it's all under the lens of this thing called materiality, and it's a really important development for public companies because it places additional–again, I'm getting back to this liability issue. It places additional liability on companies who fail to disclose those things.

And the idea from the policy perspective, the idea is that we want to encourage disclosure of these types of things because the market will work better if there's more information in the market. So, if I'm an investor, I want to know if General Electric has lost a material amount of intellectual property via cyber theft because, if they have, then I'm less optimistic about GE's future earnings. I can take my small amount of money in GE out and invest it in a company that maybe has better cybersecurity. So, I highly encourage anybody to take a look at this guide. It's very readable. You'd think that SEC . . . that sounds like really kind of wonky and 10-K's and 10-Q's and stuff, but it's actually . . . it's a very readable document.

ANDREA M. MATWYSHYN: Can I put it in a quick plug? I wrote an article on this topic in 2005 that advocated precisely this approach. It's called "Material Vulnerabilities" and it's in the *Berkeley Business Law Journal.*

JACOB OLCOTT: If only we had gotten together in 2005, we would have had it done earlier.

TIMOTHY L. MEYER: Alright. With that, we are at our time here. So, let's thank our panel one more time.

Cybersecurity and National Defense: Building a Public-Private Partnership

Lunchtime Address:
The FCC's 'New Paradigm' for Communications Security in the Internet Era

Clete D. Johnson, Chief Counsel for Cybersecurity,
Federal Communications Commission

DON JOHNSON: For those of you who were not here at the beginning of the conference this morning, I'm going to briefly introduce myself. I'm Don Johnson, the director of the Dean Rusk Center. We are a sponsor of this conference along with SPIA (the School of Public and International Affairs) and Dr. Loch Johnson. And on the first panel, one of the speakers, Clete Johnson, and I are related. I'll just give him a very brief introduction. He has already been introduced for the first panel, but some of you might not have been here, so I'll give you just a little bit of background.

He graduated from this law school in 2004 and went to Patton Boggs in Washington and did international security and trade practice there. And then, after a couple of years, he went to the Senate and worked for Senator [John D. "Jay"] Rockefeller, while Rockefeller was the chairman of the Intelligence Committee. Eventually, Clete went to the Intelligence Committee and focused on terrorism financing. He was also involved in the interrogation investigation that the Senate committee did, and that has been in the paper a little bit lately. Then he focused on cybersecurity. When Senator Rockefeller became chairman of the Commerce Committee, he began working on the cybersecurity legislation, and I'm not going into great detail about that. He only recently — at the beginning of this year — joined the FCC (the Federal Communications Commission) in a newly-created position, chief counsel for cybersecurity. So, with that brief introduction, I will call on my son to begin.

CLETE D. JOHNSON: Well, thanks. I want to emphasize that this is an informal discourse just to wrap up the day's discussion, because it does tie together a lot of the themes that we've been discussing all day. Before the conference, I asked my dad: "Is there a lunch speaker?" And he said, "I don't know — is there?" And so I don't know if I was conscripted into it or volunteered, but I'm more than happy to talk about how all of these issues that we've been discussing today — public and private, government coordination, facilitation and private sector dynamism and risk management — apply to this new role that I'm in at the FCC, which I just started three months ago. And this

is particularly for Jamil [Jaffer], who is presently a Republican staffer in the Senate. We have not begun our Hill outreach yet, so I'll just use this discussion as kind of a test run. Everything that I'm saying will be aimed at making Jamil Jaffer think this is all a wonderful idea.

Just to circle back on one of the themes that Vicky Woodbine was emphasizing: there is a truly international nature to this challenge. Later this afternoon, my boss, the head of our agency, Tom Wheeler, who's the chairman of the Federal Communications Commission, will be meeting with his counterpart in the United Kingdom, Ed Richards, who is the director of Ofcom, the U.K. Office of Communications. They're having a high-level discussion about how regulatory agencies address this issue, and I can assure you that Tom Wheeler will be saying that the way that we do this is that we need to harness the dynamism and innovation of the private sector. Private sector companies are on the front lines of defending against the cyber threat in a way that they have never been on the front lines of any other security issue in the past. Also, the private sector is our society's primary engine of dynamism and innovation, and if we don't harness those qualities, we will not be able defend our society in the way that it needs to be defended against this dynamic and innovative threat.

So, with that lead-in, I'll just take a step back and give a brief overview of the FCC's role with regard to public safety and security. It's an organization that was created in 1934. There were a lot of new government agencies that were created in 1934, including, as Jake [Olcott] mentioned earlier, the Securities and Exchange Commission, at the same time that the Communications Act of 1934 established the Federal Communications Commission to regulate wireless and wired communications. At that time, this meant radio and telephone communications.

Actually, I'll take another step back, to before 1934: The FCC's predecessor organization was the Federal Radio Commission, which was created four months after the Titanic disaster in 1912. The Titanic happened to go down in a time when there was a great proliferation of new wireless radio communications, which could have been a significant lifesaver in the North Atlantic, but didn't become that because there was insufficient standardization of communications. Essentially these radios that were talking to each other in a lot of two-way or small group communications could not communicate to each other more broadly that "there's a huge ship going down, and we all need to get there as quickly as we can to save as many lives as possible."

Very soon after that, the Congress passed the act that created the Federal Radio Commission, which twenty-two years later got rolled into the Federal Communications Commission. And so it's no surprise that the public safety and national security implications of communications are baked into the DNA of the FCC.

Specifically, this responsibility is explicit in Title I of the statute. This has been part of the FCC's mission since the very beginning: What are the national security and public safety implications of the communications sector? First, the national security element: How do we make sure that the communication networks that people rely

on don't go down? Then the public safety element: How do we increase public safety through more and better communications when the communications are needed, particularly in emergencies? Anybody in this room who has made a 911 call was making a call whose resilience and availability is undergirded by, among other things, FCC regulation and oversight. The same is true of the emergency alert system–the service that most of us would have never heard of except for the tests that go out through the broadcast networks. Today the FCC is there to make sure that these public safety communications imperatives, which don't necessarily always have strong market incentives driving them, are available for the public through the airwaves and communication networks.

The very challenging question now for the FCC, which has regulated radio, broadcast and telecommunications for decades is: What do we do now that every element of our communications infrastructure is changing? My mom–who is also here for this family reunion conference today!–will appreciate this because her father, my grandfather, was a surveyor for AT&T for thirty years and he and his crews laid coaxial cables all throughout the Southeast. I remember being a kid and my granddad had this hat that said, "Call before you dig." And I had no idea what that meant back then, but what it meant is: don't bring a backhoe onto your property without calling AT&T first, because there might be a cable that a lot of people rely on for their telecommunication services.

Well, now, sadly for nostalgic reasons, but happily for better communications reasons, those cables are being replaced by fiber optic cables. And at the same time that we're moving from copper to fiber, we're also moving from what's called switched circuit telephony, where an operator connects people with other people by a central switch. This is the old-fashioned, "Operator, please connect me with so-and-so." That's still the way most phone calls happen–now with automated switches rather than a human being, but still effectively an operator in the middle. But that central switch-based telephony is presently beginning to transition to an Internet Protocol-based communication system in which packets of data, including the voice data that make up phone calls, are routed via the vast Internet, not through a central switch.

And finally, there's another development that's yet another revolution.We're moving from fixed wireline communications to mobile, wireless communications. All of this is happening right now, and these revolutions will completely change the way our communication infrastructure works. This obviously has significant implications for whether, and how, all of those communications functions that we have long relied on will continue working the way they always have worked. Not just 911 and the emergency alerting system–increasingly, communications in general, and therefore Internet Protocol-based communications in particular, are not a luxury anymore. They underlie everything that we do, from security to business prosperity to interpersonal relationships.

And so, the real question for the FCC is: How does the eighty-year old communications regulatory agency play in that space, just as everything is changing? And how do we

continue to guarantee what the FCC calls the "enduring values" of communications, one of which is public safety and national security?

This is a very complicated question because the laws don't always neatly match what the practical needs are, but I think that the new chairman of the FCC, Tom Wheeler, who was confirmed in October 2013, has brought in lots of energy directed at harnessing private sector dynamism and innovation to solve these problems in a manner suitable for this new technical reality. I'll describe what Chairman Wheeler calls a "new regulatory paradigm," in which the private sector communications companies largely regulate themselves by aligning private interests, such as return on investment and profit, with the public interests in safety and resiliency and security.

He has some real chops on this. He's a venture capitalist who, among other things, helped create EarthLink. He has been at the cutting edge of every tech development in the communications sector in the past several years. He knows Washington very well. He has led two different industry associations in the communications sector, both times as insurgents against incumbent industries in a breakthrough era. He led the cable association when cable was trying to break through against a lot of entrenched interests, and likewise he led the wireless association when wireless was breaking through as a new technology. And then, more recently, his venture capital company's watchword was to invest in disruptive technologies.

He's bringing that energy into the FCC's regulatory environment in order to apply those principles of private sector driven innovation and dynamism into an institution whose core business has long been to issue mandatory rules. It is the reason that I decided to leave Senator Rockefeller's staff to go to the FCC: these issues perfectly align with the cybersecurity approach Senator Rockefeller has been pushing for years and years, so I feel like I am sort of "deploying forward" out into field operations.

Now I think we have a chance to implement these principles in a crucial sector, because the communications sector touches every other industry sector, from financial to energy and down the line. If we can solve network security problems in the communications sector, among the telecom providers, the Internet service providers, then that won't solve every single cybersecurity problem in our country, but it sure will help bring solutions to these challenges in other sectors. Chairman Wheeler made a very compelling pitch that he really means business about doing this and, most crucially, doing it right with the private sector leadership.

He also brought on a very accomplished Navy admiral who was the number two at DISA, the Defense Information Systems Agency, Admiral Dave Simpson, who is my immediate report. Admiral Simpson has an incredible background. He's an engineer. He basically helped the Navy get through Y2K. He's worked cybersecurity challenges at the weapons systems level. And also, more recently in Iraq, he was responsible for bringing the fiber Internet backbone to Iraq.

What Chairman Wheeler wants us to do is try to bring some of that perspective and energy into these truly new challenges about how we–our society, public and private sectors together, not just the government alone–govern the assurance of security and resiliency in the communications sector when the entire sector is changing. And I'm just going to lay out a few legal issues that we're going to encounter as we do so.

First, Chairman Wheeler wants to ensure that we are not just balancing, but maximizing, the principles of security, privacy and innovation. If we approach this right, it's not a zero-sum game between any of those three crucial principles, but rather they all mutually reinforce each other. On the other hand, if we focus too much on security, we're going to lose out on privacy and innovation. And likewise, if we focus too much on any of the three, we lose out on the other two. And that's the charge that he's given us as we go forward: Maximize all three.

For those of you who missed it this morning, there has been essentially a five-year cybersecurity policy discourse that began to crystallize last February (2013) with the executive order from President Obama that laid out a voluntary process of standards development facilitated by the National Institute of Standards and Technology (NIST). NIST undertook a year-long outreach effort to any stakeholder that wanted to join this discussion, and this diverse group of industry players helped NIST develop Version 1.0 of what is called the NIST Cybersecurity Framework. It is a reference guide for how enterprises–companies, governments, etc.–can manage cybersecurity risk. And industry really leaned into this. They dove right in and got to work. They did not play defense, they dove in and played offense. Because they wanted to shape this Framework, because they knew it was going to be an important reference point. And so, they shaped it and made it theirs.

What Chairman Wheeler wants to do with the Framework has particular resonance coming from a regulatory agency, because the guiding principle of this NIST framework is that it's voluntary. It's something that companies themselves say is a good idea, and therefore they will want to do it for their bottom line, not just because they are required to by any law or any regulator. So we're trying to find and promote and make real what the Chairman calls a "new regulatory paradigm" that dovetails with these voluntary processes, that helps poke and prod where needed, and catalyze or converge and find a confluence of interests where needed. The government role is to help bring people together and show them why it's in their own private interests to implement this Framework.

We want to dovetail with those voluntary interests, not issue new mandatory requirements. Something that Admiral Simpson has said on a number of occasions that may be worth repeating here is that "the FCC regulates best when it regulates least."

To summarize, there are three areas that we've discussed quite a bit today. First is standards and best practices for risk management. What are the best practices that institutions can put in place to secure their networks? Second is threat and vulnerability

information sharing. This is something that we talked quite a bit about today. How do we communicate both among companies and among and between government and public and private entities what the risks are and then how operationally to address those risks? And the third is always recognizing that these cyber challenges take place in an international environment and are not problems that the United States can solve alone, even if it were to address those challenges perfectly within the United States. The Internet is global, and hopefully always will be global. It has to be like-minded governments and like-minded companies, including those companies which are multinational that need to communicate risk to each other and manage risk together.

Regarding the first issue, standards and best practices for risk management, last Thursday, Chairman Wheeler launched a working group, an advisory committee, that advises the FCC on how to proceed on various security and reliability issues. It's a five-letter acronym called the CSRIC, which stands for the Communications Security Reliability and Interoperability Council. And it's a very diverse, multi-stakeholder group that, under the Federal Advisory Committee Act, provides the FCC with advice on various issues. What we did last Thursday was we launched a working group that's specifically focused on how the FCC should manage the communication sectors, implementation of this voluntary NIST framework.

The chairman is a very charismatic leader, and he really laid down these points clearly and compellingly to the stakeholders at this CSRIC launch. He asked them to make this process the gold standard of how private sector stakeholders drive a public-private collaboration, where the FCC essentially is the convening authority and the private sector is coming up with suggestions on how to develop standards and best practices that are not just a list of good ideas but that are measurably, accountably implemented by the boards and the executives of these companies.

It's not just developing a list of technical things that the IT department should do; instead it's developing a risk management approach that allows corporate leadership to know that these best practices are actually being implemented in a way that reduces the risk to the company's bottom line.

At the launch, Chairman Wheeler started to say, "If this works . . . ," and then he cut himself off and said, "No. It's not 'if it works'; it has to work because the only alternatives that we have"–and here he was referring to traditional regulation--"are not attractive." He said that traditional prescriptive regulation is not the right tool to address this challenge, because cyber threats are too fast-moving and innovative, and if we approach cybersecurity with traditional regulatory approach of prescriptive rules, it won't work. So, he laid out a challenge, really an exhortation, to the private sector stakeholders to do what they have long professed, and I think genuinely believe they should do, which is to secure cyberspace by securing their own pieces of it for the benefit of their own businesses.

It's an exciting new initiative, and it raises all sorts of novel legal issues. Does this process create a standard of care? Does it create something that will have to be

reported as a risk management approach in the SEC filings that Jake [Jacob Olcott] mentioned earlier today? How does a regulator manage a voluntary process in such a way that it doesn't become a mandatory regulatory process? I don't have the answers today, but the companies involved in this important work will surely grapple with these questions. What I can say today is that wherever this process leads us, we're going to be guided by the principles of maximizing security, innovation, privacy, and harnessing private sector-driven processes.

Regarding the second issue, information sharing, this is crucial because if the right parts of the company or the government or a particular industry sector don't understand what the risks and threats are, then they necessarily will not be addressed.

The challenge is that there are statutes that limit the type of sharing that can take place between companies. Say, if AT&T and Verizon see a threat out there, and they want to communicate about it so as to do something about it, there are complicated questions about how far they can go in in their discussions without breaching anti-trust limits. Say they come up with a solution together that might be more costly — that passes on the cost to the consumer. Is that anti-competitive collusion? Questions like this are hard, and we've got to clarify these issues so that companies can do the sharing that they need to do, and that we need them to do.

Then, there's private to government sharing: there are a whole host of privacy statutes, most notably the Electronic Communications Privacy Act (ECPA), which forbids companies from sharing electronic information with the government unless it fits an enumerated list of exceptions, for instance if the information pertains to a crime. And there are some difficult questions about gray areas in this arena. For example, if a company sees a cyber-threat which may arguably constitute a crime, but not yet a manifested crime, is that something that the company can share with the government without violating ECPA? It's a criminal statute, so if there's a gray area there, the company's general counsel is probably always going to say, "Don't share, because if we're wrong about the gray area, it's a criminal violation." We've got to work through those issues and clarify them to the extent that we can.

Finally, on the third big cybersecurity issue, again, this is an international set of challenges — Vicky [Woodbine] and Adam [Golodner] both spoke to that in-depth. The ITU has begun to grapple with it, and a whole host of countries that don't agree with our private sector driven, multi-stakeholder model want the Internet to be under government control. And there are some very powerful countries and not just what we know as adversarial countries. Russia has a view on this, and it's not our view. So do China and a number of Arab countries, particularly following the Arab Spring uprisings, and India. I would say even the EU, minus the U.K., is taking an approach that's more prescriptively regulatory than the multi-stakeholder, private sector-driven approach that the United States is undertaking.

That's why we think that this little working group in the FCC's Federal Advisory Committee can be such an important player. If we prove that this is the right way

to secure our communications infrastructure, then it won't have an impact only in the communications sector of the United States. It will have an impact outside of the communications sector in the United States and other U.S. industry sectors, but also probably, much more importantly, it will have an impact throughout the world, beginning with our closest allies like the U.K. and other like-minded allies, but hopefully eventually spreading this approach throughout other countries' cybersecurity models.

That's a tall task, but we've got at least a structure of a beginning for how we're going to do it. And so, we've got a lot of work to do, and I've still got a lot to learn, but three months in, it's a pretty exciting place to be.

Who knew this is where I would be, back when I was a first-year law student here. Three weeks into my first year, 9/11 happened, and I faced a really tough set of questions, sitting here studying the rule against perpetuities, all while the world was changing around us. And I thought, "What am I doing here? I need to get out and be part of the solution, not sitting here studying torts and contracts." And, among others, my dad and Loch Johnson said, "The best thing you can do is to focus on these legal issues. These national security challenges are not going away, they're going to be part of what we're dealing with for a long time and there need to be lawyers who understand how it works."

And since that time I've moved from the "hard security" counter-terrorism issues into this developing field of cybersecurity. I wouldn't have known what cybersecurity even was back in 2001, and I've still got a lot to learn, but it's a really exciting field to be in. And if there are any students here today who are still out there thinking about it, let me make a pitch to you. Focus on cybersecurity law; this will be a field that will guarantee you employment for the rest of your life.

So, with that, thanks very much. It has been a great day.

Cybersecurity and National Defense: Building a Public-Private Partnership

March 31, 2014

About the Speakers

Panelists

Adam Golodner is a Partner in the Complex Commercial Litigation Department of Kaye Scholer LLP and the leader of its Global Cybersecurity & Privacy Group. Previously, Golodner was an executive for Cisco Systems Inc., where for nearly a decade he created and drove its global cyber security and privacy program. In that capacity, he advised the White House, Congress and various agencies globally on cyber issues and regularly interacted with governments (including the U.S., EU, India, China, Russia, and Japan), companies, and trade associations on security, privacy, innovation, cloud, Internet of Things, social media, big data, critical infrastructure protection, information sharing, product integrity, and supply chain issues. Before joining Cisco, Golodner was the Associate Director for Policy at the Institute for Security, Technology and Society at Dartmouth College, Chief of Staff of the U.S. Department of Justice's Antitrust Division, and Deputy Administrator of the U.S. Department of Agriculture's Rural Utilities Service. Golodner began his career at a Denver-based corporate law firm, where he became Partner in 1992.

Barry Hensley is the Director of the Counter Threat Unit (CTU) Research Group at Dell SecureWorks. The CTU is comprised of the nation's top security experts who identify and analyze emerging cyber threats, while developing rapid countermeasures in support of more than 3,000 customers worldwide, including 20 percent of Fortune 500 companies. Col. (Ret.) Hensley served in various leadership positions throughout his 24-year career in the Army, including assignments with the United States Special Operations Command and deployments to Saudi Arabia, Kuwait, Somalia, and Iraq. He is also the former Director of the Army's Global Network Operations and Security Center, and a past Director of Operations of the Joint Task Force-Global Network Operations, the present-day United States Cyber Command. In 2008, Federal Computer Week presented Hensley with its annual Federal 100 Award, which recognizes government and industry leaders who serve in pivotal roles in the federal government IT community.

Quentin E. Hodgson is the Chief of Staff for Cyber Policy in the Office of the Under Secretary of Defense for Policy. In this capacity he oversees efforts to develop cyber operations policy and integrate cyber operations into contingency plans, advises senior leaders on future cyber capabilities and programs, and manages strategic projects for the office. Prior to his current position, he was Futures Team Lead in the Strategy Office, responsible for the development of scenarios used to support future force planning. Hodgson also has served as a Planner in Policy Planning, where he was the principal author of the 2008 National Defense Strategy and was responsible for Special Operations Command and Central Command contingency planning guidance development and review. From 2003-2007 he was a Stability Operations Coordinator in Policy's Special Operations/Low-Intensity Conflict division, where he developed and implemented the Global Peace Operations Initiative, a presidential initiative to increase global peacekeeping capacity, in addition to developing initiatives to improve intelligence support and planning for stability operations.

Jamil N. Jaffer currently serves as a senior Senate staffer and as an Adjunct Professor of Law and Director of the Homeland and National Security Law Program at the George Mason University School of Law as well as an Adjunct Professor at the Elliott School of International Affairs at George Washington University. Jaffer has previously served as Senior Counsel to the Permanent Select Committee on Intelligence of the United States House of Representatives, in the White House as an Associate Counsel to the President, handling Defense Department, State Department, and Intelligence Community matters, as Counsel to the Assistant Attorney General in the National Security Division of the United States Department of Justice, and as Counsel in the Justice Department's Office of Legal Policy. In addition, he was in private practice at Kellogg Huber, a Washington, D.C.-based trial litigation firm, and taught as an Adjunct Professor at the National Intelligence University.

Clete D. Johnson is the Chief Counsel for Cybersecurity in the Public Safety and Homeland Security Bureau of the Federal Communications Commission (FCC), where he helps implement the Commission's cybersecurity mission. This includes working with stakeholders to identify and address communications sector vulnerabilities, and increasing the security and resiliency of critical infrastructure within the communications sector by facilitating the development and implementation of cybersecurity best practices. Johnson came to the FCC from the Senate Intelligence Committee, where he worked on a number of initiatives within the Committee's cybersecurity portfolio and served as the Committee's lead staffer on financial intelligence issues. He was also the staff lead for Senator John D. Rockefeller, IV's cybersecurity legislation and related stakeholder outreach. Previously, he served as the Senator's Counsel for defense, foreign policy, and international trade. Before going to the Senate, Johnson practiced law at Patton Boggs LLP.

Andrea M. Matwyshyn is an Assistant Professor in the Legal Studies and Business Ethics Department in the Wharton School and an affiliate of the Center for Technology, Innovation and Competition at the University of Pennsylvania Law School. Her research focuses on technology and innovation, data security, consumer privacy,

and technology entrepreneurship. In addition, she is a Senior Policy Advisor in the Office of Policy Planning at the Federal Trade Commission, where she advises the agency on privacy and data security policy issues. Matwyshyn is currently a member of the Board of Advisors of the EU-funded Network of Excellence in Internet Science (EINS) project at the Oxford Internet Institute and a faculty affiliate of the Center for Internet and Society at Stanford Law School. She has previously taught on the law faculties of Northwestern University and University of Florida, and was an affiliate of the School of Engineering at the University of Cambridge and a corporate attorney in private practice.

Jacob Olcott manages the cybersecurity practice at Good Harbor Security Risk Management, where he helps senior corporate executives navigate complex cybersecurity policy and legal decisions and develop programs that identify and mitigate cyber risk. Previously, Olcott served as Counsel to Senator John D. Rockefeller, IV, Chairman of the Senate Committee on Commerce, Science, and Transportation, where he acted as the chairman's lead negotiator on comprehensive cybersecurity legislation. He also led a review of corporate disclosure practices that contributed to the issuance of groundbreaking cybersecurity guidance by the SEC in October 2011. Before advising Chairman Rockefeller, Olcott was Staff Director and Counsel for the Subcommittee on Emerging Threats, Cybersecurity, Science, and Technology of the House of Representatives Homeland Security Committee, where he developed and executed the legislative and oversight agenda in cyber, nuclear, and biological security. He has been honored with several national awards for his work in cybersecurity policy.

Victoria Woodbine is the Cyber Policy lead in the Foreign and Security Policy Group at the British Embassy, Washington D.C., a position she assumed in September 2012. She is responsible for tracking the development of U.S. cyber policy and its implications for transatlantic cooperation on cybersecurity. Her position in the Embassy also supports the UK's multinational engagement and the departments included in the UK's national cyber program.
Prior to joining the Foreign and Commonwealth Office, Woodbine was Private Secretary to Francis Maude, Minister for the Cabinet Office, where her portfolio covered the UK Government's Digital Strategy, ICT reform, cybersecurity and civil contingencies. Before joining the Cabinet Office, Woodbine was the Assistant Private Secretary to the then Minister for Security, Baroness Neville-Jones, working at the Home Office, where her responsibilities comprised numerous national security topics, including cybersecurity and counter-terrorism.

Moderators

Loch K. Johnson is the Regents Professor of Public and International Affairs at the University of Georgia, as well as a Meigs Distinguished Teaching Professor. He is the author of over 200 articles and essays, and the author or editor of twenty-eight books on U.S. national security. He has a long record of service in senior positions in the U.S. Congress and in the Executive Branch in the area of intelligence policy.

The recipient of numerous awards for his scholarship and service in the field of national security, Johnson currently is a consultant to several government and civic organizations as well as a senior editor of the international journal *Intelligence and National Security* (London).

Timothy L. Meyer has taught international law and international trade at the University of Georgia School of Law since 2010. Before joining the faculty, he worked as an Attorney-Adviser in the U.S. Department of State Office of the Legal Adviser, where he represented the U.S. in commercial arbitrations and real property transactions and in negotiations with foreign governments on diplomatic law issues. His current research examines the design of international legislative institutions, the fragmentation of international energy governance, and the relationship between international energy institutions and climate change institutions.

Terms and Abbreviations

CNCI: Comprehensive National Cybersecurity Initiative

CNDSP: Computer Network Defense Service Provider

CSRIC: Communications Security Reliability and Interoperability Council

DHS: United States Department of Homeland Security

DISA: Defense Information Systems Agency

DOD: United States Department of Defense

DOJ: Department of Justice

DNI: Director of National Intelligence

ECPA: Electronic Communications Privacy Act

FCC: Federal Communications Commission

FISA: Foreign Intelligence Surveillance Act

FTC: Federal Trade Commission

GCHQ: Government Communications Headquarters

HVAC: Heating, Ventilation and Air Conditioning

IANA: Internet Assigned Numbers Authority

ICANN: Internet Corporation for Assigned Names and Numbers

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

ISAC: Information Sharing and Analysis Centers

ISO: International Organization for Standardization

ITU: International Telecommunications Union

NERC: North American Electric Reliability Corporation

NIST: National Institute of Standards and Technology

NSA: National Security Agency

OSD: Office of the Secretary of Defense

SEC: U.S. Securities and Exchange Commission

USTR: United States Trade Representative

WSIS: World Summit on the Information Society