Beyond the Headlines
January 27, 2014
Washington, DC

Jane Holl Lute
The Council on CyberSecurity

David Sanger, Moderator
The New York Times

Making Sense of Cybersecurity

Ambassador Ritva Koukku-Ronde: Ladies and gentleman, distinguished guests, dear friends, it's really such a pleasure to see you all here this evening. This is actually the first seminar we have hosted this year. We are celebrating the 20th anniversary of this embassy—green embassy. We were the first embassy to have led such certification. [*Applause.*] And this is the most energy efficient embassy. We are, of course, particularly pleased that Women's Foreign Policy Group suggested this seminar at the Finnish Embassy. Thank you very much for that. I would also like to thank the excellent relations we have with the Women's Foreign Policy Group. I have found it very, very useful and also a very pleasant group. I am a member. Some of my colleagues are also and we have enjoyed very many informative, but also very pleasant events. And I would like to also congratulate the new Chair, Ann Stock, for all the work you have done and I am sure that you will be chairing well in the coming years. Thank you for coming, really, and bringing this hot topic to this evening's discussion. I am sure that we will have a very interesting discussion with two specialists that I am very happy to meet—President and Chief Executive Officer Jane Holl Lute and also David Sanger, who is a special editor specializing in these issues. And we have, of course, from the embassy also some of my colleagues are here. I don't have my spectacles, [*Laughter.*] but I see at least our defense counselor, Heikki Savola, is here and our counselor, Riina-Riikka Heikka, is here. And of course, thank you very much Tarja Thatcher, our social secretary, who is of course somewhere around here. If there are any questions later on, please contact one of us.

I will take this opportunity to say something—for two minutes—something about information technology. I cannot help myself. Information technology, the internet, and social media have created a super cyberspace world that opens up huge opportunities for civil society, private sector, as well as governments. Everyone should be able to enjoy these advantages. However, cyberspace can also be harnessed to serve negative purposes. An example of this is hacking and phishing daily in the news. They have increasingly serious repercussions for individuals, businesses, states, and the society in general. Unauthorized surveillance on the internet and other telecommunications for security purposes has highlighted the question of the right to privacy. At the same time, freedom in the online world is under pressure with attempts to control and limit online communications. Freedom of speech and expression should be respected equally in cyberspace and offline. Privacy and cybersecurity do not exclude each other. They can be mutually reinforcing. In order to improve cybersecurity, it is important that all citizens, enterprises, and authorities are able to trust the same processing of digital information. Within what is considered multistate holder corporations, in spite of both at the national and international levels, it was also emphasized in our national cybersecurity strategy from last year. Cybersecurity has become a more and more reported issue also as part of security policy. Due to the borderless nature of cyberspace as a global commons, it should be addressed through broad multilateral cooperation. Development of cybersecurity, the European Union, as well as many international organizations like the United Nations, NATO, OECD, and OSCE are very important

venues. The European Union is increasingly active in the field of cybersecurity and it is also engaging cooperations of other countries. It goes without saying that we look forward to cooperating with our American friends in order to be able to respond to various cybersecurity challenges. Finland—we are a small, capable, and cooperative country. We have excellent chances of rising to the front in cybersecurity and we have an extensive knowledge based on strong expertise and a long tradition of close cooperation with corporations built on trust, as well as interpersonal collaboration.

With these words, I would like to give it to Ann Stock, the new chair. [*Applause*.]

Ann Stock: Thank you Madame Ambassador for hosting us at this beautiful, beautiful embassy. We're delighted to be here again and we always enjoy your hospitality. Since arriving in Washington as you mentioned, you have done so much with the Women's Foreign Policy Group and we appreciate that. On a personal note though, I would like to say one thing. I met the Ambassador at one of the first State Department luncheons after she presented her credentials to President Obama. And we sat next to each other and we talked about all kinds of issues. But as everyone in this room can well understand, we bonded on one very important state secret. Where in Washington did I get my hair cut? [*Laughter.*] Anyway, Madame Ambassador, we have enjoyed our friendship very, very much. Let me also give a warm welcome to the other women ambassadors and diplomatic leaders that who are here. We're always delighted and honored to have the diplomatic community with us. As Ritva said, I am Ann Stock, the new chairwomen of the Women's Foreign Policy Group and I have several of my board members with us tonight—I see Marlene and of course Patricia Ellis, our president. I would also like to recognize McLarty Associates, one of our Corporate Advisory Council members. I have a couple housekeeping things to do before we introduce our speakers. I'd like to thank the audience for being here on this frigid night. I must say Madame Ambassador, if it stays this cold; you're going to have to give us some tips on how to stay warm. Before we hear from our speakers, let me mention two upcoming events that are very, very important to us. On February 5th is our annual Mentoring Fair at GW. This is a very important night because we work with all of the young women in foreign policy—and some of the older ones too—so please make sure you mark that down on your calendars. And February 12th is our next Embassy Series event, this time with the Ambassador of Singapore. So add that to your calendar.

And now it's my great pleasure to introduce our speaker and moderator and give you some of the highlights of their fabulous careers. Their full bios are in your programs, which I think are right in front of you. Tonight's topic, cybersecurity, is extremely timely and we have two of the world's leading experts on the subject, Jane Holl Lute and David Sanger. Currently, Jane is president and CEO on the Council on CyberSecurity. Most recently, she served as the deputy secretary for the Department of Homeland Security. And I read her job description and it was absolutely amazing. I'm going to give a little bit of description of what she did on a day-to-day basis as the chief operating officer. She managed the Department's efforts to—listen to this—prevent terrorism and enhance security, secure and manage our nation's borders, enforce US immigration laws, strengthen national resilience in the face of disasters, and ensure our nation's cybersecurity. That's a tall order and if it's not enough to keep you awake at night—which she said it did not and I want to know more about that. From 2003–2009, Lute was the UN's assistant secretary-general responsible for providing on-the-ground support for UN peace operations worldwide. She served on the National Security Council under two presidents, George H.W. Bush and William Jefferson Clinton. She has also had a distinguished career in the US Army. Clearly, this woman thrives on high-pressure jobs and loves it.

Our moderator David Sanger is *The New York Times'* National Security Correspondent for over 30 years. He has reported from New York, Tokyo, Washington on all the hot topics of the day—foreign policy, globalization, and nuclear proliferation—all in the news daily. Please join me for what will promise to be a wonderful conversation with Jane Holl Lute and David Sanger. Thank you. [*Applause*.]

David Sanger: All right, I'm just here as the moderator so I'm happy to hear Jane on all this. Here's the way we're going to go—Jane's going to talk for 7–10 minutes and I am going to then ask some questions and then we'll open it up to all of you. If I rudely slip out a little bit early, it's because I have a

school meeting which I am going to be late to in any case. It's not out of protest of anything that Jane said—though we could pretend it was!

Jane Holl Lute: This is an audience that gets putting family first. [*Applause*.]

Sanger: What's left out of Jane's bio is that she's the mother of a champion speed skater, ranked number one for girls ten and under. If you had to grow up at the Lute household and hear all the threats that you would hear about during dinner time, you would have learned to move that fast too. [*Laughter.*] Jane's husband, Doug Lute—known to many of you as the Ambassador to NATO—was the president's top advisor for Afghanistan and Pakistan. And years ago, I heard Jane utter the great line, "Yeah, when Doug messes up at the office, I have to go clean it up at Homeland Security." [*Laughter*.] So with that, let's let Jane start and then I will ask a few questions.

Lute: Thanks David, and thanks Ann, and Pat, and Ambassador very much for hosting us and for allowing me to come into your home. I can't believe it's 20 years—it seems like it's two. I remember when it was going up and it was green—and we thought, really? And really, it's gorgeous. Thank you. I'll just make one slight change, if I might, to what Ann asked for you to turn off your phones. I was a single mom for ten years. Please do not turn off your phone. Put it on buzz. I couldn't always do presents, but I was always available. And so I don't want anyone not to be available in life. But thank you, I know it was a courtesy to me and I appreciate that.

So what I thought I would ask when Pat gave me this very generous invitation—there is not a hotter word in the English language right now than "cybersecurity." My experience though, is that most of us have no idea what it means. We don't know what we are supposed to do about it. We don't know how to think about it. And we're not sure when we do grab on something that we recognize or understand that we're right—because most of us do not speak dolphin. [*Laughter.*] And it seems like the people who really do "do cybersecurity" and understand it, are speaking dolphin. Whenever you ask the simplest question—why does it matter? What's important about it? Is it changing anything? Is it changing nothing? Is this just the next, sort of, big thing enjoying its fifteen minutes of fame and we'll be onto something else? No, this will change everything. The internet is changing everything. Everything. It's changing what the word technology means. Technology is the word that was invented by somebody to precisely describe when human beings put tools in their grasp. That's what technology means. And now, it's precisely what we use to describe things that exceed our grasp. It's high-tech. I don't get it. I'm leaving this to the specialists. We are leaving this to the next generation. Most of us don't get it. I talk to my daughter Cameron, who's nine, and very commonly she'll say, "Here Momma, let me." I don't let nine-year-olds do anything, but I do hear. So, I want to talk about that. Where have we been? Where are we going? What role should the government play in cybersecurity? What's happening in the world that's even changing the role of governments in our lives? That's what I thought I would talk about.

In order to talk about it, I think I want to lay out on the table what I see to be two important, intersecting and countervailing trends. One is the trend of growth. And another one is the trend of decay. The trend of growth is one that I call the "global cyber awakening." It is the social consequence of the penetration of the internet. It's not the same thing as the penetration of the internet. It's the social consequences of that penetration. In 1995, about 6 million people were online. When did the World Wide Web become broadly available? On August 6, 1991. In 1995, 16 million people were online. Today, nearly 3 billion people are online. The internet is connected to about a third of the world's population. What else can you say that about besides soccer? [*Laughter.*] In fact, there are only five things that I can think of that claim the active affiliation of a billion or more people on the planet. Only five things that claim the active affiliate of a billion or more people on the planet—being Catholic, being Muslim, being Indian, being Chinese, and being on Facebook. And Yahoo is not far behind. The active engagement. And really, only Facebook knows it user population, certainly compared to any of the others in that category.

What are we saying? We're saying that everything is changing. There is a global phenomenon of cyber awakening where people are more connected, more aware, more informed, and less alone than ever

before. And this is for a population that is already healthier, wealthier, more educated, more mobile, more active on issues that affect their lives politically, economically, and socially than ever before in history. This is an extraordinary phenomenon of growth. Eric Schmidt and Jared Cohen of Google say that by the year 2020, the entire world's population will be connected online. I'm not sure that's right, but it doesn't matter—the number's a big one. This trend of growth is intersecting with the trend of decay. That trend of decay is captured in the near total lack of trust in public sector institutions. And this is true around the world. I was the lead negotiator for the United States with the European Union on a major, some say last, data sharing agreement called Passenger Name Records (PNR). All my European colleagues are bobbing their heads. It was a big issue in Europe. Something less of an issue in the United States, but it was a big issue between the United States and the European Union. What I can tell you is that everywhere around the world and everywhere certainly that we travel, people were angry. They were angry, but they didn't know why. This was not purpose-driven anger, in my view. In purpose-driven anger people kill each other. This is anxiety-based anger. We don't trust the banks, we don't trust business, we don't trust the media, and we don't trust the markets. Some say we don't trust our governments and on and on and on. No public sector institution, from our religious institutions to our political institutions to our economic institutions, has our overwhelming trust of individuals. And this is true globally. I think the anger that we're seeing in the public is anger that stems from an anxiety that we're not sure we know how to architect trusted institutions anymore in public space. So we have a dramatic trend of growth, with global cyber awakening, and a dramatic trend of decay, which is an increasingly lack of trust in public institutions.

So why does this matter when we're talking about cyber and cybersecurity? How many of you believe in an open internet? Let's pretend you all raised your hands. [*Laughter.*] Okay, I do. I believe in the power of an open internet. To me the greatest threat to an open internet is the lack of security. There's nothing you can do 25 years after a book was written called *The Cuckoo's Nest*, which is a famous book about a cyber intrusion in 1989. There's nothing you can do in cyberspace. You can't plug in your machine. You can't get online. You can't stop, shop, chat, do anything confident that your information and your identity are not at risk. It's completely unacceptable. It's completely unacceptable. Why? Because our reliance is so extraordinary. There's not a modern society in the world today that does not have extraordinary reliance on the internet. The governments, for delivering the services of governments that they do—what are those services? Security, well-being, and justice—the rest is commentary. There's not a government in the world that doesn't rely on the internet for delivering those services. And not one of us—I was thinking about this—we are kind if a distributive family distributed around the globe, but if you just talk about my husband, my youngest daughter, and my son, we have five phones, three computers, two laptops, five tablets, seven iPods—oh my God, seven…I better not tell my husband! Four Apple TV devices and six e-readers. Six. And that's us! Those are the human beings at our household—no I'm not even talking about our cars, which have their own connectivity. And you are all like me. I was at a meeting recently and one of my colleagues held up a phone and said, "You are all threat to me." I said, "Oh please, exhale okay?" [*Laughter.*] Or actually don't exhale because when you walked in the room you were coughing and you were a threat to me. Though why the drama over your electronic devices? Your threat began with the intake and outflow of oxygen, through whatever is going on in your head right now. So let's just take a deep breath and understand that what we say the biggest threat to an open internet right now is a lack of security. And the biggest implication of that is because of our reliance on this. Are we vulnerable? Yes. I mean, we are vulnerable to the weather. We take snow days. We're going to be taking cyber days soon. Maybe your organization has already taken a cyber day. Right? "Because the system is down." Might as well go home, because there's nothing you can do—you can't even place a phone call anymore unless you get on your mobile device. So I predict the existence of cyber days in your future. "We're closing for a cyber day. We're upgrading our system. People work from home." Our reliance is enormous, our vulnerability is equally enormous.

So who's responsible to protect us? Who's responsible for our cybersecurity? Now typically, security is something that societies assign to their governments to handle. We want safe streets—governments, you run the police. We want a safe country—governments, you run the military and you make the laws.

Security is something that societies usually assign to their governments to handle, and we'll leave aside the commentary on how well they're doing. But it is kind of a consensus assignment to governments, and governments are used to being the monopolists in security space. They are in all space, except cyberspace. Not only are they not the monopolists in providing security in cyberspace, but we haven't given them that assignment yet. We haven't said to governments, "Where are the laws? Where's the technology? Where are the techniques? Where is the staffing of security in cyberspace?" And why not? Well, why aren't we? As we begin to answer that question by saying why are governments the monopolists of security and physical space? Because they have the power to protect. Governments are the legitimate authority over the consolidated control of legality. It gives them the power to protect. Okay, well let's look at power in cyberspace. What power matters? Well if you look at the powerful actors in cyberspace, you run out of fingers—most of us, all of us—before you get to the first government. The most powerful actors in cyberspace—look at any internet depiction on the web, in terms of volume of transaction influencing your life and control over your information and identity. You run out of fingers before you get to a government. It's Google, it's Youtube, it's Yahoo, it's Facebook, it's all the things you know and none of them are governments. So what's the power that matters in cyberspace? It's the power to connect, not the power to protect. So how are we assigned responsibilities for cybersecurity if that's true? What have the big breaches in data security and data protection taught us over the last several years? Target has responded to its big data breach by mounting an impressive consumer education outreach program to teach consumers about problems with spear phishing, etc. Although one of my colleagues said to me the other day, "They're solving a problem but not the one that caused the breach." Consumers did exactly what they were supposed to do during the Christmas season, which was shop and buy and use your credit card. Now, do we need better systems? Yes. The Europeans have chip and code and the second factor authentification—should we go to that? Yes, we should go to that. Let's just go to it. Do we need a big international debate over it? We don't, frankly, we can't have one. But is that the state of the art in respect to consumer protection?—of course it is. So we can move to that.

So how do we distribute responsibilities for security in cyberspace? What should your responsibilities be? Mine? What should the manufacturers' responsibilities be? Is there anything that we can do that would have prevented a Target data breach? Is there anything at all? The answer is of course there is. And the answer is *cyber hygiene.* Are there three or four things that you can do, or that any enterprise can do, right now to measurably and materially improve their cybersecurity and reduce their cyber vulnerability? The answer is yes! There's something called the "Twenty Critical Controls" that was invented by a colleague of mine, Tony Sager, when he was in government. At the time, there were ten and the price of comprehensiveness is inclusivity so they grew to twenty. But the top four of the twenty critical controls will prevent 80-90% of all known intrusions. The top four of the critical controls will prevent 80-90%—white-listing your hardware, white-listing your software, limiting administrative permissions, and real time patching and monitoring of your system vulnerability. Hygiene will prevent 80-90%—it really is the equivalent of brushing your teeth, flossing, and visiting your dentist twice a year. It really is. And people say "Oh my goodness! If that's it, then why aren't we hearing more about this? Why aren't people doing this?" Well in part, the answer lies in three reasons. Number 1: there are those who oppose the notion of hygiene. There are those who say each situation is unique and everybody needs a unique solution. Really? I don't have a unique toothbrush…I'm going to go and buy whatever's on the shelf. It kind of works, most of the time. And there are others who say that these four measures—those twenty measures are fine—but they don't protect against everything. Neither does washing your hands. But I won't let my daughter out of the house without doing it every morning. They say oh no, no—you really need to address the unique threats that are presented to you. Well I don't say to my daughter every morning, "Okay, now you are going to encounter meningococcal this and streptococcal that. Wash your hands! I don't read her the blotter report from Arlington, Virginia. I say don't talk to strangers. And I don't diagnose for her the ways in which people navigating their vehicles on the streets could cause a hazard. I say, "look both ways before you cross." And then, over and beyond that, I say this is a dangerous corner, this is flu season so let's get a shot, and so forth. There is basic hygiene that we could use. Part of the reason we don't is because we think industry and as community is developing there's resistance to hygiene for those two reasons—it's not comprehensive

enough and those who say you need a solution unique to you. And to that I say bologna, bologna. Hygiene will prevent 80-90% of all known attacks. Every enterprise should be doing it now and every consumer should be demanding that every business they deal with has cyber hygiene in place. Every business should demand those manufacturers ship systems, equipment, and boxes with the systems activated and turned on. Is that expensive? I don't know—compare a toothbrush to a root canal. You do the math. The second reason it has not been advocated is because governments, up until recently, have treated major cyber intrusions as an intelligence problem. Businesses have treated major cyber intrusions as the cost of doing business and a nuisance. All that is changing and you are present at the creation moment. What's at stake? The future of the internet as we know it. And I don't want you to be alarmed and I don't want you to be scared, I want you to be prepared. I was a Jesse Jackson fan earlier in my life. [*Laughter.*] And so, if we're just thinking about cybersecurity and trying to make sense of what one of my colleagues calls the "fog of more"—more this, more that—there's basic hygiene you can do and you can do it right now. With that I went way over ten minutes and I apologize and David, I'll turn it back to you. [*Applause.*]

Sanger: Well thanks, Jane. That was great and probably the best explanation of how one practices "safe cyber" that I've heard in a long time. Let me try to unpack a little bit of what is the responsibility of the government, what's the responsibility of businesses, and what's the responsibility of individuals, as you do this? And all of these get to the issues of trust that you mentioned before.

A year ago, before the NSA went into the headlines for reasons it would have preferred not to have. Its leaders talked about having basically filtering of malware that was coming into the United States, which would not solve every problem by any means, but big filters that would sit where the internet service providers watch the data coming in, usually through the same fiberoptic cables and satellite connections that we all have phone calls on. And the idea was that you could watch the metadata as it was coming through and look for things that were coming from known sources of attack, say in China, in Russia from criminal groups. All those things that you see your friends at Homeland Security collect data on threats and that would be level one. The next level down would be the type of corporate security issues that you discussed. Target is now coming around to, but many other financial institutions have done. Then at the third level are the individuals. And only if you had a sort of layered, resilient defense like that could you be successful. So now you go back to the NSA and you say what happened to that plan? They'll say, well, we've got a trust problem. The problem we have is that no one thinks that any filtering we did, we would use only for filtering malware. They think we would use it to listen in on phone calls or read emails or something like that, even if it's not our intention. That's our problem. So, tell us a little more about what level the government's got to go do this, can the government really have a role or has the Snowden revelations made it more difficult for the government?

Lute: I'm thinking about how to best respond to this question—it's a good one. It's one everyone is asking themselves right now. Is there a role for defense in cybersecurity? The answer is yes. Does cybersecurity equal defense? The answer is no, in my view. How should we think about it? Is the national security paradigm the best paradigm to understand cybersecurity? Or is there another paradigm or way to think about it? One of the things that struck me when I was at Homeland Security, and I spent my whole career up until that point in international security and in national security. And so when I came to Homeland Security it was an entirely different model. It took me a while to puzzle through it. But I describe it to colleagues as follows: national security is strategic, it's centralized, and it's top-driven. Homeland security is transactional, decentralized, and bottom-driven, driven by the states, localities, and communities in the United States. It's not unity of command like national security. In homeland security, it's unity of effort. Nobody's commanding anyone. It's not need-to-know, which is the national security model for sharing information. It's duty-to-share in homeland security. It's a very, very different model of understanding security. When you think about the internet, do you think that it's strategic, centralized, and top-driven? If you do, then we're going to need to spend a little extra time afterward. [*Laughter.*] It's not, in fact, it's shockingly decentralized, disaggregated, and informally-driven. Some of the most important individuals who maintain the functioning, connectivity, and

openness of the internet, you might not allow in your homes. It's a shockingly informal network that's very effective and brought us the internet that we know today. The one that they're advocating—the open internet and the multistate holder model where you have governments and non-governmental organizations and civil society fully represented—speak about. So to your point, David, my charter over the last four years was not to think of cyber defense of this country, but to think of cybersecurity of this country. And so it was not a centralized, perimeter-focused, echelon on a defensive model. It was about how we should distribute responsibility and ensuring the security of your information and your identity when you're online. What responsibilities individual users should have, you ask. Can you go online and do anything you want and then complain when somebody is papering public wall space with things you've posted on your social media sites? Really, you're surprised? I mean what responsibilities do enterprises have? Again, Target has launched a major campaign to educate consumers and that's an important and valuable contribution. Is that what went wrong in the Target breach? No, it's not. So what responsibilities do they have? I think that what we're talking about with these top four critical controls are a minimal standard of due care that you're owed. Do you know what's on your network? Do you know what's trying to run on your network? Do you monitor it and have a sense of its health every day? And are you limiting those who have administrative permissions who can go in and do whatever it is they want to do, including bypass your security systems. So, I think of cybersecurity as a distributive responsibility. I think of it more in terms of protection than of defense. Is there a role for defense? There is a role for defense. Are people now questioning the role of government in the wake of the Snowden revelations? Of course they are—I'm detecting a bit of a generational difference, though, in that questioning. There's a number of very senior people, my generation perhaps—ten years younger and older, that say what he did was outrageous. What he did was outrageous. He violated the trust—the trust that I have in kind of a family business. Trust that my husband and I have honored in our combined case of almost 70 years. There's a younger generation that feels much more ambivalent about what this means because of what it has revealed. But this is causing us to think differently about the role of government in our lives in cyberspace and it's permeating every aspect.

Sanger: That's an interesting way to think about it. We like to think of our government as concerned about our cybersecurity, concerned about the defense side of this, concerned about teaching hygiene habits. But, we know that a lot of the money the US government spends on cyber, it spends on offensive cyber. I've read that we've been responsible for some cyber attacks used for national security purposes. I've written a little bit about that as well. And yet it's something that the US government doesn't discuss much, but it gets again at the trust issue. The President himself was concerned during America's Iran operations that once it was evident that the US was using cyber weapons; it would be used as a justification for other states, other groups to go off and do cyber attacks, even if the motives were far less pure. You saw a little bit of this in the President's National Advisory Committee report for the NSA, who said that the US should limit its use of software flaws known as "zero days." That it should strengthen encryption, not look to weaken encryption so that even if we had to take a hit on our offensive capability, we seem to be on the team of defense. Tell us a little bit about that tension within the government.

Lute: There's no question in my view that there have been certain effect of recent revelations and developments. One is the acceleration of encryption and the provision of encryption, which some say is long overdue. I'm not a technologist, you know, the voodoo that they do in cyber technology is really serious and interesting stuff. I don't pretend to understand a lot of it. But what I do know is—as someone who has run a very large operational organization—is that our reliance on IT is high. And having been in the government and involved in all the conversations in the last four years that I was the number two at Homeland Security, we were trying to figure out and narrate the appropriate role for government for cyberspace and in providing security to our populations. It is a well-settled competence of government that you protect your populations from their vulnerabilities. We are vulnerable in cyberspace, seriously vulnerable. That's why everyone has a role to play. I think, David, that there has been a major, and in my view disproportionate, occupation with the high-end, super sophisticated, frankly low payoff measures for cybersecurity. I call this "cyber couture." Everyone is about this cyber couture, which is up at that designer end of extreme expense, capability, and solution. Frankly, in my

view, it's not scalable and generates a relatively low payoff. I mean, I just spoke to you about basic hygiene which prevents 80-90% of known attacks. And frankly, most enterprises are already paying for that capability and they may not be getting it. So I'm telling you right now if you're not getting whitelisting of your hardware and software and the ability to limit your administrative permission, and realtime patching and monitoring of your networks, stop paying!

Sanger: I'm going to stop you to define your phrase—I'm not sure that everybody here would know what whitelisting or what patching is.

Lute: Know what's on your network. What is connected to your system? Do you ever plug in a device like an iPod and it says, "We have detected a device?" Is it possible to do that for all the systems and enterprises? Yes, it is. Will it take some time? It may, depending on the complexity of the network. But whitelisting is essentially knowing what is connected to your network. When you whitelist your software, what's running or trying to run on your system? Do you want it to run? Oh, Popeye's Black Arch is trying to run on your system. Is that okay with you? No, it's not okay. I ran into my daughter's room the other day asking, "What is Candy Crush and why do I keep getting texts about the next level?" [*Laughter.*] So, that's what whitelisting software is. What is realtime patching and monitoring? Let's get the machines in the game, for goodness sake. Let's automate what can be automated. Let's have systems in place that are constantly monitoring your networks and the devices that are attached and see what's trying to enter—look at the malware from the system database—prioritize the protection, deploy those protections, issue reports so you know the state of health of your IT system at any time. Here's what I believe—I believe that my colleagues and I can tell the reliability of an enterprise simply by looking at their cybersecurity posture. The viability of an enterprise, simply by looking at its cybersecurity posture. I can tell you what it's doing with its intellectual property, I can tell you the state of health and robustness of its IT system, and I can tell you, probably within a reasonable approximation, how well its complying with the overarching rules and regulations such as they exist currently. So when we say limited administrative permissions, essentially—do you know who has access to bypass, override, or circumvent the security settings of your system? Do you know? If you don't—I mean are you handing out your password? If you have, you've just given away the keys to the kingdom—your IT kingdom. That's what those mean.

Sanger: I was glad that you said before that we would all end up taking "cyber days." This summer at *The New York Times* actually, we took a cyber day. Courtesy of the Syrian electronic army, they came in and closed down our entire website and we came up with this really astounding solution. We took all of the news from the day and overnight we printed it on paper and then we drove around and we dropped it on peoples' doorsteps. [*Laughter.*] It was a remarkable invention, which takes me to my last question before we go to everybody's questions. There are a lot of bad nuclear analogies that happen in cyber. Back in the days of nuclear arms races, we used to say that if there was a nuclear war, it would bomb us back into the Stone Age. If we had a full outbreak of cyber war, based on what you said before, it might bomb us back to early August 1991. So I agree, the outfits would look pretty bad, the music might not be great, but what does that tell you about how limited the damage might be?

Lute: Someone asked me the other day, "Oh my god, what would happen to every bank if there was a major cyber attack?" I said that they would open their doors. [*Laughter.*] To your point, but, everything is different now, because of the internet. We're connected, we're used to being connected, we like it, we have near instantaneous access to the information that what we need. The companies that are powerful in cyberspace are powerful because they harness the magic of data liquidity. And they get it. And we want it, we like it, we like the concept of data liquidity; we know what to do with getting information where it needs to be when it needs to be there. It's empowering and it's changing everything. So I think on the one hand, David, there are those of us who remember what life was like 22–23 years ago before the internet. Eugene Kaspersky said to me that we are the last generation that will take any joy out of the internet—because we remember what life was like before. Not all of you can shake your head, okay? [*Laughter.*] I'm looking at you—I've got daughters your age. [*Laughter.*] So I mean there is something to that, but everything has changed, including the role of government in our

lives. Think about it—don't we expect governments to provide security, well-being, and justice? And there are a lot of people who go online for security and make their cause public. There are a lot of folks online for their well-being and to affiliate and to understand and learn. And there are a lot of people who go online for justice. Everything is changing. So what role will we assign to governments? I think that we are on a cusp of a new age, a cyber age—whatever anyone wants to call it. I think the answers to your questions—what if you can't drive? What if your vehicles don't work? What if there's no electricity? No connectivity? No information? No way to call? Would we cope? Yeah, I was in New York City during the blackout of 2003 and we coped. [*To David Sanger*:] You were there. But I think no one wants to go back to that.

Sanger: Great. So let's go out to questions. We'll start right here with Robin

Question: My name is Robin West and I'm highly in suspect. [*Laughter.*] I'm with CSIS. There's a great deal of discussion about the role of the government. My question, particularly in light of the Snowden disclosures, there's this notion that government is a threat and the government is not benign. What nobody discusses is the role of the private sector. Is Google benign? I mean, they're making billions of dollars taking information from us, which we're providing them unknowingly and selling it. And to whom are they selling it? How is it being used? I just have no sense that these are just the little sisters of charity out there looking out for us. [*Laughter.*]

Sanger: Another way to put that, Jane, might be that we get upset when we think that the NSA might have computers that are looking for key words in our emails. But, I write a lot about Pakistan and I get all these ads on the side of my Gmail that say, "Looking for a Pakistani bride?" [*Laughter.*] Not really, but we get more upset when the government does this than we do when the private industry does.

Lute: Sorry! Different rules, I mean Google's not government. Is Google powerful? You bet it is the number one internet site—go on any map of the internet. The biggest blob you see is Google by far. But it's different rules. Why isn't the government acting? Why isn't Google acting like the government? Why isn't Google subject to the same set of expectations? There are rules that apply to Google—it's called the marketplace. Market's a wonderful mechanism, except when it's not, and that's when we see social intervention in market forces. We're seeing governments move into the internet right now. Move into cyberspace. We're seeing that cybersecurity is government's best play, because governments are used to being the biggest players in security space. It's not the only play. There's governance—a whole question we didn't talk about—internet governance, and how that will play out and who will be responsible for maintaining the end-to-end technical connectivity of the internet. We haven't spoken about it. Governments are making a big play that it be them, in the first instance. So, I hear this a lot. Why are we angry at the NSA? We should be angry at Facebook, god knows what they're doing with our information, etc. Different rules. And it has, up until this point, been okay with us that it's different rules.

Sanger: Well, you know even if we don't read them we agree to some terms of service when we sign up for Gmail. I don't remember signing any terms of service with the government about my internet use. I do with Google and Yahoo. I might not like them but I sign them anyway.

Lute: There are countries around the world who control citizens' access to the internet. It's not universally the case, but in this society we have not assigned government the responsibility for cybersecurity. And you mention the nuclear analogy. I spent a long time in the military, I'm married to a soldier, I am a proud, retired member of the United States Army. I don't think military analogies are the analogies we should use in cyberspace. I don't think it's a war zone. Do I think it's contested space? It's contested space, absolutely. Even if it weren't contested space, I don't think we could manage it as a war zone. I kind of think about the responsibilities on the internet the way I think about driving. Do you drive? Of course you do. Okay, if you don't drive have you ever been a passenger? Yes. Have you ever been a pedestrian? Of course yes, so I've got you all. You've all been drivers, passengers, and pedestrians. You know what your responsibilities are? Do you have responsibilities that you expect

from the automotive manufacturer? The secondary parts makers? The towns? If everybody knows it's a bad corner, let's put a stop sign up. There are rule to being able to drive a car, to being a passenger, and being a pedestrian. This is really dating myself, but some of us remember—when I was a kid there used to be this great little song. "Don't cross the street in the middle, in the middle, in the middle—in the middle of the block. Really, that's how old I am. Don't cross the street in the middle of the block. Wait till the light turns green. That's how far away we are from pedestrian observance of good normative behavior in complex social settings like cities. But my point is—what role does government play? Does government drive our cars? No. I used to say, "Did the government build your cars?" I lost that one for a little while. [*Laughter.*] But the answer is basically "no." And do we all seem to get where we're going? In billions of transactions and trillions of potential transactions every single day and most of us seem to get where we're going, relatively safely, most of the time. And when something goes wrong, we know where to fix responsibility. That's where I think we should head in cybersecurity.

Patricia Ellis: Even if we are very religious about our cyber hygiene, what about the other percentage? What about all these non-state actors, governments, and others who are criminals, whether they're from China, Russia, or wherever they're from, who are determined to do systems in and to do bad things? I mean, how are we going to deal with this and also if governments do get in, what kind of coordination can there be amongst governments? For example, I was just, in preparation for this evening, reading that France is going to be spending something like $2 billion to upgrade its cybersecurity function because it's been attacked so many times. So how are we going to coordinate if one country does it? Is that going to be helpful? You've worked a lot on multinational agreements so one—how do we deal with these terrible actors, non-state and otherwise, who sometimes we can't identify?

Lute: So I am going to repeat what I said before, Pat, because it really matters. Basic cyber hygiene—these four measures—prevent 80–90% of all known attacks. That's a big number by any measure. So the Australians conducted a test. 1,200 machines, 1,700 pieces of unique malware, no protection, control number one and control number two—they have a slightly different array of controls that they use—and when they got to the top four or five, you know how many pieces of malware got through? You know how many successful attacks there were? Zero. Basic hygiene. Let's at least make it hard for the bad guys. The significant attacks that we've seen lately have not been hard. We can make it hard.

Question: I'm Mitzi Wertheim of the Naval Postgraduate School, but how do I do the basic hygiene for my system at home?

Lute: There's a similar version of this, this is really designed for enterprises. But, do you know what's on your network? On your wifi network? You can. The tutorial we'll have to do afterward, I'm afraid, but do you know what's trying to run it? By the way, why aren't we insisting that manufacturers ship the systems with the controls active and working? We're in the equivalent right now, where we know seatbelts will keep you safe, but you better go down to the hardware store, measure your car for seatbelts, buy the right webbing, and install it yourself.

Question: But we need to understand that in order to demand it. This is the first time I've heard this.

Lute: I don't know what to say…

Question: Jane, you mentioned the concept of "cyber couture." What did you mean by that? You said something about high cost but low payoff. Are these things that intended to try and get at the 10% attacks that actually do get through the hygiene that Tony Sager doesn't get at?

Lute: I think "cyber couture" is this approach to cybersecurity that says everyone is a special flower, everyone needs it own unique combination of fertilizer, water, and sunshine that has to be individually tailored to you. I've had some disagreements with those in the industry who say, "Jane, hygiene is great but it doesn't take you the whole way." Got it. Brushing your teeth will not eliminate every potential for a

cavity; we haven't done away with dentists. But, we don't need to treat each of ourselves as if we are so unique that the only cybersecurity solution has to be personally designed. We can take the community consensus that has been established around these top four and say, "If you want to begin evaluating what you personally need, start by doing these four things and then see what marginal difference you made back to your 10–15%." It exists. But, why in the world have we allowed ourselves to have the conversation, in large measure, preoccupied with zapping packets in transit in cyberspace. The ability to do that as opposed to brushing your teeth, flossing, and visiting the dentist twice a year. That's what I mean.

Sanger: So we are running a little tight on time so we are going to take a question right here and one more over here and we'll just do two at a time.

Ambassador Marina Kaljurand: Thank you. My name is Marina Kaljurand and I am the Estonian Ambassador. Thank you so much for organizing this event. Jane, you are great. This is not the first time I have listened to you. I enjoy it very much. And Mr. Sanger, I have to say that your articles are impressive and I have also enjoyed your moderation. My question is to both of you—if it is okay to ask both of you? I would like to bring cybersecurity to the international level. We can't go into the details, I understand, but if you'll name priorities for the international community today, knowing that there are so different states, so different approaches, such a difficult time we're at. So if you'll name three priorities that the international community should pay attention to at the moment. Thank you

Sanger: And we have one over here from this gentleman.

Question: I'm Bruce Zagaris and I'm a lawyer. The question I have relates to the question the Ambassador first mentioned—the fact that we have a number of international organizations dealing with this problem. Just this last month, the General Assembly of the UN passed a resolution with respect to anti-surveillance and the interaction between counterterrorism and human rights. You yourself were at the UN, so what role should international organizations play with respect to cybersecurity in cybercrime, especially the UN.

Lute: Governments have been trying to figure this out. Every single government on the planet has been trying to figure this out—what's their role on the internet and what's their role in cyberspace. Out of 193 members of the United Nations, no two of them are doing the same thing. Not even deploying the tools that they have meeting their international organizations most effectively. So there is a big tussle over internet governance. I think there's a merging consensus that cybercrime is crime. They're giving the laws around the world an exercise in jurisdiction, in conflict of laws, and these other kinds of things that are very familiar to us who are lawyers here. The international organizations are not going to eradicate crime. I think Budapest went a very long way. But, Budapest was actually as much an exercise in governments voicing their way they're going to get into the internet governance game as anything else. So for those of you who do not know, in 2010 or 2011 there was a London conference called the Initiative of the British Foreign Minister that was followed a year later by the Budapest conference which circled around crime. It was followed last year by a conference in Seoul. There will be a conference in The Hague in 2015. This is governance moving into a position to be able to pronounce themselves on life in cyberspace and life on the internet. I think that we're seeing that. It's still striking to me that there is not a single issue on the planet that you get a 192 governments to agree on. I have no expectation that this issue will different, except that there is a need to act. They do seem to agree on that.

What should governments do? What should be their priorities? I think their priorities should be what governments do best, which is security, well-being, and justice. Security, I think governments need to focus on hygiene and narrating out to their publics the vulnerability and the way that hygiene—washing your hands is a universally understood hygiene measure and it prevents an enormous amount of problems and preventable diseases. Can we prevent? Yes, I think we can prevent 80–90% of known attacks. One of the really interesting things about cyberspace is that if we know about an attack, most known attacks have known remedies, unlike biology and other things in the physical world. Most cyber

attacks have known remedies. So I think priority number one for governments should be security, what we have governments for, and in that respect I think they should do hygiene. Well-being, I think this about harnessing the power of the internet, harnessing data liquidity to lift the circumstances of their population, to educate young women, employ young men, and really create the rising tide that lifts all boats. Justice, I'd like to say that justice speaks for itself, but there is a play that the governments and the internet and cyberspace in justice as well.

Sanger: I'll take a brief last shot here on your question and then I think we're out of time. You hear a lot of people talk about using the treaty model, again this comes a little bit from the nuclear age that fifty years ago we were able to move to an unlimited test ban treaty and so on, doesn't work in cyber because in the nuclear age there were an unlimited number of countries that had control over the weaponry. Here it's states, it's non-state actors, it's criminal groups, it's teenagers. I don't know about your household, but in my household teenagers don't sign treaties. Okay? [*Laughter.*] So, not likely to work. I think that if the United States could press where it was going before Snowden stuff threw it off, which was to come to some common understandings with the Chinese, then you would have two of the biggest cyber powers starting with some kind of model that as Jane says, is going to be different for every country. The difficulty is we don't even have a common language between us and the Chinese, forget the other 191, about what will even define cyber crime, cyber attack. You know we say we only attack in a case of national security to bolster our defenses. The Chinese obviously have a lot of operations that are going after intellectual property. To them, that is part of national security. We consider that to be cyber crime. So we don't have a common set of definitions.

The second big thing we all need to work on is attribution. In the nuclear age, you could sit in a big cave in Colorado and you could see where those missiles were coming from. Here, you probably can't because it's going through different servers and different countries. Coming in it's creating a bot net on Mrs. Smith's personal computer in some suburban Illinois community and if you blew up Mrs. Smith's house you'd have a real problem. So, we need to have a much better sense of attribution and we don't have that right now. It's getting better, but it's very slow.

Lute: Yeah, I think I would just take a very slightly different cut on this last question. I mean it's not the nuclear issue. If the broccoli is bad, we know where the farm is that raised that broccoli, right? I think we're actually getting better on attribution. A number of years ago, there was an issue called Code Red, which was a worm that was bedeviling lot of systems. There was a guy in the Midwest at some hospital that actually tracked it and everybody said, "Well that's really cool." And it was the civilian sector that mobilized themselves and got together and organized to address this problem. It wasn't the government at all. So governments have had to confront the reality that they're not monopolists here, they're market participants and they're struggling with their role. But they're also, I think, value added because they represent a social consensus when we think that none of us can agree on anything. So it's in our interests, as they move increasingly into the role of cybersecurity, a subset of which again is cyber defense, that we all give them the assignment we really and truly want them to have.

Sanger: Well thanks, Jane. This was great. And the last word goes to Ann.

Stock: Madame Ambassador, thank you so much for this timely, important conversation and for your hospitality. We will be back. [*Laughter.*] And also, let's give another round of applause for Jane and David on a scintillating conversation and to the audience on good, tough questions. Stay warm and we'll see you February 5th for our Mentoring Fair.