THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2016

CYBER'S ROLE IN AMERICA'S SECURITY ARSENAL

Doerr-Hosier Center
Aspen, Colorado

Thursday, July 28, 2016

LIST OF PARTICIPANTS

EVAN PEREZ
Justice Correspondent, CNN

VINNY SICA
Vice President, Defense and Intelligence Space Ground Solutions, Lockheed Martin

STEVE GROBMAN
Chief Technology Officer, Intel Security Group

MICHAEL DALY
Chief Technology Officer, Cybersecurity and Special Missions, Raytheon

JOHN CARLIN
Assistant Attorney General for National Security

* * * * *

CYBER'S ROLE IN AMERICA'S SECURITY ARSENAL

(11:30 a.m.)

SPEAKER: -- continues. What role should cyber tools play in securing the nation both offensively and defensively?

Now everyday we see the impact cyber has on our national security and our global economy. Cyber terrorism comes through the exfiltration of intellectual property data, the attacks on the critical infrastructure, cybercrime and also the importance of securing our military government and civilian cyber networks, all of this of course moving at wire speed.

Now it's my pleasure to introduce our moderator for this session, Evan Perez. Evan Perez is a CNN justice correspondent based in Washington DC bureau reporting on legal, crime and national security issues. He helps lead a team that covers breaking stories ranging from the cyber attacks on Sony Pictures to the recent attacks in Paris, Brussels, San Bernardino and Orlando.

Before joining CNN, Evan led justice coverage at the Wall Street Journal. He began his career in Miami as a reporter for The Associated Press. He was born in Belize City, Belize and studied journalism at the University of South Florida. And with that, I'd like to turn this over to Evan to introduce our distinguished panelists.

MR. PEREZ: Thank you. Thank you very much for the introduction, appreciate it.

(Applause)

MR. PEREZ: And thank you all for coming. Obviously, it's a very timely panel to talk about some of these issues given what has been happening. I guess, we'll start by introducing the panelists here. John Carlin is the in-charge of all national security investigations at the Justice Department. Next to him, we have Vinny Sica, Vice President of Defense and

Intelligence Space Ground Solutions at Lockheed Martin. Steve Grobman, I did it right?

MR. GROBMAN: Did it right.

MR. PEREZ: Chief Technology Officer at Intel Security and Michael Daly, Chief Technology Officer for Cybersecurity and Special Missions at Raytheon. Thank you for joining me.

We'll start with the story and certainly the subject that is on everybody's mind right now and that is the hack into the DNC computer systems and the suspicion by some of the investigators that this is the work of Russian intelligence.

I guess I'll start with you, John. We've heard from both me and other reporters who are at this event have heard repeatedly from people that they were -- there are some hallmarks of this attack that mirror what was done to some of the government systems at the State Department, at the White House and that gives them some confidence that this appears to be the work of the same people.

Is there anything you can tell us about whether or not you've seen enough here to indicate that it is Russia or if someone else has done it?

MR. CARLIN: So I'm so glad you asked about what our approach is to national security cyber threats?

(Laughter)

MR. CARLIN: And the -- when I think about where we were two years ago, when I was at Aspen we talked about, I think it was two, maybe it's two -- three years ago now, we talked about applying a new approach to how we treat cyber threats that our national security. And by that I mean nation state, potential nation state actors or terrorist groups.

And we talked about applying an approach where we took the lessons we learned after 9/11 that led to the creation of my division, National Security Division. One of those was that prior to 9/11 we failed to effectively share information across the law enforcement and intelligence divide that it was a mistake that in part led to the death of thousands of people and that was something we couldn't repeat again.

And so in addition to certain legal reforms that allowed for the sharing of information across that law enforcement intelligence divide they also created things like the National Security Division, my division, where the lawyers who do terrorism cases, the prosecutors sit with the intelligence lawyers, sit with the policy lawyers that help the intelligence community out and sit with the lawyers that review certain transactions for national security risk.

And the idea is when it came to terrorism, we can no longer say success is a successful prosecution of a terrorist after the fact that success is not when families are grieving. Success is the prevention of the terrorist attack from occurring in the first place. And what you've seen over the last couple of years really since 2012 is we're trying to apply that same approach when it comes to national security cyber threats and the fact is we weren't at first. So we weren't applying for instance the lesson that you should share information across the intel law enforcement.

We were treating national security cyber events as intelligence events. Great work was done in terms of getting better at mapping out from an intelligence perspective what was happening. When I was over at FBI's Chief of Staff to Director Mueller working with the intel community and others, there was a giant jumbotron screen and you could literally watch in real time as nation states intruders hopped into places like universities then into companies and you would watch the data exfiltrate out real time.

But that was an incredible intelligence feat, but what you're seeing was horrifying and it wasn't the solution. And so, the change was we need to take that intelligence and then use it to come up with solutions to disrupt what you're seeing. And you've seen since then as try this new approach out. Part of it --

MR. PEREZ: The name and shame strategy basically, right?

MR. CARLIN: And some have called it name and shame and that's part of it because you want to use every single tool in your arsenal. But let me say, I think we've shown now it's not just name and shame. So one of the cases, yeah, it was the indictment of five members of the People's Liberation Army Unit 61398. And what we showed in that case is; one, we were able to do the investigation attribution and figure out who did it, not just what country, but by name, by face who was hacking into nuclear, solar, steel, management side, labor side.

And that what they were stealing was not traditional national security secrets, they were stealing things like right before a company went into a joint venture to lease a lead pipe, they stole the design specifications for the pipe; or to give another example, right as they wanted to compete with a solar company, they stole the U.S. subsidiary's pricing information so they could price dump right below that price and then to add insult to injury, when that company stole -- when that company sued, they then stole the litigation strategy out from the company through cyber mains.

So that's why we brought an indictment. What the indictment showed is this wasn't just, you know, a couple of actors. This was their day job. So the activities we showed attachments started around 9:00 a.m. Beijing time and would spike. And then you'd see these hackers activity continue to spike until around noon. It would then take a break at noon, sounds like the Aspen schedule for about 12:00 to 1:00 and then will go back up from 1:00 to 6:00 and then it would decrease again overnight.

And so, you had uniformed members of the second largest military in the world day-in day-out their day job was to attack not government, but private companies and do it for profit. So, we brought the case and part of that was a philosophy that said many of you guys are familiar with the concept of an easement. And this is the idea in our own -- in U.S. law that says if you let someone walk across your lawn long enough, they get the right to walk across your lawn. It's called an easement.

And that's how international law works. International law is a law of customary law and so that case and this approach is a giant no trespass sign, get off our lawn.

MR. PEREZ: But -- all right, let's just interrupt there for a second. But what has come of that? I mean, we know about the case, it's -- one of the -- certainly one of the big cases of your section of the Justice Department. What has happened since then and what does that have to do with the DNC hack and the Russians, did they do it?

MR. CARLIN: I'm glad you asked more about China. So the -- I think what you've seen since then --

MR. PEREZ: So, yes Russia?

MR. CARLIN: So --

MR. PEREZ: Yes.

MR. CARLIN: It is a definite change and so and that's something that. So when we tried out this approach, we thought we'd keep trying different tools to see if you can get behavioral changes. And what you've seen since then, let me tick through a couple things briefly. One, we then responded to the Sony hack in our division and that was new. In national security we gamed out for years. What's it going to look like if a rogue nuclear armed nation decides to attack the United States through cyber enabled means and not once.

Any of us in this field did we game out that it would be over a movie about a bunch of pot smokers. The only time in my career I have had to go to the situation room and try to brief the President, I don't know how many of you have seen it on the plot of that movie, which is hard to do in a minute. So -- but we treated it as a national security event and you saw a new presidential directive that talks about codifying that approach. And the reason why is because it wasn't about that movie although I do blame North Korea for having that.

I've seen it over Christmas along with the rest of national security committee, it's not the best. Well, they had every right to make it. The -- it wasn't about that, well they were -- deliberately a foreign nation was trying to influence U.S. They were attacking our fundamental values by saying you couldn't have political free speech by doing a cyber destructive attack. It wasn't just theft of information, they were turning computers into bricks. And so it was important to say number one, try this new approach, investigation attribution can we figure out who did it, yes we can and that's because Sony did the right thing and reported it to government and so we were able in 28 days to do attribution with sufficient confidence to say it is North Korea.

Two, we said it. So that's new like take it out of the intel channel as we did with PLA, be public about it because that's the only way to change behavior, not just theirs but all the others trying to figure out what you can get away within the space. And three, sanctions and in that case we had existing sanctions. Later that April, we passed a new executive order that allows sanctioning of cyber actors, whether the north -- no matter who they are if they attack and cause damage. And not just the people who steal secrets, but those who benefit from the stolen secrets can be sanctioned and that changed China, if I could you just finish the last.

You saw China send over a high-level delegation, 35 -- 37 people right before President Obama was meeting with President Xi. We met with them through marathon negotiations came up with this five-point agreement. You have President Xi say for the first time on stage, I agree publicly we shouldn't be using our military and intelligence to target private companies for economic game. That's really important when you think about the cyber in some respects --

MR. PEREZ: But have you seen change in behavior?

MR. CARLIN: Yeah and let me -- yeah, two in things in that. One, I think you are hearing from folks inside and outside the community, there is a change. Now how long lasting that will be, we'll see, yes.

MR. PEREZ: Less activity, less hacking, less breaking into companies, less stealing in the United States?

MR. CARLIN: That look -- less that looks consistent with this pattern like less stealing that looks like it's for the commercial gain. And you also saw not just the G20 but another 15 countries have signed up to this norm. So for the first time, we have an agreement around the world that that's wrong. Now in terms of your question, will it stop? It's like we wouldn't -- we would be out of business as prosecutors and law enforcement agents if passing a law meant that the activity stopped.

But I think because we have this agreement on what the law is now, the next step is getting private companies to go -- come forward, share information with us so we can see what's occurring and then be committed to figuring out who did it, being public about it and imposing consequences if they break this new norm.

MR. PEREZ: Well let's talk -- I want to bring in the other members of the panel to talk a little bit about -- again there's -- I know there's very limited things you can talk about with regard to this DNC investigation which you are overseeing.

MR. CARLIN: You want to talk about Iran next.

MR. PEREZ: No, I want to --

MR. CARLIN: Oh, okay.

MR. PEREZ: I want to talk about --

MR. CARLIN: Okay, just checking.

MR. PEREZ: -- when you see -- let's talk in general terms. If you come to determine that a foreign country has hacked into a political party computer system and you determine secondarily that it was for the purpose of influencing the election. Tell us what happens then? What happens next? If that's -- again we're speaking theoretically, since you can't speak specifics.

MR. CARLIN: I think --

MR. PEREZ: And you know, I'd welcome some thoughts from you --

MR. GROBMAN: Yeah, I guess you know just one point that I would like to make on the attribution side that is a bit different from where we are right now on the DNC case and Sony was with the Sony case there was strong attribution asserted by the U.S. government using a combination of technical forensics along with traditional intelligence information in order to come to that conclusion. I think one of the things that we need to be very cautious of is prior to a trusted government source coming out with a firm statement around attribution as only the technical side is available jumping to a conclusion that technical information alone is definitive proof that any individual actor is necessarily to blame.

MR. PEREZ: And from what you've -- gentlemen have seen publicly, is there enough here to -- for us to say with any amount of certainty, if any?

MR. GROBMAN: But I think that's actually my point is that if we're only looking at the technical data, it can give indications that help give indication of the potential actors, but it's really until John along with the IC are able to merge other information into that that strong attribution case would be made.

MR. PEREZ: I mean but -- sometimes I mean John, you know sometimes it takes him a couple of years to reach that conclusion. In the meantime, we have an election. We have great public interest in this and we want to know what do you think?

MR. DALY: I think you are touching on a, maybe even a bigger issue that we have non-state actors and a problem of attribution, maybe they are acting on their own for money, maybe they're acting on their own for some other reason. But we also know that states are manipulating the non-state actors and in a particular case here that we're dancing around. We have a country that has promoted criminal activity, allowed it to continue and has embedded itself across all of U.S. critical infrastructure.

We've been talking about espionage as a problem, but it should maybe give us pause and a little bit more anxiety that it isn't just espionage that they can do. And if other crises around the world escalate, these other countries now have a set of tools they can use to disrupt our entire supply chain.

MR. PEREZ: They're -- these are levers of power, they can use it as influence of anything --

MR. SICA: Right. I guess that's --

MR. DALY: That's right.

MR. SICA: -- kind of bring it back a little bit to more of a practitioner level, right? You know we do similar work on our own network that we would describe it earlier where you know we're looking from an intelligence perspective who's coming and when they're coming and what are they doing because you know I'm sure all three of us are around the top five of the top 10 listed companies behind the government that are being attacked every day. So it is using that intelligence that you're gathering there not just trying to keep a full defense. The real I think and I know you're dying for one of us to say, oh yeah, here's the smoking gun, here's who did it and we're not going to do that.

MR. PEREZ: That will be helpful.

(Laughter)

MR. SICA: But we're not going to do that obviously, but, you know, the bottom line is nothing should be assumed as safe.

MR. PEREZ: Right.

MR. SICA: All right? Same thing you tell your kids when they're out on the Internet doing stuff, it's all in the public domain. The real issue -- well, I think the real scenario we need to be focused on is do we have the right, you know, intelligence monitoring capability to see what's coming in, are we taking that capability and flowing it into our systems that we either doing for our own company networks or the systems we maintain or operate or deploy for our customers. We were talking earlier before the panel, you know, we don't just deliver new systems that honestly by the time we deploy them are out of date from a cyber perspective to say that.

But you know there constantly an evolving threat so you constantly need to be staying on top of that as well as modeling what's happening. So --

MR. GROBMAN: I also think there may be a little bit too much focus on only thinking about who did it. I think we also need to take a step back and look at what was done and what can we learn and really think about the value of different types of assets. Many of the people in this room with long careers in government think about cyber attacks as stealing intellectual property or top secret information. But if you look at the damage that was done both that Sony and in the DNC case, it was e-mail.

MR. SICA: Well, no e-mail, but you have --

MR. GROBMAN: E-mail, but if you don't think of it as a sensitive medium.

MR. PEREZ: You have personal information of donors, you have personal data, you have people being threatened now because their information is out there.

MR. SICA: Right.

MR. PEREZ: So it goes beyond that and if it is a country, a foreign government that has done this, I mean, they've gone a place that we haven't seen before really to this level to this, you know, to this extent.

MR. SICA: Kind of following up on a question from the earlier panel, you know, we need to be war gaming those scenarios.

MR. CARLIN: Right.

MR. PEREZ: Right.

MR. SICA: Across the board, whether it's company government you know as those attacks happened, what are you going to do once that data is on that.

MR. PEREZ: One thing that we've heard recently from the FBI Director and from you, John, is the estimate that perhaps only about 20% of companies ever call the fed or the FBI or anybody else when they detect that they've been breached. They -- 20%, that to me seems like an astonishingly small number and we saw it, I mean even the DNC hack as we reported we're told that the federal government did go to the DNC some months ago and said, hey, we believe that you've been compromised and apparently very little happened until they were able to call in a company to fix the problem in June.

So the question here is are companies doing enough, do they have a responsibility to cooperate with the federal government so that perhaps that information can be shared to protect the other people. What do you think? Is there more that needs to be done there?

MR. CARLIN: Yeah, the point you raised is vital. More -- there is more that needs to be done. The vast majority of companies today still do not report criminal intrusions into their system and a failure -- if you think about the reforms that we made enormous expertise in switching so that we did a better job in federal government of sharing across the law enforcement intelligence divide. So everyone was working off the same sheet of music.

This challenge is one step further because we can't do it in federal government. We had to get better there, but it requires figuring out a way to receive and incentivize people to share information with federal government and we got to do a better job of sharing back. And then the consequences can be life and death. And I just want to use one example. So imagine today you're in a company and you see a low level hacker go into your company and your IT folks say, this technique is not very sophisticated.

It just doesn't look like someone that really is the world's best hacker, doesn't look like a nation-state. Then you kick the person off their system, your mainstream trusted retailer, you kick them off your system and they send using commercial e-mail, a clumsy extortion attempt and they say give me 500 bucks through Bitcoin or I'm going to embarrass you that same kind of technique by releasing this personally identifiable information.

The vast majority of companies that exact fact pattern don't report. In this case, the company did work with the U.S. government and on the other side of that keyboard it turned out was not a low-level criminal. It was an extremist from Kosovo who had moved to Malaysia was in a conspiracy with the fellow extremists and what he was doing was providing that stolen personal identifiable information not a lot by, you know, by the standards of hacks 10,000 15,000 names providing it to Junaid Hussain, who at the time was the most notorious cyber terrorist in the world.

A London citizen who had moved to Raqqa, Syria where he was located at the heart of the Islamic State of the Levant, when the leads and trying to recruit people to commit terrorist attacks inside the United States and the west. And what he was doing was calling through the list for government names and addresses creating a kill list and then using Twitter was pushing that information back to their adherence and saying kill them. Because the company came forward, we were able to take effective action, not name and shame, but arrest Ferizi in Malaysia on U.S. charges.

He's in Eastern District of Virginia now where he's pled guilty for what he did and the military CENTCOM announced publicly that in a military strike about 30 days after in Raqqa, Syria Junaid Hussain was killed. It's incredibly complicated threat where things move quickly in a cross-country, but when we work with the private sector we can take effective action. I think any company if they knew it was a terrorist on the other side would come in. The problem is you don't.

MR. GROBMAN: But John, I think one of the things I worry a little bit about is sometimes it's positioned that threat information sharing is the silver bullet, the cure. And as valuable as it is and as important as it is for one element, I think it's critical that we recognize the limitations. Things such as threat intelligence inherently needs to be based on something you've seen, so that first action is not going to be part of your threat intelligence almost by definition.

I think a lot about threat intelligence largely forcing the actors to have to convert operational execution into new research and development, forcing the bad actors to constantly change their playbook and I think we frame our thoughts on threat intelligence around that line of thinking as well as really thinking about the incentives so that there's more value to share information and it's not just for the good of wanting to do good as in the case you talked about, we'd be much more effective at actually having the industry cooperate.

MR. PEREZ: Well let me -- I want to just change the focus a little bit from, we -- we've been talking a lot about the defensive side of this, right? The way how people can protect themselves and protect their networks and protect the personal information of their customers and their employees. There's also the whole part of the discussion about what role cyber plays as far as an offensive weapon and we've seen the Department of Defense's talked quite a bit recently about things that we can't see that they're doing to try to mess with ISIS and to try to perhaps sow confusion and discord within the ISIS troops and they say it's working.

So perhaps that gives us one view of how that could work and maybe talk a little bit about what you gentlemen see as the use of cyber tools in you know, an offensive way.

MR. GROBMAN: Sure.

MR. DALY: Right. It's a fantastic advancement because it provides us with additional non-lethal techniques. If we need to disrupt command and control of an adversary, you know historically, it's a kinetic effect, right? You can drop a bomb and take out an antenna or a ground station and now you're in a rebuilding mode, you've threatened lives. Cyber has the ability to change hearts and minds. It has the ability to give us those non-lethal effects, so it's an important advancement.

It still has limitations though. We're really struggling because with cyber, there are issues of assuredness. Is this really going to work because I will only get one shot at this, I can't mess around. I need to know that that cell tower is going to go off on. And then it has issues of containment. If I, you know, push this on that cell tower, how is that going to affect the other cell towers down the road or that hospital or the school?

MR. PEREZ: Something we saw in (inaudible), right?

MR. SICA: Right.

MR. DALY: That's right because you know those techniques can then get out and sometimes we call that being perishable as well. If I use this technique today somebody's going to figure out how to, you know, shut it down so I have to be more cautious. Do I use it today or save it for another day? And so that's another aspect of cyber that's unlike kinetic world.

You know if I drop bomb, the bomb blows up, it does it every single time but cyber weapons become perishable and not useful.

MR. PEREZ: Where is the government on this issue as far as I mean what rules are you guys talking about to put in place for -- to, you know account for what Michael is talking about.

MR. CARLIN: Like put a couple different frames on it. One, there's sometimes a discussion when we talk about cyber at -- cyber intrusions into United States, what are we going to do to respond through cyber means and I think -- well, we need to do and I was trying to do in the presidential directive that just came out this week codifies this approach, is just because someone causes you pain through cyber means doesn't mean that your response has to be through cyber means.

And if you think about it, we've built the biggest glass house in this area because we moved faster than anyone else to digitalize what we value over 25 years about 98% of what we value that used to be in analog is now in digital. And we did so systematically in government, in the private sector, we did so without adequately calculating what the risks were to this information that's stored in a way that was fundamentally never designed to be secure. So we're playing catch-up.

That doesn't mean you don't cause, come up with ways to do deterrence or to take actions. It just means your action might be asymmetric, so they come in through cyber. You do a prosecution, they come in or you do a sanction or you designate them as an entity to whom you can export or you use diplomatic means to respond. So that's one frame.

A second would be in armed conflict, you are going to start using and developing doctrine over when it's appropriate to use cyber. And I think you've hit on many of the policy issues. If it's something that's confined just to the theater of operation, then it looks more similar to our traditional frame both of international law and U.S. law. If it's an action because this happens more often in cyber, there's some analogies but more often in cyber than other areas where you -- you're trying to impact the theater of operation, but in order to do that actually servers are in all these different places --

MR. PEREZ: Right.

MR. CARLIN: -- across the world that raises a different set of policy issues you need a framework to make sure that they're --

MR. PEREZ: Well, we're going to open up for questions, so prepare your questions and now we'll take that in just a minute. Vinny.

MR. SICA: Yeah. One quick point on that because I think we would all kind of say, you know, we support our customers in the offensive cyber activities that they're doing, right. Really what we're doing there is providing them people, technology, tools, capability and the government agencies will take care of that side of it. Well, we use that knowledge and learning what we do there is how we both protect our networks and kind as Michael mentioned, you know, these are fleeting capabilities.

So as you're looking at what is your next offensive capability tool or scenario, how are you making sure that you've got the defenses on your network, the government's network and your programs so bringing both the offensive cyber knowledge or gaining as you're trying to do things in the cyber world -- in our offensive cyber world --

MR. PEREZ: Right.

MR. SICA: -- to make sure you continue to strengthen your defensive posture and your intelligence of stuff that's coming after you because it is fleeting. I mean every day that threat is changing.

MR. PEREZ: It feels like, you know, maybe a couple years ago and last year we were talking at this forum about cyber and we were talking a lot about China and what they were doing and the change in behavior, we're still -- the jury was still out. There seems to be now this view that the Russians are showing more assertiveness in various things that they're doing. There was the attack on French Television which I believe they -- it is strongly believed to be a work of Russian intelligence as well.

What do you see from your customers, I mean, are you seeing them being more active? Is there anything you can talk about with regard to what the Russians were doing generally, in general terms?

MR. CARLIN: Well, say -- just broadly prior to -- so there have been four actors, the Director of National Intelligence Cells Community et cetera, the primary threats in cyber right now nation-state actors; Iran, North Korea, China and Russia. And if you -- if we were doing this at Aspen and we did, you know, four years ago, or four, five years ago and said what have you done, okay, we're hearing that that's the assessment, what have you done to show that it's them, be public and cause deterrents, the answer would be we had.

Now since then, you've seen with China not just the PLA case there's an individual named Subin who is -- was in the conspiracy with two members of the PLA hacked into a Boeing and was arrested pursuant to our charges in Canada, pled guilty and has been sentenced to over 40 months in prison. It's just that when you mention name and shame, it's not just name and shame, they are real charges with real consequences.

MR. PEREZ: Right.

MR. CARLIN: With Iran, you saw a spring charges early this spring where we laid out seven Iranian affiliated hackers who worked with the Iranian Revolutionary Guard Corps to attack 46 different financial institutions affecting hundreds of thousands of customers costing tens of millions of dollars. And in that same charge, you saw us outlay that one of them had hacked into the Bowman Dam in Rye, New York, relatively small dam, access the sluice control system, which would allow you to open the damn.

Now the dam wasn't working as intended at the time, but I don't think that's our best defense long term. And you saw as we've discussed before, with Sony North Korea or to use another example Syrian Electronic Army we've brought charges there and there's an individual who's been arrested. You haven't seen yet a public action against Russia, but I wouldn't assume and I think would be mistake for them to assume that we're not going to apply this deterrence model when it comes to their actions if they continue to intrude.

MR. PEREZ: Is it --

MR. CARLIN: So, this approach is new, but we need to keep following it and we need to be committed to even though it causes churn, when we figure out who did it being public and causing consequences.

MR. GROBMAN: But to hit on that, I guess one of the things that I wonder about this approach is given the inherent asymmetric nature of cyber that you can have an entity like ISIS not even need to develop the technology themselves, but simply hire the right talent and pay for it. And I think that it's very easy to think about cyber weaponry in the way that we do traditional kinetic types of weapons. But in my mind, it's actually quite different due to the ease of generation and execution.

MR. CARLIN: I don't disagree with it.

MR. PEREZ: So we -- we'll open up to some questions with this gentleman. Right here, just trying to -- right there and then back there.

MR. GARVEY: Good morning. Thanks for the discussion. My name is Patrick Garvey I work for the Congressional Research Service. My questions for the CTOs among you and I'm curious as to the progress the government has made in the last year or two to share its understanding of the threats that are coming at you whereas you've spoken as the government is consistently asking for your information to help them go after mal actors. Thanks.

MR. DALY: Right. So we actually have a very active engaged program with the government. They are providing us with threat information. We are able to defend our networks with that information, and it's been much more timely in the recent period than it was let's say in the past where we would receive something and say, well I saw that you know three months ago. We're now seeing that it's much more viable information.

MR. GROBMAN: I would concur. The only thing that I would add is I think only looking at what has happened for planning your defense isn't sufficient. So a large part of what we're focused on is trying to figure out what the next wave of technology will be, so that we can start developing the defenses for that now versus waiting until we start to see it.

MR. PEREZ: Right. Next question.

MR. DALY: But if you didn’t mind, a follow-up on that. I agree completely and what we need to do is move to a more automated ingest of this information so we can take action nearly immediately. And DHS has done some wonderful work promoting the capability to do that so that they'll stand up systems that will publish these indicators in near real time and we can ingest them in written in real time and take action.

MR. PEREZ: We have a question right there.

MR. FAGIN: Thank you. Barry Fagin, Director of the Center for Cyber Space Research at the U.S. Air Force Academy. I'd like to thank all the panelists and I mean in particular whoever organized this session and because this topic is really important. So, on the one hand, I'm delighted to hear about the progress and I'm delighted to hear that we've managed to get attribution.

On the other hand, I'm inclined to think that the members of the PLA who were got -- for whom the -- who got caught actually probably got shot and their -- probably their attribution -- their just -- their ability to cover their tracks will just be improved. What I am concerned about is that no one on the panel yet anyway has said anything about why these systems are so easy to penetrate in the first place, and what -- but we -- and -- of course we all know why that's true, but could someone on the panel please say something about what can be done to improve, for example, the mathematical rigor that which these systems are designed so that we have more programmers and more systems designers who were trained in mathematics and formal proof so that you can actually prove certain things that these security problems aren't present in these old poorly designed systems written in really lousy programming languages.

MR. SICA: In other words people aren't doing enough to protect themselves.

MR. PEREZ: Right.

MR. SICA: I guess if I could jump in to start on that, again a lot of our programs, some of the challenges we have -- I know Michael for sure and I have a lot of the same type of programs. You are taking over programs that were designed, built, had requirements that were years ago.

MR. FAGIN: Sure.

MR. SICA: And you're in a sustainment mode. So you're trying to, you know, change the wheels while you're driving around the beltway at a real fast speed, you know, and that threats ever changing. So it is a combination of things. The new requirements are going to be old by the time you start coding them. So but it is starting with academia right, so it is building coding, right coding standards from the start to build secure code, make sure you have the right architectures that you starting with.

You know, but again I think that's all necessary but not sufficient. It really comes back to having the that network monitoring that intelligence capability that you're looking at that sees people coming into your network because your systems will be secure for a very short period of time, no matter what's that you're complying against or what -- you know what sort of new requirements you are trying to go to, you know, it's -- they're going to find ways back in and if you're not monitoring it and taking a prosecution route, you know, and fighting back with through the government, you know, they're going to be at a date before you get there. So I think that that monitoring systems work --

MR. PEREZ: I think we have time for a couple more. This lady right here and then the gentleman back there.

MS. LARSEN: Hi, Amy Larsen, NYU Law and the Harvard Kennedy School. Thanks so much for being here. I was wondering what kinds of programmatic policy or other kinds of incentives might mobilize companies to actually share some of the information and data with government that John was referring to earlier?

MR. CARLIN: And I'll be -- let me start because I'm curious to get views on. So we passed earlier it's been years in the attempts, Cyber Security Information Sharing Act and the idea was when I was going out doing outreach hearing from companies, I would hear again and again about certain issues that were deterrent to sharing. One, sharing with each other, they are worried. I am normally not allowed to talk to the people in my industry, why am I allowed to do it on security, is it going to be an antitrust violation?

So, the Act clarified that you'll get certain immunity of what you're sharing is threat information. A second issue that had come up was am I violating the Electronic Communications Privacy Act if I share this information. So it set out standards for which you'd also get immunity if you share it, if you took, if you took certain steps. One thing we fail to pass and this is just bad -- there's no explanation for it other than a desire to employ more lawyers, which is currently there are 46 different data breach notification statutes throughout the states in United States.

And so we've been attempting to get one federal rule so the rules are clear when you need to report and when you can do get safe harbor of you're working with law enforcement. Well, one thing I'm curious is what should we do next? What should the next policy should be?

MR. GROBMAN: So, I think John, part of the challenge that I hear is you've done a lot of great work to remove the barriers to information sharing, but you haven't done enough on the encouragement side. So I think when entities are looking at should I be an active player in providing information? What is the value to that entity in doing? And I think in some industries, it's a lot clearer than other. So in some of the (inaudible) financial or the defense industrial base it's worked fairly well, but as far as a broader -- the broader private sector I think there's not been the inherent incentives.

MR. PEREZ: All right. We'll try to get one quick question before the final question.

SPEAKER: She asked my question.

MR. PEREZ: Okay, all right. Anybody -- somebody behind you right there.

MS. SPAULDING: I'll just add -- I'm Suzanne Spaulding, I'm the Undersecretary for something called National Protection and Programs Directorate at DHS. We have the responsibility for cyber security and critical infrastructure protection. And I just want to add to John's terrific summary of the Cyber Security Act that it also provided liability protection for automated sharing with our cyber center, the NCCIC and it goes to what Steve talked about the automated information sharing or Michael, I guess, you talked about that.

MR. DALY: Right.

MS. SPAULDING: Right, which provides tremendous benefit potentially to the private sector. It's a fairly simple way to plug in and share and receive threat indicators that you can use to immediately protect your system and force the adversary, to Steve's point, to change the way in which they are coming at you which today they don't have to do. Today they can come at you the same way over and over again.

This system of sharing benefiting everyone from the information that any one entity sees with regard to threat indicators I think is holds tremendous promise. And Congress advanced that by providing that liability protection.

MR. PEREZ: We have one minute left, so if anybody wants to take one last swing at John to try to get an answer about the DNC hack.

MR. SICA: Anybody left?

(Laughter)

MR. PEREZ: Anybody?

MR. DALY: Somebody over there.

MR. SICA: Left to --

MR. PEREZ: I want to say thank you to everybody for coming here and to the panelists for your great work. Thank you very much.

MR. CARLIN: Thanks Evan.

(Applause)

* * * * *