THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2016

INTELLIGENCE-LED CYBER SECURITY: OPERATING GLOBALLY WHILE BALANCING RISK AND SPEED

Doerr-Hosier Center
Meadows Road
Aspen, Colorado

Saturday, July 30, 2016

LIST OF PARTICIPANTS

JAY HEALEY
Senior Research Scholar, School of International and Public Affairs, Columbia University
Nonresident Senior Fellow, Cyber Statecraft Initiative, Atlantic Council

SEAN ROCHE
Associate Deputy Director for Digital Innovation
Central Intelligence Agency

PATRICK WALSH
Senior Vice President, iSight Partners
General Manager, ThreatSPACE

RYAN LIZZA
Washington Correspondent, *The New Yorker*

* * * * *

INTELLIGENCE-LED CYBER SECURITY: OPERATING GLOBALLY WHILE BALANCING RISK AND SPEED

(10:30 a.m.)

MR. WATTERS: Okay, folks, we've got to get going here. Thank you. I'm John Watters, founder and CEO of iSIGHT, and as of six months ago, an executive officer or FireEye, pursuant to the merger. The topic today on intelligence-led security, how it shapes the way you think about global operations, both from a government perspective and a private sector perspective, I think is important and timely. If you think of this conference, the intelligence theme has led how you shape policy, how do you shape strategy in dealing with ISIL, ISIS, extreme, -- you know, extremists around the world, and then in terms of how you shape operational strategy for any kind of military action.

But to date cyber has been largely driven through both policy and regulations that has driven the advent of cyber, and is beginning now to pivot in terms of intelligence-led operations, and how people use, now that cyber has become more of a risk-driven function than a regulatory driven function, how you think about your global operations, deploying assets, deploying security measures to control those assets and investments globally. So this panel will be a good timing, I think, to kind of round up the session here today. So, I would like to introduce Ryan Lizza, who is the Washington correspondent for *The New Yorker*, in addition to being a contributor to CNN, and a professor at Georgetown in his spare time. So Ryan, thank you.

MR. LIZZA: Thank you very much.

(Applause)

MR. LIZZA: So cybersecurity is not necessarily my area of expertise, and when we were first putting this panel together I was telling some of the folks at Aspen that, you know, I am going to be at the Democratic National Committee the week before, and just, you know, throwing me into a cybersecurity panel may just be a little bit difficult, but fortunately my interests this week have combined --

(Laughter)

MR. LIZZA: -- and so I am very excited to talk to three of the preeminent thinkers on this issue, and leaders. And let me start by introducing the panel. First we have Sean Roche, who is the Associate Deputy Director for Digital Innovation at the CIA. This is the -- just was stood up last fall, the first new directorate at the CIA in 53 years, and hopefully Sean will tell us a little bit about why that directorate came into creation and what exactly it does.

To his right is Jay Healey, who is a senior research scholar at the Columbia School of International and Public Affairs, and a non-resident senior fellow at the Atlantic Council. To his right is Patrick Walsh, who has a long and distinguished career in the navy, correct, Patrick?

MR. WALSH: I don't know how distinguished it was. It was long.

(Laughter)

MR. LIZZA: His current hat is a senior vice president at iSight Partners, and the general manager at ThreatSPACE, which is now the same company. The same company? No? Yes, it is. Okay.

MR. WALSH: We were acquired by FireEye earlier this year.

MR. LIZZA: Got it. So look, I know, Sean, you are going to be very limited in what you can say about current events, but I want to start, since it's such an important topic and on the minds of everyone here, with what happens at the DNC, and how -- why don't I start you, Patrick, about one, how should the -- to me this is sort of a watershed moment in cyberwarfare, right? This is the first cyberattack that the public, that every voter in America has a personal interest in, even bigger than the

Target attack or the Sony attack. So, help us understand how the public should think about this. This is presumably an attack by, from what they reporting so far has been, an adversary on one of our political parties that may or may not be trying to influence the outcome of a presidential election. Even in the worst days of the Cold War, it's hard to remember something -- hard to think of something as serious as this. Help us understand, one, what's your assessment of what happened, based on what you know, and how do you think policymakers should respond?

MR. WALSH: What you missed earlier in the week was this question came up over and over again, and often times the summary point that the audience would ask is, is this a game changer.

MR. LIZZA: Yeah.

MR. WALSH: Depending on who received the question, if it was an intel practitioner, they would say not really. If they were from the spy community, they would say it's just spy craft by another means. There were others who were quick to point out that we're in an ongoing investigation and we don't really know. So what we do know is that there is, when the malware is reviewed and looked at that closely, the forensics associated with it follow patterns. These are advanced persistent threat actors that are involved. They're sophisticated in terms of what their capabilities are and the way they are introduced into the environment.

We've described this as APT-28 and -29, in terms of the actual malware involved, but that's only a microscopic inspection of malware. That doesn't get to attribution, because there's no context associated with it. So we don't know the broader sets of questions, which the audience is very interested in. I'm going to tell you that I do think it's a game changer, but for different reasons. To me, as I left the navy in charge of the Pacific Fleet where we would rehearse contingency planning through the course of exercises, we knew that cyber was going to play an important role, but we didn't really know how to test it. And so what we did was we wanted to understand what role cyber would play in escalation as well as de-escalation.

So we reached out to the private sector because we wanted to go beyond our comfort zone, we wanted to reach out and challenge our understanding, and the blinders that we had set up ourselves in the course of our long careers, and try and think differently. And what we found is that when we were able to leverage the private sector and bring it into the scenarios that we were in, we could be far more effective than we had ever realized in a non-classified environment.

The system that we have set up today is a very Westphalian orientation, which is to say that if you look at our organizational structure in DoD and DHS, we have a presumption that there's a tidiness about the system in terms of how it enters into the U.S. Government, how the U.S. Government responds to it. The reason why I say the DNC hack is a game changer, because it forces us to realize what we are really up against, and that doesn't happen very often where it's put right in front of the American people in a way that you're not going to be able to just walk away from this and think, "Well, that's just business as usual."

Now you're seeing it in ways that most people never knew this kind of stuff was going on, to begin with. And I'll be succinct here. So the real question is not so much the tantalizing information about the DNC hack. The more important question for this audience is: Are we prepared to deal with now a threat that focuses on data? It's the ubiquity of data. People want your data and they've got lots of motivation behind it. They either want -- they want it for profit, they want it for criminal purposes, they want it because they want to exploit your personally identifiable information. They want it because they want to make a statement. But the point is your data is key to your future, and the ability for you to rely on that data, meaning people can now manipulate that data, that presents a real problem, because it undermines our whole understanding and the foundational sort of sets of principles of how we are as a people.

I think the question is, is Congress organized in a way to deal with this when it comes hearings. I mean you think about the committee structure, you think about, you know, authorities, resources, policy, and it just increasingly does not fit into a DoD, DHS category for cyber. I think we have a chance, particularly with a new administration, to now grab cyber in a way that recognizes DNC as part of the future, that type of capability, and that we need to think about it differently.

MR. LIZZA: And I should not just the DNC. Of course, it's the DCCC, the House campaign arm of the Democratic Party and the Clinton campaign. So you have three major Democratic entities that have been hit. Jay, Clapper this week was sort of blasé about this. He suggested, uh, it's -- everyone gets hacked. Of course, the Democratic Party was hacked, and sort of downplaying it to a certain extent. What's your level of outrage and how much of a watershed moment do you think this is? And then, I know you have written about this, what do you think the policy prescriptions going forward should be?

MR. HEALEY: When the news first broke on this, it started to come out in June that the DNC had been hacked in -- and for me right now even the Clinton Campaign and the DCCC, I said -- and especially the way that the U.S. national security community has approached this, is there is no foul here, right? Going into a campaign, going into a party, that is absolutely valid geopolitical intelligence. If the U.S. -- of course, the U.S. is trying to get that intelligence on other people. I doubt, if NSA wanted to do that, they would even need to go and get permission from the White House, right? That is absolutely the kind of thing that they are expected to go after. So if the Russians or the Chinese do that for us, and the Chinese went into both McCain and Obama's campaigns back in 2008, that is no foul. We can get angry about it, we can seek to stop it, we can get riled up, but we can't get too angry because we do it as well.

Once those e-mails were released, now you're starting to see tampering, now you're past espionage, you're into covert action. And for me that really started to put me in a different place. Now we've got different levels of confidence. The level of confidence that the

Russians were in the DNC and these other places, as I have talked to the experts, is very high -- eight out of ten, or higher. And FireEye has written about that, amongst others. So whether or not it was Russia that released the e-mails is a lesser degree of confidence. I think as experts we can imagine more than one group being in the DNC, and theoretically it couldn't have been some other group that did that. Cyber-threat intelligence has some to bear on that, but it's really in the government Intel space to really truly come down.

So what we do about it. So I had a piece that came out in *Christian Science Monitor* two days ago, when I looked at four areas. One is especially if we do get better confirmation that it was, in fact, the Russians that released the e-mails, in that the President needs to make sure that this is about policy, not politics, that we are there to defend the Constitution, not to defend a particular political party, I think, and to help keep people in the mind that this isn't just a regular hack. And I think the media's had a good role there. I have loved the coverage in places like *The Times,* that has really put that out front.

Second is, really reaching out, especially to our European allies. With French, German, Austrian elections coming up, this is absolutely something that we need to work with them, share our intelligence with, connect them into the great companies that have been doing the cyber-threat intelligence on this, and come up with something common that says, no, you don't get directly involved in elections in this way.

Third is a set of actions on Russia. If this were China, I might react differently. The way that Chinese have come at us and the way they have responded to our counteractions has been very different from the Russians. The Russians have been very, very aggressive, and so I think the President needs to start looking at brushback pitches. You know, how can we throw some inside so that we can get them to back away from the plate a little bit. Certainly, covert action is going to be in that, but also cyber command set up a cyber national mission force, which in cyber-speak looks in red space.

So, it's looking at the bad guys and saying, if they ever cross the line, how can we disrupt them.

Sony would go down very differently now than it did just 18 months ago, because we've got people that are looking at North Korea and saying, if the President gave the order, how can we disrupt them. And I am certain that we have got people that are looking at these APT-28 and 29 people and how we can disrupt them.

Last of the four is looking within the U.S. There are a lot more direct ways to mess with an election using cyber means than just releasing e-mails. There is a great article that came out in *Business Week* a few months ago on a Colombian hacker, and he was doing all sorts of dirty tricks directly in the campaigns all up and down Latin America. We saw in Ukraine, maybe two years ago, hackers went in and tried to change votes within the electoral database, directly going in and trying to change who voted for whom.

The election machines have a lot of vulnerabilities, and so I think the President needs to try and work with Congress for some emergency funding so the states can bolster their cyber defenses. The President currently has a cyber commission. They should form a separate electoral taskforce and come up with ideas in working with Congress. People like Representative Langevin, from Rhode Island, who had been a secretary of state, he knows cybersecurity. He knows the electoral process.

MR. LIZZA: Jay, it's actually possible to hack into our vote counting, some vote counting machines.

MR. HEALEY: Absolutely.

MR. LIZZA: That's not just the Diebold conspiracy theory.

MR. HEALEY: Absolutely, and if --

MR. LIZZA: These are connected to the Internet.

MR. HEALEY: And if you voted in Northern Virginia in the last 10 years, the system in Northern Virginia, it was optical systems. You can kind of press -- I mean, that connected in the public WiFi, with easily guessable default passwords. You could go in directly to the machine and change votes. They got rid of it maybe in the last two years. But if you are in Northern Virginia you had one of the crappiest voting systems possible, extremely easy. You didn't need to be the FSB to change it. You needed to have a laptop and some curiosity.

SPEAKER: They literally had to go back to paper ballots.

MR. HEALEY: Yeah.

MR. LIZZA: That is frightening.

MR. HEALEY: And someone said, we literally had to go back to paper ballots. And that get raised yesterday in the session with DNI Clapper. I think it's okay to start thinking about some backups, and what we can do.

SPEAKER: Use paper (inaudible).

MR. SPEAKER: That's what Trump said this week, just always use a courier for everything. Sean, I want to ask you --

MR. ROCHE: Yes, Bin Laden did that.

(Laughter)

MR. LIZZA: Good start.

MR. ROCHE: Just saying.

MR. LIZZA: Sean, in the private sector world when we get these reports, it's almost like the Wild West out there. Any company can come out and make an argument for attribution. Take us inside the government and your directorate, and when you have an attack, what is the process by which you are getting -- I imagine at some the

President is going to want to know what is the attribution for any significant attack. But what's the process by which you confirm attribution?

MR. ROCHE: It depends on how far it extends. First, cyber and U.S. Government is very much a team sport, and people say that, but it's very true, and the reason is that while there is a little bit of overlapping capabilities, you really need all the players to get the full picture. So right from the beginning there's a huge effort on building an integrated picture of what's happening. For any domestic event, DHS has the lead for informing across the government and doing that messaging. Phil Schneck (phonetic), who came out of (inaudible), by the way, doing an amazing job in that area, and FBI, in terms of criminal investigation.

For an overseas component that's where my directorate at CIA, but also our colleagues at NSA, and sometimes cyber command, and others, and sometimes there is an overseas component for some of the other parts of the IC, will get involved. So the first thing, you know, that kind of what happens is there's a lot of -- the reporting that comes out from private firms is extremely valuable reporting, and it's part of open-source. And years ago open-source didn't enjoy the same sort of panache, because it wasn't marked up all top-secret and hush-hush, and so people thought it wasn't as valuable. And, of course, we all know the value of open-source, the first open-source reporting on the Abbottabad raid was Twitter from, "Hey, it sounds like a helicopter. That's not very normal." So, we know that open-source is a lot more valuable.

So what we did as part -- in following a 90-day study that Director Brennan commissioned a few years ago is, we put open-source into this new digital organization, because the reporting coming out of open-source, and not just the reporting from our colleagues in the private threat industry, but the deep-level reporting, what people are saying. Turns out that people who carry on these kind of activities have keyboards and use them all the time for lots of stuff. They are not just conducting these activities. Therefore, there is a lot of digital dust, as was mentioned the other day, out about them. So, it's very deep-dive of the open-source, and that open-source center is part and integrated within this digital directorate.

The digital directorate, the idea there was, with these really high-performing digital components within CIA, but they weren't integrated in a way that allowed us to act at speed, and so that that is my charge in life, is go faster, go faster. So, you have the open-source, and then you take the event, and what you know of the event, you take what you know about the actors, and the actors all have personalities, and then you translate what you need to get that's not in cyber. All the intelligence that comes from everything that is not the cyber intelligence. In other words, we have overhead reconnaissance, and we have humant, and all things that the community brings to bear across a pretty wide range. DIA has defense attaches, et cetera. So, you have to translate what those missing pieces are into a system that will leverage all those IC components, and start to build that picture. And there's a lot of integration among these groups.

The cyber experts in the various part of the IC know each other extremely well, get along well. They're very anxious to share with each other, and anxious to have a community of learning. And there has been a couple of things to accelerate that. The C-Tech was formed last year to integrate cyber-picture at the national level for DNI Clapper, and the people that were assigned there are highly capable. They have been doing reporting for about a year. It's a great product, and that's working really well. But again I would offer that when these things happen, much like when an airplane goes down, everybody wants to know what happened, and the pundits get on pretty quickly. I think it's on CNN, it's always that pilot with Tom Selleck mustache, and he's very quickly --

MR. HEALEY: He must be very wise, with such a mustache.

(Laughter)

MR. ROCHE: Yes. Yes. And he is very quickly figuring out what's going on. In the same way, when we have this response to cyber, our job is to apply detailed disciplined analytical tradecraft. So when you mentioned bringing things to Whitehouse, bring in the answer, and bring the right answer.

MR. LIZZA: Do you want to follow-up on something?

MR. HEALEY: I know some of the audience might not know a lot about cyber-threat Intel, and so just when you hear about attribution, I mean, in general, when we are in the field and we are trying to attribute and say who did it, I mean by attribution we are trying to say who did it, and especially if we can get to national responsibility, because at the end of the day it might be the President having to pick up the phone and so you want to work it both bottom-up on the technical and top-down.

And there is really kind of three broad areas that analysts are trying to do. One, they're really looking at are there technical artifacts? You know, are there ways that we can figure out is there something in the code, you know, on the DNC hack, it appeared that, for example, maybe they use Russian keyboards for part of this. We heard, you know, while they were working -- are they working during Moscow time or Beijing time?

The second is the mode of operation. And anyone like the *Ocean 11* movies? I love those, right? And if you know anything about crime, you can tell if you got robbed by the Ocean's 11 gang or the Knight Fox, right? They have completely different styles of operation, and once you know something about how they operate, then you can figure that out. And that's one thing that FireEye has been really good at, is helping us understand that. And the third is the context.

Now if you're a national security international relations person you might not know much about those first two, but we know a lot about context, right? I mean if there is something going on in Estonia and they subsequently get an attack, those facts about context can really, really help you figure out what's going on, and your instinct, as a national security person, can carry you far away.

And how this is getting used, I'll talk to some of the banks, and one of the ones that's particularly far ahead say, if you are going to do a deal, say, you know, with Brazilian (inaudible) offshore oil drilling, we will look at FireEye reports, figure out what groups would most be interested in spying on such things. We'll figure out what their methods are of how they tend to prefer to hack, and then we will go to that business unit that's involved in that deal, and we will go and we will specifically look for how they're doing. This is really sophisticated use of intelligence that you don't normally think about companies using. You really only think about this as this is very government, is how you would think about, but it's really very, in some cases, very sophisticated use of this intelligence to drive defensive operations.

MR. WALSH: Yeah. So what you've just heard is the articulation as to why companies invest in intelligence products, because they're trying to understand what the risk profile is, they are trying to make intelligent decisions about where their investments need to be in terms of resources, and in terms of how they protect and defend themselves. So, what we find is that the intelligence product, while it's commonly understood in government circles, is not necessarily understood in terms of how it's used and applied in commercial circles.

Yesterday you heard a briefing from someone who talked about what it takes in order to put the intelligence playbook in front of the president every day. It's an hour-and-a-half briefing, takes a long time to put it together, a lot of people involved. Essentially that's what we are doing, except we are doing it at the corporate level. Those are the kinds of decisions that companies now have to make, especially since all of the very high profile breaches that took place in the 2012 and '13 time frame.

MR. ROCHE: Just to add to that, one thing past that is -- well, as we push more of the analytical judgment out of the intelligence community and into the private sector, the private sector will need to build up an analytical, well, so a receptor for that. Today there's a lot of very tactical response of what do I do, what patch do I issue. When we are getting more to the here is the intended purpose, here is what may happen next, here's how this actor is going to come at you in the future, that relies on a commitment to an analytical component in those companies which is an expense that knows how to take that analytical judgment and turn it into action. And we have the date, on the ones we have pushed out, we have not seen a lot of companies be able to respond.

MR. LIZZA: Let me ask you a question on the prominence of some of the private sector reporting on these issues. I mean just as when CNN first went on the air in the '80s, suddenly there was a spotlight on crises all over the globe that didn't necessarily have 24-hour coverage, and it created enormous pressure on policymakers to do something, depending on where this new 24-hour news network was. With cyber, very recently that, you might know something, but the public wouldn't, and that would give policymakers a much broader range of options. They might not disclose anything. How does it change your job when you have a prominent public attribution story the way we do with the DNC hack, or just in general how does the private sector reporting, when it blows up into a major issue, how does it change things for policymakers?

MR. ROCHE: Well, it's -- so I am not making any comment about the DNC hack, as it's under current investigation. But for larger, let's take OPM. OPM happened just a few days after it was announced this new directorate was standing up. So the first effect it has when a major issue like this happens is that there's an incredible amount of education that happens across the government. I would say that we always want our digital acumen to be higher, so the first mode you go into is teaching, and you are explaining, okay, here is what happened. The reporting out of the private companies, and you kind of calibrate the reporting across, as I said, you aggregate the reporting, then you kind of calibrate each one of the companies, based on how they do their analysis and their tradecraft. But the first happened is you have to take that, which is very understandable within the cyber community, and translate it for senior policy officials, and for Congress, et cetera. And that's really important to get that right, because this is not a language we have been speaking for the past 20 years at level of depth. It's not the same as other kinds of events.

So when there is a prominent way, and by the private community, I think the effect it has beyond getting everybody quickly more on the same page, is it really helps us in the prioritization process for how we set priorities for the collection that is other than cyber, and for what we would do with our cyber capability. The digital director has, we have a cyber capability in the agency, we team with NSA, we have cyber threat analysis. So all of those folks have priorities that they are working, a very prominent effect, it helps to say, do we have the right priorities, because asking for more resources is not going to be response if you are not going to get them in that time frame.

MR. LIZZA: Jay, I know you have thoughts on this.

MR. HEALEY: It can be very difficult because we have a smart group here, I mean that understands national security, that understands homeland security, and a lot of times when one of these comes out, you get a lot of mixed messages. Like one company is saying X, but another group is saying no, no, no, it's not that, and it really tracks itself. There is so much uncertainty in the cyber field, it attracts contrarians, people that say no matter how much tradecraft and expertise you get in, there is going to be someone that say, no, no, no, no, it wasn't them, it was China, or this was the U.S., or this was false flag. A lot of those folks tend to be -- they come two ways. One, they are coming from the very technical side, and they are only staring down the wire the ones and zeros, and they don't understand the other ways that you can try and understand who had done it.

Sometimes as companies are also driven by their marketing departments to try and say something interesting so they can make news. I am really pleased when I saw the sponsors for this group, because some of the most -- I mean intel security, McAfee was some of the first ones in this business to start doing these reports. FireEye has brought in many of those most trustworthy companies into the same place. And so when I saw that in the DNC hack, it was first another company that I really trust that broke the news, and when I saw that FireEye was coming in and saying, based on the evidence that we saw, I was done. I said okay I'm convinced. And so I think that --

MR. LIZZA: Who are some of the less reputable ones out there?

(Laughter)

MR. HEALEY: I've got one in mind. And one of them went under. I mean one is a company named Norse. And they had reputation of being a little driven by their -- they had the fanciest graphics, and they ended up going under. And one other thing I do want to point out in this, so as you are kind of trying to figure out this new cyber field, to understand the dynamics. We in this country are great about screaming about what the other folks do to us, and we classify the outbound fire. And so when we are trying to understand, for example, the dynamics of deterrence, the dynamics of look at all this that has been done to us, we need to increase our pain back on them, there is a lot of pain that has been going back on them.

In fact, we started out throwing a lot of these punches in this space long before the other people started to get in. So, if you want to understand these dynamics of this back-and-forth you really need to kind of get into those headlines a little bit more so that you can understand both sides. It's like trying to understand the Cuban Missile Crisis without even knowing that the United States had nuclear missiles, much less that we had some in Turkey, but you have got to understand both sides.

MR. LIZZA: All right. We have only 10 minutes left, so let do some questions. Were you going to ask something? No?

MR. WALSH: He burped.

(Laughter)

MR. HEALEY: I was like, can't believe 10 minutes left.

MR. LIZZA: All right. Right over here. You, sir. Yeah.

MR. GARVEY: Thanks. Patrick Garvey, of Congressional Research Service. Admiral you said something interesting, and I had an interesting conversation over breakfast that spurred this question, and it's about the government's ability to respond to buy the capabilities it needs, identify the requirements legally, according to defense procurement law, et cetera. How do we get ahead of that? Because that's such a time-lapse process that takes five to seven years to buy what we need. And one of the speakers yesterday said something about, you know, this is data that was created, you know, going back generations that now we need to secure as well, as we put it up and make it available.

MR. WALSH: I think it's a great question.

MR. GARVEY: So any of you gentlemen with Irish extraction, I would appreciate your thoughts on it.

MR. WALSH: Because if not informed and not done in cooperation, with an understanding of what's going on in the private sector, then it puts you on a path to spending quite a bit and not necessarily being relevant. I mean you can put your -- you put yourself on a path of obsolescence, you are very quickly in this space, if you're not careful. So, what we are finding is that increasingly the language inside the private sector is one that recognizes that with the changing threat landscape, I have got to be far more nimble and far more forward leaning, that I have to look at my technical team, and the integration of that technical team and their communications abilities up to the C-suite as one enterprise unit that now has to work and rehearse in ways that they had never planned on before.

Typically, when we put companies through a crisis simulation, the first thing we hear is can we do it again, because we assumed, through technology and single-point solutions that we would've had answers, and that we would've been far more effective. This is a people process, technology problem and it has to be looked at holistically. If it is looked simply as a technology issue, then you're missing out on really the real value of what intelligence tells you, which is you are not moving fast enough, and you're not keeping up with what's out there.

From my own perspective, I started my comments just a step prior to yours, which is given the resources that we have, are we structured appropriately in the committees on the Hill to deal with the kind of hearings that the DNC and other hacks will prompt. My own personal view is that until you go to a joint hearing sort of approach on cyber where you have DoD and DHS side-by-side, I don't think you have a full view in terms of all that's out there.

MS. LIZZA: Fatima.

SPEAKER: Fatima (inaudible). How easy is it for hackers to hide their tracks and misdirect investigators? Is there a possibility that a certain actor is being set up and investigators are being directed that way?

MR.LIZZA: Sean?

MR. ROCHE: Okay. So increasingly, as more of this is discussed in the open space about what people are doing, the techniques they are using, the tradecraft advances. So more and more there is a misattribution of and -- hide their tracks. And, you know, the question was asked yesterday, are attacks as prolific or are they getting fewer attacks, but a lot more devious and a lot more difficult to detect? And I would offer that the level of stealth of operating in the space has increased dramatically, and that's because there's been a, I'll say a community of learning. Again, this is a community, either on the bad side, and on the good side, that share, they naturally share. It is a very collaborative community. So, they're constantly exploiting new techniques.

The other thing that's happening, of course, is that digital space is expanding rapidly. So, when we talk about internet of things, one opportunity we have to do, we have to recognize, and we've got a small window, is that we would have to get ahead of that and understand how to secure that edge much better than we did for the previous parts of the system before that's fully prolific, and we only have a small amount of time. So, hiding the tracks, being more stealth, lowering your signature, that's all trends that we are seeing. And this is part of an evolving tradecraft, and the same could be said for the way we maneuver aircraft into enemy airspace. As their integrated radars get better, and their ability to respond gets better, we change the aircraft signature, and we change the tactics we use, which is another big part of it.

MR. HEALEY: And remember, I mentioned those three different broad areas. It's easy to falsify some of those signals. It gets very, very difficult to try and falsify all of them, and the analytical tradecraft on this over the last, especially in the private sector, I'd say, six years, has really just gotten incredible, of them being able to spot that. So it's possible, but it becomes very, very difficult. And look at the TV, the French TV hack from two years ago, that it was supposedly ISIS, and the analyst got through and said, "No, this looks like it was Russia."

MR. LIZZA: Down here?

SPEAKER: Well, cybersecurity is a team sport, so I totally agree with that. I would like the panel to elaborate, the corporate responsibility, in support of cyber security, and really is supporting the cyber resilience in the national level, as well as even in the global level, how the government can leverage and collaborate better with the private sector?

MR. WALSH: From one perspective, what we witnessed was that prior to the high-profile hacks in 2012 and '13 it was difficult for companies to rationalize, setting aside time for preparation and training. That changed with the understanding that with these breaches now comes accountability, and accountability in ways that reach out not only across the technical team, but can include the C-suite, and involves Boards of Directors as well. So, the decision to invest in people, and time, and resources to prepare for eventual breaches, and then the responses that were associated with it, now become something that companies have increasingly embraced.

So, in terms of their responsibility, they have taken ownership in terms of their level of preparation and training. At the same time what they are increasingly realizing that, with the infusion of intelligence, is it's more of readiness model rather than simply a one time a year certification training and focus on individuals. So the ability of these groups inside the network and technical teams to work together is increasingly important, because up until this point they've really been siloed inside their own organizations.

MR. LIZZA: Let's see, right here, in blue.

MS. WERTHEIM: Thank you. I am Mitzi Wertheim, with the MIT Seminar 21. How do you tell this story to the general public in language they can understand? My experience dealing with academics, and whatever, academics write in code. When I first came to the navy, the reports we would get for contracts would be at least an inch-and-a-half thick, and we used to have writers on staff, so they could get it down, so that admirals can understand it. I think so much of what we pay for in terms of contracts are just lost because they're not putting language that anybody can understand. So, my question to all of you is, how do we get it down into language and into publications that we, the general public, recognize what's going on?

MR. HEALEY: It's a great question. I am so glad you asked it here, because so many of the people here are the ones that are going to help, and that's the press. When I started in this business, you know, these things would be buried on the tech pages, it was very difficult to get through, and the journalist didn't really understand. And now I will tell you the translation function they've gotten to right now in being able to try and explain this -- I remember I used to do events with Tom Gjelten from NPR and he said, "I had to take these cyber things and make it so that the guy in the tractor in Iowa could understand," and I will tell you, I think that they are going to be the ones that translate this better than any of us.

MR. WALSH: So Mitzi, I'll give it a shot. So when we were in the navy together, one of the things that your office and others helped us do was to prepare to go overseas. While we served in uniform we went to where the fight was, and that typically was over the horizon, because the away game was something that we wanted more than the home game. Here is where the fight is, right here. This is where the enemy resides. So if you realize that you have personal vulnerability that you're carrying in your pocket, and your trusted device where you keep all your financial information, your personally identifiable information, this is now a problem that we share. So how's that first for a start?

MR. ROCHE: Mitzi, we have got to get some discipline on how we use these words. People are using words during this forum like cyber attack, cyber event. These are all very, very different things. There's a wide lexicon that we throw around that is not very accurate that now. Education in this country needs to start at the most basic level. We teach children how to cross the street. We need to teach them same sort of safety in the electronic world, because they're very good with those devices. Augusta Georgia University, Augusta has started a cyber program. Many others have. It needs to be ubiquitous in our education system, but getting to some common dialogue and doing that accurately is a big part of it.

MR. LIZZA: I think we probably have time for one more question. This gentleman here. He has been very patient. I'm sorry.

MR. ASSAY: It's part of my training. Alan Assay (phonetic) retired govvy. One of my previous tours was a warning officer on the NII (phonetic) warning staff. Has the president actually received a strategic warning notice that this event is different?

MR. LIZZA: Sean, that's a good question for you.

MR. ROCHE: I have no comment on this event. It's an ongoing investigation.

MR. ASSAY: No. Wait, wait, wait. The ongoing investigation is to prove who it was. The issue is whether the President understands that this is different, that they didn't just extract data, that they were trying to reinsert it to affect --

MR. ROCHE: With great respect to your question sir, I'm not going to comment on the --

MR. LIZZA: It's really a question for the White House.

MR. HEALEY: I think Director Brennan's comments yesterday, actually along those lines, I mean General Clapper said, "Let's not get all excitable about this." I think Director Brennan's comments was, if it turns out this was what it was and we are really going to do that et cetera, et cetera, then this is going to be a really significant deal. So, I mean I think that comment from him, where he was really talk about policy, not Intel, he was still talking as the next White House guy, that's where I look for my enter on this, and that was a yes.

SPEAKER: (Off mic) Keep in mind that some of the other questions had to do with how we were going to (inaudible). And if you want to get something going, if you want to get the President picking up the phone (inaudible), that strategic warning (inaudible) is one of the things that does it.

MR. HEALEY: Yup. Great.

MR. LIZZA: And that will do it for us. That's the end of the panel. Thank you very much gentlemen. That was excellent. Thank you.

(Applause)

* * * * *