THE ASPEN INSTITUTE

ASPEN SECURITY FORUM

WAR BY OTHER MEANS

Thursday, July 20, 2017

LIST OF PARTICIPANTS:

JEFF GREENE
Senior Director, Global Government Affairs and Policy, Symantec

BOB GRIFFIN
CEO, Ayasdi

JOSHUA SKULE
Executive Assistant Director for Intelligence, Federal Bureau of Investigation

CLINT WATTS
Senior Fellow, George Washington University Center for Cyber & Homeland Security

SHANE HARRIS
Senior National Security Writer
The Wall Street Journal

STARNES WALKER
Homeland Security Group Member
The Aspen Institute

* * * * *

(3:45 p.m.)

MR. WALKER: Thank you, Rob. Good afternoon everyone. It's a pleasure to be here. I think the stage is set very well for our upcoming session. I am Starnes Walker, I am a member of the Aspen Institute's Homeland Security Group, and I'm the Founding Director of the University of Delaware's Cybersecurity Initiative. Before that, I was the Chief Technology Officer to stand up the U.S. Fleet Cyber Command at Fort Meade and the Executive Director of Office of Naval Research and the Director of Research for the Department of Homeland Security.

Today's session and the discussion really builds on everything we've been talking about today. And the title of our session is War by other means. This is very timely in a sense. If we look back and we look at what we have seen in terms of the Stuxnet attack on Iran's nuclear power, we take a look at the aspects of North Korea's attack on Sony, we have the recent attacks that occurred on the SWIFT financial system in Bangladesh where $81 million was lost. We have continuing efforts across the, in terms of challenging, I would say, the infrastructure of the world, let alone our own critical infrastructure which we talk about is the Internet of things, everything is connected, that means everything is vulnerable, and vulnerabilities occur at seams. So this session will be most important and it will build on today's discussions earlier.

Now it's my pleasure to introduce our moderator, Shane Harris. Shane is a senior writer at *The Wall Street Journal*. His responsibility covers intelligence and national security. He's the author of two books, *War: The Rise of the Military-Internet Complex,* explores the frontiers of our new cyberwarfare capabilities. A book called *The Watchers,* tells the story of five men who play central roles in the rise of surveillance in America, which has been again a topic of discussion this last year.

The Watchers in fact has won the Helen Bernstein Book Award for Excellence in Journalism. *The Economist* has named it as the one of the best books in year 2010. And prior to joining *The Journal,* he was the senior writer at *The Daily Beast* in Foreign Policy. Thank you very much.

(Applause)

MR. HARRIS: Great. Thank you all for being here for the last of our full panels before we go on to hear from Director Pompeo.

Let me just make brief introductions to everyone here on the panel so you can get a sense of the breadth of expertise that we have here, and we're very lucky to have all of these people together for this topic. To my left here, Bob Griffin, who is the CEO of Ayasdi. And I got that right, didn't I?

MR. GRIFFIN: You did.

MR. HARRIS: I did. All right.

Josh Skule from the FBI. He is the Executive Assistant Director for Intelligence for the Bureau. We have Jeff Greene who is the senior director of Global Governance Affairs and Policy at Symantec, Internet security company. And Clint Watts, formerly of the FBI, now Robert A. Fox Fellow at the Foreign Policy Research Institute. And if you like to watch congressional hearings you know this is the first man to become a celebrity out of a congressional hearing. It's how everyone breaks out. Right, right, exactly, exactly.

So I wanted to actually begin this panel by briefly looking back to a year ago when the security forum convened, we were just learning about the hacking of the DNC, and at that time officials had not come out publicly and officially said that Russia was behind that event, but it was a pretty much becoming sort of a known fact. And the Aspen Homeland Security group actually put out a communiqué at that event on election system security which said, I'll quote here, "Voting processes and results must receive security akin to what we expect from critical infrastructure." And when we talk about critical infrastructure in this space, just so we're sort of setting the table with the terminology, we're talking about big stuff, we're talking about power plants, nuclear facilities, communications capabilities, transportation. There's a long list of it, but the kinds of things that are the nuts and bolts of many ways of what keeps the country going. So that was a year ago.

Just a couple of highlights of things that have happened since then, and of course we've come on to learn much, much more about the Russian interference. About a dozen U.S. power plants, including one in Kansas, were believed to have been probe possibly by Russian actors. We've seen attacks that cut off the power in Ukraine, also believed to be Russian actors in that case. In Ireland energy networks were probed just this month according to reports. We saw the massive WannaCry ransomware attack which wreaked havoc on multiple continents, a Botnet attack that took over the so-called Internet of things, all those devices in your houses, your washing machines and your thermostats that are hooked up to the Internet. And cyber attacks that have crippled activities at shipping companies like Maersk and Fed Ex, actually stopping -- in one case caused the Honda production plant domestically to shut down because of one of these massive attacks that were spreading.

And that's just a little bit of the highlights of things that have happened in the past year that are affecting critical infrastructure. So when we talk about these threats, these broad cyber threats particularly from nation states, you often hear experts and policymakers for the past several years saying we're kind of in a pre-9/11 moment when it comes to cyber, or the cyber Pearl Harbor is coming.

I want to throw out though a question for the panel to start us going which is is it time to retire that metaphor because from where I'm standing covering this and I think probably from a lot of experts' respect is it seems like the calamities that people were worried about are already here. And they may not necessarily have led to loss of life but we now have an environment in which elections are being interfered with, power facilities are being shut down, business is losing revenue, massive disruptions because of cyber. So are we -- should we just get rid of the whole pre-9/11 moment and just acknowledge that we are in the bad thing that we have all been anticipating. Maybe you like to start.

MR. GRIFFIN: I think that's a great question, I think the answer is yes. I think -- I don't think we have to worry about the next Pearl Harbor type of attack. The realities are here people are preparing for today, we

started -- you see the probing activity that goes on, people are starting to look at ways that we can start producing cascading failures which will drive to a critical infrastructure shut down. You know, it's interesting, I was having a conversation at breakfast and we were talking a little bit about critical infrastructure protection, and while we all start to look at things like, you know, what can we do proactively from a technology perspective to look at anomalistic behaviors to predetermine if there may be an event and be prepared for that event, there are policies and programs and procedures that we have to look too that can take these things into consideration that we aren't even prepared for.

Let me give you a little story, a quick example of that. Did some research out in the Hawaiian Islands about protecting the grid, in particular for some activities were doing some time ago for Pacific Command and the challenge in the Hawaiian Islands is if you lose the grid it could potentially shut down not only Hawaii but Pearl Harbor, and that's the largest combatant command, one of the largest combatant commands in the world. And you have to be prepared for those kinds of things.

Well, what's interesting is across the Hawaiian Islands from the Aleutian Islands down to the Hawaiian Islands were a series of buoys. And those buoys do things among other things like provide early warning for tsunamic activity. In Hawaii that's important? Well, if there's a tsunamic wave heading toward the Hawaiian Island you want to know that as early as possible because you want to orderly shutdown the grid so you don't short the grid out, have these challenges.

Well, there's a program in Hawaii that we discovered called Dial-A-Buoy. And Dial-A-Buoy is if I'm a surfer and I want to learn what the wave rate is and the temperature the water is I dial a particular buoy number and call and the buoy will say temperature is eighty eight degrees, the waves look at this rate, it's a good day for surfing. Problem is what if the bad guys spook the buoy. And the buoy says tsunamic warning happening. Well we don't have to worry about the bad guys shutting down the grid, we'll shut the grid down, because that's the standard operating procedure. So while we talk about all of the collective issues around Internet of Things, and I worry a lot about those kinds of things, so forth, we ought to look

at more than just the broad set of challenges around things like just what technology can do, what it is we also do from a procedure and process view.

MR. HARRIS: Josh, let me ask you the same question, and at the Bureau, I mean obviously 9/11 is a transformative event, it very much repositions the FBI into a role of having to predict bad things that are going to happen or to at least anticipate them. I mean, are you all moving past this idea of we're at a kind of on precipice of a big moment when it comes to infrastructure attacks and just recognizing that we're already in it or do you think that that's the wrong way to think about it?

MR. SKULE: No, I think that's the right way to think about it. I mean, I don't know what precipitous event would cause us to be more concerned, right. We have ransomwares on the rise, we have a slew of nation states out there that are looking to attack, you know, our democracy, they're looking to take advantage of us economically, financially, change our culture, whether you look at, you know, Chinese investment inside the United States, which has increased threefold in 2016. Despite their agreements not to potentially attack us economically, I'm not sure that they stay to that agreement. So I don't know what other events that we would need to do, and it really goes to the FBI and DHS and other USIC agencies partnering with the private sector in a very transparent way that we can move information at the speed of technology, that we leverage technology amongst not our USIC and our law enforcement partners but also with the private sector.

MR. HARRIS: What's your best guess, just staying on this theme, we've seen obviously this really rapid escalation and probing of infrastructure and in some cases even, you know, you might even qualify it as attack on infrastructure in other countries and so far as shutting it down. What is the FBI, or your best guess, for why nation states feel compelled to do this? Why are they poking us in this way and presumably knowing that if they were successful in triggering something like a blackout it would presumably, I think, trigger a pretty massive response and maybe not just via the Internet. What's their motive maybe?

MR. SKULE: Yeah. So that's a great question. I think nation states are positioning themselves to be at an advantage, period, right? And that's how they think of it. It should come as no surprise to this audience that there's others out there that would not like to see the United States thrive. You know, whether it's China, Russia, Iran North Korea, they're looking for us to be -- take a second seat to them, whether that's militarily, financially, as I said before, culturally, they are looking to be the world power, and they look to destabilize what we have in our country in order to do that.

MR. HARRIS: Jeff, do you want to, from the point of view of industry and you all at Symantec are in the thick of it when these attacks break out of trying to analyze them quickly. Does it feel like a pre-9/11 moment to you or are we well past that?

MR. GREENE: I think we're well past that. You know, I remember that I was working this issue in the Senate 7, 8 years ago, and I always took out big red when I saw a draft speech from my boss with cyber 9/11 or cyber Pearl Harbor because I don't think it's helpful. I think it -- yes, we're in the thick of it but I also think we need to think about what message that conveys. People hear that, you can have one of a number of reactions. Some people are just going to freak out, some people are going to think, well, this is hyperbolic and just turn off and not read the rest of it and hear the important conversation about just how vulnerable we are. And some people are going to think, well, there's nothing I can do personally or the government can do, and I think that is equally destructive.

In cyber generally one of the things that consistently worries me is the constant drumbeat of all these bad things happening creates a view among folks that there's nothing they can do to protect themselves, and that's not true. On an individual level there's a lot of things people can do, but things like talking about cyber Pearl Harbor, cyber 9/11 I'm afraid convey, even if it's theoretically you could have infrastructure damage that would cause mass casualties in individuals, I mean citizenry, at an individual level it puts the threat far beyond what the average Joe is facing every day.

MR. HARRIS: Kind of drilling down on the variety of infrastructure issues that we've talked about here, probably the one that I think people in your position take the most seriously in terms of the greatest disruption that could be cause would be one targeting the energy sector. So we talk a lot about the grid and, you know, a blackout, and let's be clear, I don't think anybody is contemplating a scenario where all of the power across the United States is lost, the grid is quite disjointed and disconnected, but the possibility of a major blackout or a power disruption in a large metropolitan area and the cascading effects that would come from that are something that are, seems quite real and that people are preparing for.

So let me just throw this out to whoever wants to respond to it, I mean, what, a, what is the motivation do you think behind countries that are doing that. And, b, where are we in terms of the spectrum of things that we need to be doing and that we hopefully have been doing for many years to get prepared for that kind of an event.

MR. WATTS: I'll talk to it a little bit. So when we are watching, you know, J.M. Burger (inaudible) watching the influence around the election, what was most startling in a lot of ways aside from the presidential debate was how hacking powers influence, whether it is, you know, hacking personal information, dumping it on the Internet and changing people's opinions, or taking real-world incidents that occur, amplifying them or hacking infrastructure to create fear in audiences.

If you're a nation state you can do both, if you can hack in and also manipulate or control an audience you can amplify that to a great degree. We witnessed it with the Russian troll operations. If there is a security incident inside the United States, airports close down, a shooting, they would amplify that as well because it incites fear. When you are scared you will do things you will not normally, you know, consider or contemplate.

So I'll give you an example, which is Hurricane Sandy. Most of the models about how people would respond if they lost power or ATMs or power grids were wrong. We thought it would take longer for people to panic. They actually are making runs on ATMs. You remember we had gas lines like we've never seen, and you would have thought it was 2 days from *The Walking Dead.* If you were in New

Jersey during Hurricane Sandy. There was that kind of a fear around there. That was something that was just a manmade disaster. But if you're a cyber actor and you watch that in terms of modeling, if you can influence an audience base and then create a real world provocation like a dark energy attack that you saw in Ukraine or instill fear the power's not going to come back adequately and you need to make a run on certain sorts of supplies, I think it's not just about the energy sector or the banking sector or any one sector, it will ripple into all of them.

And how do you quell that panic? You know, I think in the U.S. base I've seen people meltdown if they lose Wi-Fi for 5 minutes. And so think about if we had 3 days with no Netflix and, you know, in all seriousness and all power, you see weird manifestations in the American public that you don't see in other places. And so that's what concerns me about the crossover between the two.

MR. HARRIS: Now, it seems like we -- even in the run up to the election I remember there being, a, a fear about Russian interference with voting machines, right, which seemed a pretty remote possibility. People I talked to, the greater concern was that if the rumor that voting machines had been messed with or there was a rumor of disruptions at polls that that would cause sort of a cascading effect. So I mean it seems like what we're dealing with here is, a, the physical threat which is hard enough to manage, and then, b, the psychological impact of it and that the people who are probing the systems know that know that, no?

MR. GREENE: You made a really important point about motivation. So we know that there are entities probing our electrical system. You talked about, you know, several things you talked about is highlights for the past year. Well, they're still going on. The activity that we heard about in the past few weeks, probes the energy grid, we reported on that same group in 2014 and then said had been going on since 2011, it's still going on today. So you bring the question of if that's happening why has nothing bad happened, because you talked about earlier, the repercussions would be significant. So in terms of where we are as a nation, the folks I've talked to, Symantec, government and otherwise, you know, our view is that we're at a point where a competent state actor, yes, could have

an impact on the grid. It would be pretty tough for a criminal gang at this point at least in the U.S. But more importantly is why would they.

The criminal gangs work to make money. There's not a lot of money in causing -- maybe unless you were shorting a stock ahead of time, but there's not a lot of money in trying to take down the grid. And more importantly, all those groups have a home base. If a group from country A took out the U.S. grid we wouldn't just look to that group we would look to that country. And an organization sophisticated enough to impact the U.S. grid is more than likely going to be known to the country or we're going to assume they are. There are lot of motivations that work against an active attack on the grid.

MR. HARRIS: Josh, yeah.

MR. SKULE: No, I think that's right. I mean, I think that you have essentially different sets of actors out there, you have nation state actors who are looking to posture themselves in order to position themselves so if we were to cross a proverbial line that they could take action, I think that's one. And I think they won't take action or they don't take action because of the consequence. And then you have criminal actors who are, what Jeff said, looking to make money.

There's also another subset of that, and we've seen that in some of the malware where some are just looking to watch bad things happen and see what happens out of that. And I think that's probably more dangerous than the criminal element that wants to make money because they -- because can you track -- at some point you can track them, they're going to want to get their money.

MR. HARRIS: So somebody who just wants to --

MR. SKULE: Cause chaos.

MR. HARRIS: Cause to watch it burn essentially.

MR. SKULE: Yes, essentially watch the world burn.

MR. HARRIS: Yeah.

MR. GRIFFIN: And it's interesting. As we've moved from, what I would say, nation state terrorism to market state terrorism, right, you get various different set of players. And I think those that are involved now, to your point, are looking for a sociological disruption, but they don't really -- they don't have necessarily an ideology, they are looking for how quickly can I disrupt and cause widestream panic. And with their growth and explosive opportunity sets in technology today that enables everybody to participate into the creation process with the ability to buy off the dark web, you know, template-based malware programs and disruption programs it is enabling more and more people to become non-state actors.

MR. HARRIS: So let's put this in some real context. If today I decided I wanted to abandon my career as a *Wall Street Journal* writer and go out and hire somebody in the dark web to go out and launch an infrastructure attack on a power grid in a minor metropolitan area, and, let's say, I had unlimited resources to do it, conceivably how easy is that? What obstacles would I face in doing so?

MR. GRIFFIN: Very little, very little. If you can navigate your way across, or you can find somebody to navigate your way across the dark web you can find people that are willing to participate. Again, their motivation is economic. It's the ultimate pay-for-performance job, right, they don't get paid unless they do things that cause them -- value expressed. I think it would be incredibly -- I think the barrier to entry for somebody to be able to do that is minimal at best.

MR. HARRIS: Josh.

MR. SKULE: The only thing I'd caution you against, Shane, be careful who you talk to in the dark web.

MR. HARRIS: Well, explain that.

MR. SKULE: -- show --

MR. GRIFFIN: Absolutely.

MR. HARRIS: And I always --

MR. SKULE: I'm just saying. So right -- both good guys and bad guys operate in the dark web.

MR. HARRIS: Which is my next question --

MR. SKULE: -- and so which helps us to, you know, defend the United States against, you know, anything from terrorism to cyber actors, whether you want to talk about it as a modality or spies, criminal organizations operate off the dark web and so, yes, we have a great relationship across the intelligence community, we have deconfliction methods in place in order to combat some of this, not all of it. I mean, obviously the Internet is vast, but we've been very successful in combating everything from the terrorist in Iraq with a smartphone in his hand and working through the inter-agency in DOD to help combat that to spies to criminal organizations all operating on the dark web.

MR. HARRIS: So in the way that the Bureau classically has informants and people they work with to try and learn what terrorists are doing in the physical space, there's an analog then in the dark web to that?

MR. SKULE: I think the world, I think the United States needs to get very comfortable with the fact that the virtual and the physical are now becoming one and the same. And so, you know, smartphone tracks how you move, how you walk, how you -- how many steps you've taken, you know, those things are all -- and we're all interconnected, and so the defense is really what we should be talking about, paying attention to, you know, your home security not just in the sense of the physical but in the virtual.

MR. HARRIS: Just to stay on that for just one second, does the bureau have the sort of statutory, the legal authorities, the tools to do what it needs or what you feel it needs to do to combat this in that space, are we -- or are we, to borrow the pre-9/11 metaphor, in a place where before 2001 the Bureau would have said there are impediments to our ability to protect physical terrorist attacks in United States.

MR. SKULE: No, I appreciate that question because I think one of the greatest debates we have right now is 702, and often we think of 702 collection in the realm of just terrorism when in reality what we use it for

is all of our national security tools, and it's not just there interagency that benefits from that, it's domestic landscape that helps keep us safe. And so to what Tom Bossert said this morning and how he explained it, I could not agree more. 702 is a critical national security tool to keep our nation safe.

MR. HARRIS: Let's talk about the Russian bear in the room. So I assume nobody on the panel would dispute the Intelligence Community's conclusions that Russia did interfere in the election. Let's go ahead and ask that pro forma, we'll get that out of the way since every panelist now on this topic has to be asked that question.

Clint, I want to go to you first because I think that you've obviously very closely studied many aspects of the Russian interference campaign, particularly we talk a lot about the hacking of the DNC, the leaking of e-mails, that's the piece that people are probably most familiar with. But talk about your expertise in your area of the use of social media and trolls and bots and give us a sense too of the level of sophistication of that Russian campaign. I mean, it's not -- this is not the first time that we have seen Russia use these tactics and techniques in an election context. This is first time perhaps here. But put this in perspective for us of the sophistication, I mean how big of an operation was this, or was this actually sort of pretty low grade stuff for what the Russians did?

MR. WATTS: Yeah. So I'm going to -- I'm not going to talk about Trump-Clinton, because I'm pretty bored with that, and I think most -- everyone is. But I think there is some important things that haven't been discussed in that, and that is, you know, when we started watching it, it was January, February 2014, and so we, you know, I always characterized troll armies as, you know, hecklers hackers and honey pots, and, you know, the hackers or taking your information, compromising your systems. And they were hitting corporations as much as they were hitting political opponents. At the same point we saw this sort of heckling or trolling activity and we forget that they perfected these active measures by doing it on their own population first.

They do this inside Russia and they use these techniques to sort of bubble their audience. And I think the important part is really what happened in 2015. The

reason Russian influence on social media work was because they worked at it for a very long time. They're not like Americans. We want to influence people and win them over in on one quarter or 30 days, and if it doesn't work we then talk about how the guy who made that program sucks, let's quit it and move on.

The Russians don't do that. The Russians are in it for the long haul and that's because they see it not the way we do, it's national security in a world of audiences now. You are linked with people that share your views on social media. In your communities right now you live in gerrymandered political districts where you are physically surrounded with people that just think like you, you are on social media sharing information with people that are just like you, we will all share our discussions from here today with each other and people like us and there's a whole another part of America that either doesn't believe this exist or has even heard about it.

And so what the Russians were able to do was to smartly test in 2015 all of the audience in America, every one of them, they would try everything. They don't try and figure out who can be influenced, they try and influence everybody. And when they see success they reinforce that. And they were winning over audiences in 2015 so that when 2016 came around they had options to nudge them in directions that they wanted to. They win audiences then they direct them. They still own audiences in the United States today.

Black Lives Matter protests, Bundy ranch standoff, Jade Helm exercise in Texas, they were there in a big, big way. Active measures is about exasperating political divides. It's about fomenting chaos. It's about undermining confidence and trust in elections and elected officials. It's about sowing chaos and distrust between information sources that you can't distinguish fact and fiction. And when you're scared you will fall back on your gerrymandered communities and your social media bubbles that you're in. The idea is to reinforce your audience, always reinforce your audience and to try and keep them.

And so when you fast forward it to 2016 on election night I was not worried about who won or lost, I was worried about Pizzagate times 100. What we were watching in those social media feeds was if someone's

candidate doesn't get elected could they be manipulated by a foreign actor to show up and commit violence. That phenomenon that you're seeing right now continues today. We've got a huge cancer in our country, and that is that we are completely bubbled from each other. To have an effective democracy, if you go back to Tocqueville, that was to have overlap. We had social capital, we exchanged ideas.

I have a Facebook feed, I'm from Missouri. There are people that want to kill me right now because of my comments about the election meddling and don't believe it, things that happened to me, like being cyber attacked. "No, it didn't, that is fake news." I'm like, "No, these FBI guys came and told me it happened to me, I didn't know about it." "You're full of it, you don't know what you're talking about." So we -- I think what we really should look at is if you have that power to control or influence audiences when things don't go your way you can shift them, and we need to stop talking about as Russian active measures and start talking about American active measures, which is how people are bubbling themselves, how different audiences are segregating themselves out.

And it doesn't matter if it's left or right, Democrat or Republican, we're in a very dangerous space such that when a real hacking on infrastructure happens we toss blame back and forth in different ways. Audiences are manipulated. We don't trust a company that's maybe in defending us even though they're doing a great job because the other opponent doesn't want to take responsibility or credit for it. So we're getting into a weird twist where if you're in this like Russian space you can really control and manipulate audiences and do your bidding while they fight amongst themselves, and we are already there in this country.

MR. HARRIS: Let me ask a question to Josh, and -- but anybody respond to this. Please, go ahead, respond.

MR. WATTS: Just if I can say, I don't care about the GOP or the Democrats, it depend on what website you go to, I'm either a shield for Clinton or a deep state operative of the Republicans, it's hard to pick.

(Laughter)

MR. WATTS: But my point is that this election audience, you know, sort of dynamic that happened on both sides continues today, and it is visceral and it's the biggest challenge I think we have in our country right now aside from election meddling and those sorts of things.

MR. HARRIS: And I think another point of this is I mean you talk about them having already captured the audiences in a way you could think of it like their infrastructure. Something that kind of gets lost in the Intelligence Community assessment that came out late last year about this is that the Russian operation did not start out per se to elect Donald Trump, right, they had a broad spectrum of goals and ambitions and various things happened along the way. And what you're describing is one that was probably more successful perhaps than even they had anticipated that it would be.

MR. WATTS: I think it was way more successful than they anticipated.

MR. HARRIS: So, well, Josh then a question for you, I mean, a, would you agree with that. And then for the -- from the bureau's perspective what -- how does that set the stage now for 2018. So there is this landscape that Clint has described that we're all now familiar with, the adversary is not going away, they're inside the infrastructure, they're inside critical infrastructure too, but -- so how does that -- so what does 2018 look like for the head of intelligence for the FBI?

MR. SKULE: So your first question was do I agree --

MR. HARRIS: Do you agree the success, yeah.

MR. SKULE: -- well I -- so just judging by the fact that I've been here all day and on almost every single panel we've talked about Russia, I think they would determine that they have been successful, right, I mean I don't think that Russia is having a private public media moderated event to talk about the United States. So I don't.

For 2018 I think, first of all we learn, just like they learn, right. So, you know, we have all 56 field offices were setup for 2016 to be on alert. We had reps

that were assigned to be electoral reps for each of those. We worked very closely with DHS on those and other inter-agency partners to make sure that we are postured in the right way. I think our posturing going into 2018 will be enhanced. I think our knowledge base both working with the private and public sectors will be enhanced. And I think we will position ourselves not just in the FBI realm but working with DHS and other community members.

MR. HARRIS: And what can the FBI do to stop it? I mean, what can you do to go out and prevent these messages from being spread or these bots from infiltrating and infecting the media stream? Is there anything you can do?

MR. SKULE: So I think we can do what we've continued to do, right, which is stay true to what we know to be the truth and stay away from providing opinion on what would be things that we can't attribute to actual state actors or other activity. I think we can stay in our mission, uphold the Constitution and protect the American people. And as long as we stay within those confines, leveraging the totality of the community to do that, you know, I think we work very well to -- whether it's NSA, CIA, DHS, to make sure that we are posturing ourselves inside the domestic architecture and then conveying that information frankly to those that need it, which whether that would be a law enforcement entity or a public or private company.

MR. HARRIS: So let's take a company like Facebook, for instance, which is where so much of this gains currency. And I would argue that in the information landscape Facebook has become a critical infrastructure, and so far it's how people get information. And it's been documented how fake news spread through that channel. Should the FBI be doing more, can the Bureau be doing more to share information with a company like that to say, look, there is a hostile actor, it is spreading information through your system, it is getting out to your users? And should there be things that law enforcement should be able to do to compel a company like that to take action against it, do you think?

MR. SKULE: I'll start with the latter question, compel. I think that's more of a policy discussion, so that's where I'll lead that one. As far as being a data

pointer telling industry or companies or Facebook particular like, hey, we have noticed that there's an actor, whether it's Russia, China, Iran, North Korea on your system, we do that already, DHS does that already, other community members do that already. Could we increase our posture in that arena? Sure, we can. We're having great discussions right now with the private sector to understand what is the most important to them so that what are they protecting so that we also know in the government infrastructure what is it that the bad guys are trying to achieve inside those companies. So outside of Facebook but other industries as well.

MR. HARRIS: Let me ask a policy question. I may go to Jeff for this first because you used to work on the Hill, so you used to make policy, so you can put that hat back on. This question came up yesterday in the conversation with Secretary Kelly where he said that, you know, despite the fact that nearly every state during the election in 2016 did come forward and ask the government for help, the state's message to the feds right now seem to be mostly we don't want you involved in our elections, we don't necessarily want your help and what DHS may be able to do.

But if we're going back to the idea articulated here a year ago that election infrastructure is critical infrastructure, there is clearly a federal role for protecting critical infrastructure from foreign adversaries. What should -- shouldn't the feds be getting in more into this and basically saying you're going to take the help even if you don't want it?

MR. GREENE: So I appreciate the generosity of the assumption that the Hill makes policy nowadays, that's perhaps questionable. But -- so there are lot of pieces to the entire election infrastructure, and the one -- you start with the fact that we're a federal system, the states and locals run it. Then you look at how an election can be influenced or changed, you can try to change with tallies and you can try to change influence. I think right now where we are, we're relatively good place, for the most part, in terms of massive changes in vote tallies. We have shown how individual machines can be compromised. We did a demo on it the last year. But in order to do that at scale you would need an incredible volume of people spread out in a large geographic area, spending a lot of time on

machines. Someone is going to notice what's going on, someone is going to call the FBI's involvement. You're not going to be able to do in my view the kind of attack you would need to or the kind of structured operation to affect individual machines.

So where the feds can help is, number one, providing guidance. The designation of critical infrastructure carries a lot of baggage going back to the, here we go again, post-9/11 days. And mandates on the states is not what was envisioned, it was more guidance. And I think when they got out and had the one-on-one conversations it was a lot more effective. But the thing the feds, the area the feds really need to be involved in is that not the subversion but the shifting policy, the shifting people's views, going back to the fake news. That to me is what worries me more in 2018.

I'm not even that worried about, I would like to think that most campaign managers, Senate, even congressional are going to have their e-mail systems fairly well protected. But that's not going to stop an adversary from generating fake e-mails. And those are going to go out and then we're going to be in a discussion over whether it's real or not. And as Clint pointed out, there's going to be huge segment of the population that's going to believe that that fake e-mail is real.

MR. HARRIS: So what would the federal government's role exactly be in dispelling fake news then?

MR. GREENE: It goes back, I think, to a couple panels. We need to put better deterrents in place for actors that might do that.

MR. HARRIS: Okay. I'll ask another question, it's been brought out before, how do we credibly implement such a policy when the President of the United States will not acknowledge that Russia interfered in the election?

MR. WATTS: I'm begging you for this one.

MR. GREENE: I'm happy to let him have this one.

MR. WATTS: And I know Josh for sure can't comment on that, so I'll take it. But I don't think the government should be involved at all in policing fake news,

it's a disaster waiting to happen. Any way the government tries to do it they will have to take on responsibility for thought police, and it undermines what we're about, right, freedom of speech and freedom of the press. And so I also don't believe in tagging and tracking every fake news story, it's impossible, right, I can make fake news faster than you can refute it. I'm very good at it, my government trained me to do in the counterterrorism area.

But in all reasonableness, you know, the approach that we having watched this over many years, I have advocated is what I call the nutrition label or information consumer reports system for news, which is you develop a rating system in an independent agency that works with social media companies so when news stories come up on your feed or in your social media feed, the outlet that actually makes news is rated over a time period against many different variables. What's their accuracy? How many retractions of the issue? Do they have an editorial board? Who is the financing system behind this? What state sponsor does this.

And so that when it pops up in your feed it says this outlet is 90 percent true. And if you come up on a really crazy fake news group they get 10 percent. And then it's your decision as a consumer whether you want to read garbage or not. If you want to read the National Enquirer and believe every story that's in there, that's on you. But the problem in social media and the Internet is I can make a fake news site that really grabs at you way faster than you can ever figure out if it's real or not. And if you look at some of the good stuff, BuzzFeed has done some really good work on the top five fake news stories that traffic through there or whatever. If you look at those websites most people go I have never heard of those websites and some of them are even gone. They pop up and go down.

And so I think there are other models that we can use in the private sector that help protect American values and keeps the government from having to do thought police, which I feel like is an impossible mission for long.

MR. HARRIS: I want Bob to jump in here.

MR. GRIFFIN: You know, I think you make a valid points, it's difficult for the government to legislate that

kind of activity. But it's -- you know, to your point, this is not new. I mean, it came to highlight in the last election. I mean think back to 2013 for those of you that may remember the AstroTurf or the fake tweet that supposedly was attributed to *Associated Press* that went out and said, explosion in the White House, President Obama injured. And in less than 6 minutes the Dow drops 140 points and that the S&P loses over a $138 million in value, right, that's the power behind what can happen quickly because we are in an instantaneous consumer society, we want to consume information in the way that we feel comfortable with. And unfortunately a lot of people feel comfortable in social media aspects of consumption. And effectively bad actors have turned social media organizations' capabilities into what I would say, I don't know, smart bomb delivery devices, right, because you can target very precisely populations, groups, individuals and, you know, people want to believe what they see.

MR. HARRIS: I want to turn to the offensive component here that the United States has. We talk a lot about things that people are doing to us, we have a lot of capability to do things to other people. In the context, I want to stay a little bit too in this area of external threats to critical infrastructure. We're talking a lot in the past few years about deterrence, and is there a deterrence theory in cyberspace and what can we do to demonstrate to other nations that they should not try anything too catastrophic with us, and we can argue how successful that's been. But I want to posit the question of does there need to be some kind of demonstrably show of force on the part of the United States? Let's take Russia for instance, I mean there are plenty of covert things that we can do to Russia, maybe we have, I don't presume to know all the things that we have done in response. There's been a lot of talk about whether the sanctions were too tepid or not forceful enough. But does there need to be something to do that we do that demonstrates both to Russia and the world this is what you get when you interfere with our system?

MR. GREENE: I don't know that we need to go that far yet. I think a starting point may be a more public discussion of just what capabilities we have even if at the highest level if you go to the Cold War analogy we were able to set policy negotiation, panel talks to talk about nuclear policy because it was no secret that we had nuclear

weapons, we didn't publish the plans to our latest warhead, but it was known we had X missiles and they had independent reentry vehicles. We're not there with cyber because of the level of secrecy. I'm not saying that we should go out and say we could take down this plant in Kiev and this plant in Beijing but perhaps if we had a more public discussion over, yes, the U.S. could impact critical infrastructure if forced, et cetera, with all the appropriate caveats.

I don't -- I do think that the level of secrecy around it limits our ability to have those types of conversations and to create deterrence. And I - the genuine question, I'd like to know what is the downside to acknowledging what is pretty widely accepted, do we get a benefit out of this strategic ambiguity because it seems to me like it is hurting our ability both to develop policy and to use it as a deterrence tool.

MR. HARRIS: Josh?

MR. SKULE: So I think we have the greatest country in the world with probably the greatest capabilities in the world. So I think to what -- my question would be to what would a show of force, what would be the determining factor, why would we need to do that, did they cross -- despite the fact that folks disagree with certain policies or they disagree with the sanctions that may have been placed on Russia, things were done. And so that would be my response. What are we looking to achieve when I think it's widely accepted that we possess the greatest capabilities in the world.

MR. HARRIS: Bob and then Clint.

MR. GRIFFIN: So let me change it a little bit from a different thought process. I don't worry much about our show of force from our governmental perspective. Most of our work is done in what Title 50 traditionally versus Title 10, and I think it's going to stay that way, right, it's deniability.

MR. HARRIS: So secret, not acknowledge publicly, yeah.

MR. GRIFFIN: Right, right, right.

MR. GRIFFIN: Here's what I worry more about. I'm the CEO of Sony and I'm really pissed off that this nation state that somebody has not proven to me has taken down my world, you know what, I get the smartest guys coming right out of Stanford University or UCLA or, you know what, let me go put them in their place, that's the escalation piece that I worry more about --

MR. HARRIS: Great point.

MR. WATTS: It's exactly what I want talk about. I think we heard this morning that dot-com is on your own based on the discussion that was in here. We saw 3 to 4,000 Americans allegedly be cyber-attacked, I got to enjoy some of that. If I'm not protected by the government, you know they provided me notification and I appreciate it, but if I'm not protected about it and I'm provided no means to do anything about it, how many times do I need to get hit by a cyber attack if I'm a company or a person before I start to look at I have to protect myself or, you know, sustain my business. So in my case I'm going to do some things in the coming weeks and the Russians are going to cyber attack me again. And this has happened before.

And when they're done cyber attacking me and stealing my information, they're going to dump it out on the Internet and they're going to hope you guys in the media, you know, start taking me out of the game by reporting on it. So let's say if I'm not protected by dot because I'm in the dot-com world, then why can't I retaliate. If I know who the hackers are that hit me and, oh, by the way I know who some of them are because they left some of their stuff on the Internet, and I know where the dark web is, am I allowed to go do that? This is just going to happen, you know, if the U.S. government doesn't set up a policy.

You know, it was funny Putin's, you know, lie was it was patriotic Russians that participated, you know, in the influence. Well, what if patriotic Americans stop and go, you know what, there are lot of protests going on in Russia right now, maybe I want to support those, so I do. That's why I think the policy part of it is extremely important right now because we're at a threshold I think in corporate America and in -- and just civilian America where people are going to start sticking up for themselves if the government doesn't come up with a policy and you don't know

how many times do we have to see public officials, government officials. If someone had robbed Colin Powell's house and taken his letters out of his house and dumped them on the e-mail, you know, on the Internet, we would be talking about a massive retaliation. Iranian DDoSs against the banking sector in the United States have cost billions of dollars. If they showed up in New York City and stole a $100 million from banks we'd be going to war, but we treat it completely different in cyberspace.

MR. HARRIS: So that begs the question then, okay, so Iranian DDoSs have caused all of this problem with the financial sector, why is it a bad idea for the United States to respond and say we're going to proportionally take down a portion of your financial sector for 48 hours or whatever, cause you a lot of problems, cause a commensurate amount of damage and we are going to announce to the world that we did that, the same way that we immediately announced that we had bombed a base in Syria after the chemical attack?

MR. WATTS: I don't know. But I think my concern is the policy ambiguity, and this isn't just about today, this goes back 10 years now, has reached a threshold where to be competitive as an American company or to survive even as an individual that maybe doesn't take a stance that Russia or China or Iran or some actor doesn't like, you are now putting yourself at risk and also told you can't do anything about it. And so it's going to put America in a very tough vise, I think, in terms of cyber, so.

MR. GREENE: And the response, you talked about, I think if it is, a, part of a larger strategic policy that we have adopted as a country and, b, consistent with norms that a large number of nations have agreed to then, yeah, it makes sense. But if we come out of the blue and just respond to it, I don't think we're going to get the result we want because there's going to be in the international community a discussion about are we evil ones --

MR. HARRIS: And there are no international norms --

MR. GREENE: It's hard to have those conversations.

MR. HARRIS: Right. Right. Let's turn to questions from the audience, we have about 10 minutes left so we have plenty of time for questions. I'll go first in the back there and then to Julia right here in the middle.

MR. AUL: I guess Richard Aul (phonetic) with the University of California. I've read that if a bad actor such as North Korea were to lob a non-precision nuclear weapon at high altitude over an area of the United States that the electrical grid system could be destroyed over an extremely wide area. My questions are relating to this, is this true, is it possible?

Secondly, I've read that U.S. agencies are not responsible, U.S. agencies are only allowed to protect U.S. government agency assets, military or security, whatever, is that true? Is any part of the civilian U.S. grid protected? Is it possible to protect the grid in any way anyway? If they were not protected why not or how does that get --

MR. HARRIS: Okay. There is a lot of question.

SPEAKER: I'll leave that you guys.

MR. HARRIS: First that EMP question because this always comes up in the context of cyber and electromagnetic pulse and air burst, if you will, being an equally grave threat to -- Bob, do you want to address that?

MR. GRIFFIN: No, it's a threat. Just like solar flares, plasma clouds, right, if there's a plasma that heading toward Earth and it's likely to enter the atmosphere at a particular occasion you want to do an orderly shutdown of the grid because otherwise you'll overcharge the grid you'll have problems. The biggest risk you've got is when those things happen and you do physical damage. There aren't a lot of people that manufacture parts for the grid. And they don't make them sitting around waiting for you to call to say I need a new turbine or I need whatever. They could take six to eight months to manufacture it, and that's the big risk, because you're -- so.

MR. GREENE: And it won't be manufactured here, it's going to have to --

MR. GRIFFIN: No, it will be manufactured -- exactly, shipped in.

MR. GREENE: The major pieces of the grid that -- they're susceptible to a rifle shot just as they are to a solar flare.

MR. HARRIS: Josh, can you address the question, it is a good question about what is the authority of the U.S. government to protect outside of the U.S. government assets. I mean, we think obviously the military is responsible for our border defense, we have an air defense, what's USG responsibility for the, you know, the dot-com space if you will.

MR. SKULE: So I think what -- you know, DHS has responsibility for our critical infrastructure, you know, PPD-41 puts us in the investigative role and then the ODNI and the --

MR. HARRIS: Well, not literally protecting it but working with industry to protect it.

MR. SKULE: -- industry to protect it, right. So I can't answer the civilian aspects of that. I mean, I think the DOD preventing a missile from landing inside the United States is probably the best defense rather than worrying about that. But, you know, post event there would be some of the things we've already discussed.

MR. GREENE: There are critical infrastructure cyber rules under NAERC, North American Energy Reliability Corporation, that a large portion of the grid has to conform with, not all of it. There are holes in the structure that Congress has tried to address it at various times. Some of us bear the scars from those failed attempts, but there is an effort, it's not perfect.

MR. HARRIS: To be clear, the United States Government does not regulate cyber security in the energy sector.

MR. GREENE: There's no easy yes or no. I have to rewind my brain six years to fully remember.

MR. HARRIS: Julia.

MS. IOFFE: Julia Ioffe from the Atlantic. After Vladimir Putin and President Trump met there was talk of, you know, having a joint cyber security force which was laughed down of course. But Russia has been advocating for some kind of formalization of the rules of the game here, kind of Geneva Conventions of the cyber space. How do you -- I mean you guys talked about how there are really no rules at this point. In the Cold War there were some rules, at least unspoken, unwritten ones. How do you feel about this suggestion that there should be a kind of Geneva Convention for the cyber universe? Thank you.

MR. HARRIS: Okay. Great question.

MR. SKULE: It is a great question. I think it's a great idea, I mean, where diplomatically we can resolve a conflict and set norms across the globe, I don't know how anybody could dispute that.

MR. GRIFFIN: You know, I think it's a -- I think you're right, but that's -- the challenge you've got is ensuring that the people that are involved care about the rule of law.

MR. SKULE: Right.

MR. GRIFFIN: And most of them, a lot of the bad actors don't care about rule of law. And, you know, the reality is at the end of the day if we have a policy like that, which I think is not a bad idea by any means, then it's got to be, you've got a place such as the Hague or someplace that you can bring people and try people and go through that process. But again, it's all associated with the rule of law.

MR. SKULE: And again, it would only cover nation state activity, it would not cover other bad things happening on the Internet.

MR. GRIFFIN: Exactly, exactly.

MR. GREENE: A benefit of norms is for, you're not going to deter the bad actors but for the good actors you have the lines, if a bad actor crosses, if you have the ability to rally the troops so to speak. The Xi-Obama agreement on economic espionage, lot of reporting that the activity dropped dramatically after that, but another

benefit of that was the public acknowledgement by two major nations that this type of economic espionage is not acceptable that is useful. Now, whether we're going to reach it -- so my answer to your question is we should absolute try, but I wouldn't go into it with feeling like we got to come out there with something because we may not get there, but the effort I think I agree, we got to at least try.

MR. WATTS: Can I add one thing?

MR. HARRIS: Yeah sure.

MR. WATTS: Anything that's bilateral in cyberspace is a waste of time in my opinion. So I'm all for setting up norms or whatever but cyberspace is a wide open space. And for us to go into that sort of exchange with one country, especially one that maybe doesn't abide by the rule of law, I mean Russia's primary technique for executing most these things in cyberspace is through proxies who wittingly or unwittingly do that. So they may be able to set the parameters by which they can enlist people of all shapes and sizes around the world to, you know, conduct these actions on their behalf. So I think it's got to be -- it's an international effort I think in cyber space, the -- you know, the two parties, I don't think it's going to work too well.

MR. HARRIS: Julia mentioned the proposed, well, I guess it was proposed, Russian-U.S. cyber cooperation agreement which got laughed down and the President kind of walked that back. Reuters reported a few hours ago quoting a Russian official that that idea at least from the Russian side is back on again. Maybe Clint can tell us but it sounds more like the Kremlin trolling the White House than anything --

MR. WATTS: Yeah, I mean that's super awesome, right? You just --

MR. HARRIS: So that's been thrown out there --

MR. WATTS: -- you just hacked the election and now you're getting a shared malware signature so that you know what worked whenever you send it over the fence? I mean, there is a little bit of goofiness with it. I am for some of these, you know, I've worked in the private sector

with cyber and I do see the value in a lot of the stuff. But you don't go to the guy that just punched in the nose and then tell him how to punch in the nose again. You know, I have a big problem with that. And I would like to see it done through NATO or the EU or through a series of partners.

MR. HARRIS: Over here, sir.

MR. SIMITIAN: Joe Simitian, Santa Clara County California. I want to go to Clint Watts and the rest of the panel on the notion of a nutrition label for fake news, and I understand why you've pushed government policing aside. But given the fact that we've got PolitiFact and FactCheck and 4 Pinocchios and folks didn't seem all that interested in what they had to say or what their evaluation of truthfulness was. Does that really hold any promise going forward of being a way folks can or will check out just what's real and what's not, you know, are we sort of in a post-truth era or --

MR. WATTS: No, I think it can be done. I think part of it is you need to build a widget that works on all web search engines or social media feeds. And all the social media companies have to come together on it, that's the toughest part. They would all benefit too by taking away the liability they have right now of being false-spreaders. So, you know, if you're Facebook, Twitter, any of these companies, you're now having to do thought police, if you can outsource that to independent agency and then give everyone the position to opt in or opt out, do you want this to show up on your search engine or your Facebook feed that tells you what the rating is of the outlet. A lot of people won't want to see or know, they would rather be blind to it. It's the same as eating the thousand calorie donut, you know, when you go in. Doesn't matter what you put on the label, they're going to eat it.

So there are people that will be the same way with information. But you are giving a mechanism, I think, that is outside government, it doesn't violate free speech, free press. It allows anybody to write what they want. And if people want to come to it, they can. I think the trouble with the fact checkers is you have to read an article or look at an e-mail and then go Google and search it. This would be something that you could essentially, you know, opt into and it would tell you in real time what

that rating is. And you can even go to the rating and see why the outlet is rated that way.

MR. GREENE: Rotten Tomatoes for articles.

MR. WATTS: Exactly. And you put a consumer portion in it too. You could even, you know, change the color of it, you put a number as truth versus fact and you put a color. And there is some great Columbia Journalism Review mapping that's going on that says, okay, this one is more right-leaning, this one is more left-leaning. That's fine; you could even rate it that way. Just let people know what they're getting because if I'm a fake news maker and you put that label out there it makes it really hard for me to gain audience interaction.

And I also think it puts a check on mainstream media. We hear a lot of complaints that -- about fake news. Well, start rating the big outlets. The outlets that do well in terms of fact versus fiction are going to get a higher rating, they're going to get more clicks. They may even get more subscribers. But it's a system. And that will be really hard to do unless all the social media companies agree to it. You know, you have to have some sort of collaborative relationship.

And I think they should want to do that because if I guessed right now using -- use of a lot of these social media platforms since the election is down because you can't trust the information on these platforms and the user experience sucks because of your friends and the arguing back and forth about fact and fiction and true and false and all these things. So I think it provides a tool that could benefit everybody.

MR. HARRIS: Well, to the panel, you've scared us but also give us a lot of solutions and things to be hopeful for, which is a great way to end it, so thank you all and thank you all.

(Applause)

* * * * *