THE ASPEN INSTITUTE

ASPEN IDEAS FESTIVAL 2016

THE POWER OF CONNECTIVITY
MANAGING RISK IN THE AGE OF CYBERTERRORISM

McNulty Room, Doerr-Hosier Center
Aspen Meadows Resort, 845 Meadows Road
Aspen, Colorado 81612

Thursday, June 30, 2016

LIST OF PARTICIPANTS

THAD ALLEN
Executive Vice President, Booz Allen Hamilton

TOM FANNING
Chairman/President/CEO, Southern Company

DAVID PETRAEUS
Retired General, U.S. Army
Chairman, KKR Global Institute
Senior Fellow, Harvard Kennedy School

ELIZABETH SHERWOOD-RANDALL
Deputy Secretary, U.S. Department of Energy

* * * * *

MANAGING RISK IN THE AGE OF CYBERTERRORISM

(10:20 a.m.)

MR. ALLEN: Good morning, and welcome to the Cyberterrorism panel this morning. We're delighted to be here. We've got an extraordinary panel. I think you're going to find them extremely interesting. Our goal is to make short introductions, start off with a couple of questions, and get some views on our panelists, but start to engage in a conversation and take this where you'd like to. You've got an extraordinary opportunity to deal with some folks that have dealt with the problems of cyber firsthand, and I request you all take ultimate advantage of that.

Let me start off by just a real quick comment. I had an opportunity earlier in the week to talk to Michael Daniel who's got the lead in the National Security Council for cybersecurity. Talking to a larger group he characterized the current cyber landscape as having four dimensions that we need to understand fully at all levels of organizational structure and in the public. The first one was the heterogeneity of information systems we have right now.

We know the world is globalized, but it's also globalized networkwise with ubiquity of information in the hands of everybody with mobility connected to the Internet. That includes the intersection of information technologies formally in backroom of enterprises and operational technology that runs our industrial control systems in manufacturing and large enterprises that rely on machinery. The second is there's no barrier to entry. If you buy an Apple computer and get an Internet address or you buy a cell phone, you can enter that world of work.

And it's very difficult to keep track of who's there, who they are, the norms are still evolving. And a lack of legal structure, as it is evolving as well, presents a challenge. Third, it's very low-risk for high reward for malicious actors out there. With very little

expense and very little risk they stand to achieve a great deal of return on malicious activity, and that's encouraging the field of potential adversaries to widen.

And finally, the real issue here is risk management. This is not an IT issue, this is not an issue for CISOs, this is not an issue for people that generally deal in IT. This goes clear to the highest levels of government, to boardrooms, and any enterprise that wants to secure what really is important, the crown jewels of data, and to keep their network safe.

So with that let me make a couple of introductions, and we'll get right to the business at hand here. To my immediate right, Dave Petraeus -- General Dave Petraeus -- you all know of his military background. But right now he's a partner at Kohlberg Kravis and Roberts where he's doing extensive work in private equity investing in technology. Next to him is Elizabeth Sherwood-Randall, the Deputy Secretary of Energy.

(Laughter)

MR. ALLEN: Oh, hi. Hey, Tom.

MR. FANNING: She's actually much better-looking than me. It's her.

MR. PETRAEUS: This is his avatar.

(Laughing)

MR. ALLEN: You know, Tom, you're absolutely right -- she is better-looking than you.

MR. FANNING: I know that, I know that.

MR. ALLEN: What I was about to say was Tom Fanning who is the CEO of Southern Company. In addition to education at Georgia Tech and the Darden School of Virginia, he is the chair of the Federal Reserve in

Atlanta. He's got great insights in electric-generating industry and links to cybersecurity.

And finally -- I had it written the other way on my sheet of paper here -- Elizabeth Sherwood-Randall who's the deputy secretary of Energy. She's got extensive prior background in Europe National Security Council countering weapons of mass destruction. As the assistant secretary of DOD she was responsible for Russia, Eurasia, and the Ukraine, and by the way, a Rhodes Scholar as well.

So thank you to our panel. Let me start off by asking you all to give your current characterization of the threat environment and some of the challenges we face. Dave?

MR. PETRAEUS: Well, this is clearly an area that represents one of the greatest threats to our country, and really any industrialized country around the world. We know, and it's publicly known, that foreign intelligence services, cyber criminals, and others have conducted cyber reconnaissance of the systems -- the industrial control systems that operate our electrical grid, water systems, and other critical infrastructure.

We know that these systems are often legacy systems as they say, i.e., they're old, they're not the most modern in the world. We know that many of them are local in nature; they're not all as big as the all of the above kind of company that Tom is privileged to lead. They don't have the -- again, the most up-to-date technology, nor can they attract the kind of Silicon Valley expertise that we'd really like to have focused on this, although this is increasingly an area on which they're focusing as well.

And then finally we know that the Internet of things, everything being more connected, which will include the industrial control systems which are old and outdated in many cases, that this will make even more vulnerable these very important systems so that there's a prospect that someone who has conducted the cyber reconnaissance,

who understands the network writ large could actually attack it, take it down, and keep it down for a period of time. And that is obviously the nature of the threat.

And my two colleagues on the panel and even again in the investment world, what so many are doing to try to deal with and to combat, and gradually I think actually making progress as there are breakthroughs in the technology, breakthroughs in the organizational architecture of government, in industry, and indeed, entrepreneurs like Tom -- leading organizations that are making rapid increases in these areas.

MR. ALLEN: Why don't we go to Liz? Liz, why don't you go?

MS. SHERWOOD-RANDALL: All right. First of all thanks to Aspen, Walter, and others who are friends in this group who I see in the audience who've done so much to make Aspen the vibrant, vital place it is for this kind of discourse. It's a delight to be here. It is true that we face a very dynamic threat environment. And in a world that has become increasingly interconnected, these capabilities are enablers for all of us and we value them. And at the same time they are new threat vectors.

And so what we are working to do is figure out how we can engineer in the solutions that will make our grid, upon which we all depend to power our nation, more resilient against both manmade threats and the effects of climate change and natural threats. So we see in government the opportunity to continue to build the strongest grid in the world and ensure that we can prevent and protect, and where necessary, mitigate and respond to attacks.

MR. FANNING: So I lead the Southern Company. I'm also chair of the -- what they call the Edison Electric Institute to be our industry organization. So that'll be our electricity. I have this role with the Feds, so I chair the Atlanta Fed. I'm also the vice chair of what they call the conference of chairs at the big Fed, at the

FOMC level and -- you know. So I have this kind of Fed finance thing.

And then I work in partnership with my good friend Liz Sherwood-Randall, deputy secretary of Energy, in leading something called the ESCC, the Electricity Sub-Sector Coordinating Council. Homeland Security has segmented American commerce into 16 pieces. One of those pieces is electricity. And what we do is work in partnership with our sponsoring cabinet level organization, Department of Energy, to assure that we provide the best prevention for and responses to cyber and physical terrorism.

And we've been exceedingly -- unfortunately -- exceedingly active here recently with Paris and with Brussels and with Orlando and a variety of other things. I think the one point I would want to get out to you right away is that there was no such thing as a silo in all these important activities. When you think about the federal government and all the three-letter agencies that we all know so well, we must harmonize our activities whether that is systems, whether that is technology access, or whether that is information-sharing regimes.

Likewise, private industry must develop an effective partnership with the federal government. Eighty-seven percent of the critical infrastructure in America is owned and operated by private industry like Southern Company, like the electric utility industry. We can't work in a silo. We must understand that we are inextricably intertwined with the other lifeline sectors. We generally call out five of them -- finance, telecom, transportation, water, and then of course electricity.

And then, let's not forget that for the federal efforts, the private industry efforts, we must integrate an effective partnership with state and local governments. In fact those are the folks with the boots on the ground that when the stuff hits the fan, they're going to help us put us back in the place we should be. One other point I would just mention, this is not a North American issue. For so

many years this nation has been blessed by oceans on both sides of our coasts and it has insulated us from a lot of bad stuff.

As was pointed out, there are no borders to cyberterrorism. And so now we must evaluate effective partnerships internationally. In fact, I'm going over to England here middle of July to work with the U.K., the EU, Israel, interestingly enough, and other representatives of the United States government to figure out ways to partner internationally on these important issues. Anyway, lot of stuff going on. It is a multi-variant threat environment. It is one of these issues where to be completely safe it is almost an aspiration. But we are skating to where the puck will be and we're working like crazy to make it happen.

MS. SHERWOOD-RANDALL: Thad, can I add to that? I think it's useful to describe the nature of the cooperation that we've built. Most people don't believe that government and industry can actually work effectively together. And one of the innovations of this administration has been to forge an extraordinary partnership between the Department of Energy and the electricity sector. And I want to describe four things we do together to make that tangible for you.

First of all, we share information and we share -- we're trying to share information at the speed of the Internet, not just the speed of human beings. And we're doing that in both an unclassified format, but now increasingly, in a classified format so that we can get out threat information quickly and get information from industry out again to other industries when threats are unfolding. Second, we are working to innovate together. We are looking at the vulnerabilities that we face and making significant investments in innovation on the grid.

And our electricity partners are working with the 17 national labs that DOE owns and operates to generate the kinds of solutions that we can push out quickly to address these cyber threats. So, for example, you're working with Berkeley National Lab on a way to detect spoofing so that

when there is a threat, somebody is also trying to spoof the information so we can get it out quickly enough to protect ourselves. You're -- we're working on an innovation to prevent that spoofing from deterring us from the threat.

And finally, most importantly right now we're exercising. And we are conducting a whole series of exercises involving federal, state, and local partners, industry and other stakeholders across the country to prepare for the worst eventualities because we want to be sure that we know how to respond if something happens before it happens so we can improve our performance.

MR. FANNING: And let me tell you something, for all the stuff you hear in this election season, isn't it wonderful? This is better than Netflix, isn't it? I mean for all the crazy stuff you hear and for all the hysteria out there around this issue, I want you to hear me clearly that we do have an effective partnership with government. It has been exceedingly constructive. On this ESCC that I lead there are something like 20 CEOs that are engaged very deeply on different issues. And we are making progress.

We don't talk about this all the time. The last thing you want to do to the bad guys is let them know everything you're doing to prepare for and respond to. But it is effective, it's working well, and we can go into more depth later.

MR. ALLEN: But there is a ton more that needs to be done.

MR. FANNING: Sure.

MS. SHERWOOD-RANDALL: Of course.

MR. PETRAEUS: There's not enough resources for it right now. This focus has been on the energy sector, understandably, given the panel. But as you mentioned, there's financial, water, transportation, and so on. Every one of these areas has something similar to that. And at

the end of the day, the Department of Homeland Security has such breadth that the secretary has to oversee that it is a -- it's going to be miraculous if they can pull all of this together and build the organizational architecture further so that then private industry and as well as government can all partner together.

And perhaps to address a question that some in the audience might be thinking because we have lots of titans of industry of the financial world and a variety of other walks of life -- and I often get the question -- so what should we do about this, what's the big idea here. And I think that the big idea is you have to pursue in all of the above or defense in depth strategy. You've got to have networks -- everything from network security all the way to endpoint security.

By the way, each of these is discrete even to identity security, to the psychological, the behavioral aspects of this. You've got to have -- I don't know if you have a dual-key system. But in the agency when we were going to -- you know, it's publicly known that the CIA contracted with Amazon Web Services for the Cloud. We couldn't build our own Cloud fast enough for all the big data that we were accumulating.

And so we went to Amazon Services, they provided it. We actually have a dual-key system now so that the network administrator who is arguably the single point of vulnerability if a foreign intelligence service can ever get that individual so that they -- there are limited authorizations even for them without others chiming in, and then all kinds of alerts and alarms and so forth so that a Snowden like event could not take place there.

And by the way, the NSA was painstakingly taking measures that would have prevented that and it just had not gotten to that particular location in Hawaii where he was located at the time that he was able to do what he did. But DHS has got to build this out at the end of the day. They're the governmental quarterback. They've got, again,

DOE, they have Treasury, they have others that are all leading their sub-elements --

MS. SHERWOOD-RANDALL: Sectors.

MR. PETRAEUS: -- sectors. But this is a gargantuan task and it has to come from the bottom up as well.

MS. SHERWOOD-RANDALL: One point on two-factor authentication -- we're beyond that now. We're at fourth factor --

MR. PETRAEUS: No, not two-factor, I'm talking two people.

MS. SHERWOOD-RANDALL: Right, we've got -- we -- have to -- we are increasingly looking at all the ways in which we can add layers to ensure that those who get access, especially to the control system, are trusted.

MR. PETRAEUS: We're talking dual key, not two -- not dual effect, not -- you know, you --

MR. FANNING: Okay. But here's the other thing. One of the great things that the digital economy has availed us of is this wonderful, almost kind of infinite flexibility in obtaining information, how we behave with each other, and how we communicate and everything else. The ideas of dual-factor authentication or four factor or -- those are "what's." One of the other things that we are challenged with in this new environment are the "how's," it's our behaviors.

We have to think differently about how we interact with each other and how we are able to access critical infrastructure in America. For example, you know, one of the biggest threats we have is insider threats. And so now we have now layers of behavioral analysis and requirements as to how you intervene with any digital technology in terms of your ability to compromise critical infrastructure for America.

It is -- listen, this is aspirational. We always must change. The threat always changes. We've always got to skate to where the puck will be. Are we safe today? Yeah, I think we're safe today. Are there threats that are always changing and always threatening us? Absolutely. Are the bad guys there? Absolutely. Whose cards would you rather have? The United States? The bad guys? I take the United States every day.

MR. PETRAEUS: One other -- just I guess that folks also ask, well, gee, I hope we're doing to them what we're -- what they're doing to us.

(Laughter)

MR. PETRAEUS: And without getting specific I can assure you that we've got the world-class folks that are doing whatever is necessary to ensure that if someone does something to us, that the return address would receive some loving attention as well.

(Laughter)

MR. PETRAEUS: In fact, one of the challenges of this area, though -- and I'll be interested in the other two panelists -- is that the theory in this has not been able to keep up with the advances. If you think back to the world of nuclear deterrents theory, I mean this developed over decades and it was quite straightforward. It was just the U.S. and the Soviet Union. Yes, some others got them, but it really was just all about one side deterring the other.

And you have the Wizards of Armageddon, as they were called, you know, developing these very complex theories and back and forth and so on. We just don't have that in this case. It is outstripping. Every time people think they have an answer to something, there is a new challenge, a new threat, a new situation. And most significant, I think, in terms of the threats is that some of the organizations actually don't have return addresses

that are meaningful. So there are literally transnational extremist organizations we have to deal with, cyber criminals, not just foreign intelligence from other governments.

MS. SHERWOOD-RANDALL: Tom and I think this is a huge opportunity for those of you in the private sector, especially. We need to invest in innovation because what we need for the next generation of infrastructure in this country is to engineer in the solutions. When we deploy new technology, we need to have -- anticipate it so that we're not playing catch-up, so the solutions aren't Band-Aids because really much of what we do right now is Band-Aids. It's not preventive, it's not durable, it's not resilient.

And when we look at the requirements, these are billions and billions of dollars of investment required in the innovation, from the development of the technology to the testing early. And we need patient private capital to support that early testing and then the deployment and wider deployment through industry principally. As you said, most of the infrastructure is in private hands. Government's never going to be able to do this alone. But that partnership is going to be absolutely critical because the capital will be necessary to the widespread deployment of the technologies.

MR. ALLEN: Well, as you can see, we have no shortage of expertise here on the panel. What I neglected to --

MR. PETRAEUS: Thanks for the great questions though, Thad.

MR. ALLEN: What I neglected to say at the start in my zeal to introduce the panel is I'm Admiral Thad Allen. I'm the executive vice president at Booz Allen Hamilton.

(Laughter)

MS. SHERWOOD-RANDALL: We all know you.

MR. ALLEN: We're a very proud underwriter of the events here at Aspen, always have been. Thank you very much.

What I'd like to do is maybe take this to the audience, see what's on your minds. I've got a bunch of questions I'd like to ask these folks, but I get to see them all the time. So if there's something you'd like to ask, please let us know. We have people with mics.

MS. SHERWOOD-RANDALL: Will you introduce yourselves too?

MR. ALLEN: Yeah, go ahead.

SPEAKER: (Off mic.)

MR. ALLEN: You've got a mic coming there -- thanks.

MS. SHERWOOD-RANDALL: Also tell us who you are.

MR. KLONOWSKI: My name is Mike Klonowski from Shelton, Connecticut. Sir, just war theory. Is there a point where a cyber attack warrants a physical response? Because the potential for destruction from a cyber attack that shuts down grids could kill just as many people as bombings or a conventional type attack.

MR. PETRAEUS: Well, as you know, first of all, that just war theory has the concepts of, you know, justification of action and proportionality as well. And to date, although there have been some very significant cyber events against financial institutions, against motion picture studios, against infrastructure, you know, the Little Dam that was hit in New York, I gather, was actually not the real target of the particular event.

Although there have been lots of these, there's not yet certainly been something that has risen to the

level that you would respond not in kind but rather with an actual kinetic activity. I, though, would certainly not rule out the possibility of a kinetic activity, and we know that again decision-makers certainly have that as among the options. But again, each time you do this you're crossing this threshold and you've got to consider, you know, then what and then what and where does it ultimately lead.

And if you come back to nuclear deterrence theory, of course the then what ultimately led to sort of oblivion for either or both sides, and that tempered the thinking upfront. The challenge here, though, is that these are not in all cases, as I said, "responsible" government organizations making decisions. In some cases these could be extremists who see the world very differently and would like to provoke something. So again, not something I'm sure that -- you know, you're at the Situation Room table now, not me -- that this is under consideration, but it is -- we've not yet gotten close to it.

MR. FANNING: We think about physical terrorism and cyberterrorism the same. We think about those thing as a joint effort by the bad guys. And let's think about the bad guys real quick. You got kind of goofballs, thugs, criminals, and then quickly we rise up into nation states and that's where you have the mutually assured destruction and the mutual threat and if you do this, I'll do that. I think the scarier ones are the guys that don't have anything to lose, and those are the terrorists.

And so we -- number one we think about those together. So when you think about all of the plans to prepare for and respond to, they involve thinking through a cyber threat and a physical threat. Second thing we do is GridEx III we just got through with. I think it was the largest tabletop exercise in United States government history. I think it had 20,000 people, took 2 days. It was an enormous effort.

MS. SHERWOOD-RANDALL: And it was for physical and cyber threats to the grid.

MR. FANNING: And we did four kind of big stages. And this fourth stage that we did was essentially existential threats -- threats combined physical and cyber that would impede our ability to govern.

MS. SHERWOOD-RANDALL: -- to function as a nation.

MR. FANNING: And so we went through all of that, okay? So please understand that we're taking all that into account.

MR. ALLEN: And I also know that the lessons learned out at GridEx III, which I was involved in as well, informed thinking of the National Security Council at deputies level exercises. So it's being heard.

MR. FANNING: And around the table the final exercise we had all the branches of the armed services. We had the three-letter agencies involved. We had all the major cabinet-level officers and that kind of thing. It was quite an effort, you should be very proud of that.

MR. PETRAEUS: One other consideration that certainly has always been in the background and actually on the table is that as one considers taking action, we should always remember that we are probably the most vulnerable of all societies because we are more connected than really any other large nation that is out there. And so when you open Pandora's box again, you've got to realize what that could ultimately lead to for us, not just for what we might be doing to some other folks.

MS. SHERWOOD-RANDALL: Interestingly, our partners -- as Tom and I were talking earlier this morning -- are working to ensure that they still have the capability to get off their use of these advance technologies, the analog systems. I mean one of the things we saw with the Ukraine cyber attack, which we evaluated afterward to learn lessons from it is that Ukraine was not as connected as we are. And they were able to restore

power more quickly because of that. So the ability to revert is important and industry sees that and is working to accommodate it.

MR. FANNING: And let me just tell you that here again to counter a lot of the hysteria you hear about, when you think about kind of the way we think about structuring as a response to a cyber threat, we have real-time systems. They would get attacked. We have backup systems that mimic everything we do that are completely insulated. Let's say both of those get taken out. We are developing a cool concept, it's in different places. It's in Southern called Spare Tire where we could roll in enough functionality for us to keep the lights on.

Maybe 70 percent of the functionality, but you would still have lights, okay? The fourth level is to run the system manually. Now, we ran the system manually before the digital economy came to fore. You should know in the United States Naval Academy they are now teaching midshipmen to use sextons that's if the GPS systems ever go out. That's an important backup. There is a whole backstop, I think, as to how we operate America without the digital economy that is a failsafe backdrop.

MR. ALLEN: As a proud craftsman in celestial navigation myself --

(Laughter)

MR. ALLEN: --due to my age, I appreciate the comment. We have another question in the back of the room here.

MR. FILIPPENKO: I'm Alexei Filippenko, astrophysicist at Berkeley. Another physical threat, of course, that can cause global damage is the Sun. That's a bad guy. And the coronal mass ejections can end up shorting out the power grid. And they short out the transformers, they fry them. And my understanding is there aren't a lot of transformers, extra ones sitting around because they're expensive.

Now, one way to, you know, mitigate this is to shut down the power grid, especially the long lines, the long power lines. But that doesn't mitigate the whole thing. It doesn't prevent the transformers from being shorted out. What you need are Faraday cages. Are those being built around the transformers? Because the U.S. without power for a year would be a global calamity, of course.

MR. ALLEN: Before our panelists reply, about 6 weeks ago I participated in the annual NOAA Space Weather Workshop out in Boulder, Colorado, where they have the Space Weather Prediction Center. We now have a national space weather strategy that has gotten the attention of the senior leaders in the government. And there's a movement to make that more of an enterprise approach to how we're doing it. And I'll pass it off to our panelists at that point.

MR. PETRAEUS: Let me just underscore the importance of the threat that you identified, because if you've been engaged in rebuilding a country's electrical grid as my colleagues and I were during the surge in Iraq or in Afghanistan, you do find out how few these transformers are, and in many cases how specific they are to specific systems. And the extremists learned how to take those out quite effectively with sniper rifles or other explosives. And then we had to delve over the time finding replacements for them.

Now, that's obviously a different part of the world than that in which Tom's operating. But just to, again, highlight that particular threat in much of the world that is out there but --

MR. FANNING: So we absolutely get this. And we've been working on this for some years as a program, mutual assistance in the United States electric utility industry called STEP -- Spare Transformer -- whatever that stands for. But what we have inventoried around the United States in critical areas are spares and plans to move the spares -- these things are extraordinarily hard to move

around -- to be able to accommodate those kinds of problems.

The other thing that has gotten a lot of play in the media that is again I would put in the category of hysteria was the notion that you could take out nine transformers in United States and take the nation's electricity networks dark -- that's garbage. You should know that the nation's electricity networks are operated in a dynamic manner. Southern uses an N minus two standard. And what that means is for any specific load area you would have to lose both a major generating facility and a major transmission corridor in order for there to be a problem.

And so what you do is you build your system so that there are multiple branches and any major load center that can either be accommodated with backup generation, different sources of generation, or different sources of transmission to move the juice from where it is to where it needs to be. There is a whole another level of spare inventories that go beyond the transformer level to other critical infrastructure. And the utility sector has decades-long practice of helping each other.

You should know that genetically these companies in America have a mission way beyond kind of keeping the lights on. We know that our success and failure really has a huge impact in how American commerce is run and how communities survive. And so when we think about responses to storms and Sandy, we sent something like -- I forget what the final number was, but say, 20,000 people. Southern had, I think, the leading number of people up to the northeast. So we have a mutual assistance program on the physical side as well as on the cyber side that we take very seriously.

MS. SHERWOOD-RANDALL: One final point on transformers. And we have recommended to Congress that there be a national transformer reserve that would be built because of what Dave said, that these are long, lead time items. Unfortunately, they're mostly manufactured overseas. It can take 18 months to 2 years to get one. And so that's something we need to fix, and it requires investment.

MR. ALLEN: And next question --

MR. PETRAEUS: And you learn in a combat zone --

MR. ALLEN: Oh, I'm sorry.

MR. PETRAEUS: -- how easy it is to take these out actually if you have skilled folks.

MR. ALLEN: Right here.

SPEAKER: (Off mic.)

MR. ALLEN: You got a mic coming by you, ma'am.

MS. ROSENAU: Okay. My name is Pamela Rosenau. And I'd like the panel to discuss what Mike Bloomberg said today in the *Wall Street Journal* about Apple and how Apple has not only not cooperated with the government, but has been a huge block in this whole encryption debacle. And I wonder whether we could take this -- I just wonder how many, you know, Silicon Valley companies are on your 20 CEO and government group and whether they should be forced to really work with the government from actually introducing the phones and the electronic types of gadgets so that they can be accessible by the government at the start.

MR. FANNING: So I'll take the first shot at that one since I'm private industry. I tend to be kind of a -- I hope -- I don't know if -- I am right-winger here. I think national interest supersedes commercial interest. And so therefore a business like ours, I assure, under my leadership Southern Company will commit whatever resources are necessary to cooperate in protecting the national interest. I'll stop. Okay.

MR. PETRAEUS: And let me pick it up from there. And interestingly, this is one where one of my predecessors in the CIA and also NSA, Mike Hayden and I come at this a little bit differently. And with respect in part, you are a national organization. You are not selling your products overseas. Apple is, as do virtually all of the IT empires that we have built in our country and that are such an

important part of the innovation economy and all the rest of that. I think that when you're addressing an issue what we're really talking about is the privacy of data versus the government's need to know to protect us, to safeguard us.

And I've always thought you ought to try to get the big ideas right, the concepts right on this kind of stuff. And in my view I strongly feel that the law enforcement elements and the intelligence community together ought to be able to crack any encryption in the world, very likely with help from industry in doing that. And that has generally been the case. It's not something we need to go out and pound our chest about. In fact the less we talk about it, frankly the better. And one of the challenges in this case is that this became so very public and it became an existential issue for both government and for industry, in this case, Apple.

This is a hill that both decided to die for, and that's probably not a constructive approach either. But so, along with the idea that we ought to be able to crack anything but not necessarily talk about it, I actually believe, as does Mike Hayden, that we should not be able to compel a commercial entity to provide a backdoor into a product they're making. Keep in mind that more -- much more of this is made overseas than at home.

So the -- all that would happen is that the bad guys will go buy it overseas, and Apple and Google and all the others, any of the other makers are going to be enormously disadvantaged. And this has a huge knock-on effect in our economy, where again these are such leading organizations. Beyond that let me just say that there was, when I was privileged to be in uniform, in final -- the four-star jobs in particular and then at the CIA, there was a wonderful partnership between government and the industry.

The Snowden revelations are what caused that to fray. The revelations of Snowden not only did enormous damages to sources and methods and led to terrorist leaders changing how they communicated, conducted their operations, and everything else, it also cost these IT firms tens of

billions of dollars. These are not trivial amounts. Google -- and it gave the excuse to foreign countries to balkanize the Internet which some of them wanted to do, which helps their industries keep data at home. In fact, we're in the business of getting a U.S.-EU partnership on data now that wouldn't have been necessary perhaps had it not been for these revelations.

That caused again the relationship that we used to have where we actually could go to any of the folks out in Silicon Valley and say, hey, can you give us a little assistance on this, and they did. But it was all done quietly. And I think so the solution to this is number one, we got to get back in the business of doing things quietly rather than staking out the top of the hill for each of them and then it becomes again a public issue that you're going to die for. There is a good commission that is ongoing that is trying to come to grips with this that is -- again, these are very, very tough, tough issues because of the loss on one hand versus the loss on the other.

And try to figure out how we can get a constructive dialogue going once again behind closed doors, which I think is actually beginning to happen. Again, I'm out in Silicon Valley and on Silicon Beach in L.A. and Silicon Alley in New York, actually in start-up nation Israel which we want to make scale-up nation -- all these different places. And that dialogue is beginning anew. And I think it is more constructive now. But it's particularly more constructive if you keep it out of the press and keep it quieter.

MR. FANNING: Well, that's absolutely true. I think the idea of having to provide a backdoor, though, is a red herring. That's really not the issue. Should companies, out of national interest, cooperate with the federal government in order to protect its citizens? That's the big idea. And the answer is yes. There is right ways to do that, and do it in a --

MR. PETRAEUS: Sure.

MR. FANNING: -- quiet way. We can do "and"

here, not "or." It's a false choice to say we got to do one or the other.

MS. SHERWOOD-RANDALL: And --

MR. PETRAEUS: But compelling is part of the desire by some folks right now, without question. I mean that's what some of the legislation proposes. So this is not a minor throwaway issue. There is legislation on the Hill right now that would compel industries to do what we just both agree is probably not the wisest of thing to do to help our IT industry.

MS. SHERWOOD-RANDALL: But what Dave -- what you are touching on which I think is important is that the private sector has a stake in cooperating with the government.

SPEAKER: Yeah.

MS. SHERWOOD-RANDALL: It's not just one way. It's not just government needs industry.

SPEAKER: Yeah.

MS. SHERWOOD-RANDALL: There is a lot that we have to do together. And if our telecommunications companies or our manufacturing companies are -- prove to have created new threats for the American people, our friends and allies around the world, that's a vulnerability for them. So they've got to --

MR. PETRAEUS: Yeah. But keep in mind --

MS. SHERWOOD-RANDALL: -- would collaborate with us --

MR. PETRAEUS: -- that at the IT summit that the President held in Silicon Valley, the executive chairman of Google did not attend, nor did I think the Apple. I mean so they -- my point was there has been --

MS. SHERWOOD-RANDALL: Though they all attended the cybersecurity summit hosted at Stanford.

MR. PETRAEUS: It's coming back together, and that's what needs to happen.

MR. FANNING: And there is a whole another effort going on. Homeland Security Advisory Council, which works kind of separately for Jeh Johnson and -- on that and there's other CEOs involved there. And what we're really focusing on are the big three -- that would be electricity, telecom, and finance. CEO participation working there -- and ma'am, just to be clear, the 20 CEOs I mentioned were all electricity CEOs. And they all have specific assignments, cross-sector support, R&D, extending the partner -- extending and deepening the partnership we have with the federal government.

MS. SHERWOOD-RANDALL: Supply chain work.

MR. FANNING: Supply chain.

MS. SHERWOOD-RANDALL: Lots of supply chain work. So that's an example of the kind of partnership that's essential.

SPEAKER: Yeah.

MS. SHERWOOD-RANDALL: Industry can't do that alone. We see --

SPEAKER: Yeah.

MS. SHERWOOD-RANDALL: -- more of the threat information.

SPEAKER: Uh-hmm.

SPEAKER: And this is --

MS. SHERWOOD-RANDALL: But these are --

SPEAKER: Yeah.

MS. SHERWOOD-RANDALL: -- investments being made that --

SPEAKER: Yeah.

MS. SHERWOOD-RANDALL: -- need to be based upon that current information.

MR. FANNING: And I may be sounding parochial here, but this is not the business of chief information security officers --

MS. SHERWOOD-RANDALL: No.

MR. FANNING: -- and chief information officers and --

MR. PETRAEUS: That's the CEO.

MR. FANNING: This is CEO stuff, this is boardroom stuff.

MR. ALLEN: Thanks. We have another question right here.

MR. POTTER: My name is Bob Potter. I come from Dallas, Texas. Not all targets are on the ground. There are targets in the air -- airplanes. What is the -- is any of your work addressing protection of airplanes? And it seems strange that whether it's Egyptian Air or Malaysian Air or it could be American Airlines next time -- these planes get into trouble and disappear. And we seem to know so little at the moment it happens. And it seems to me that with the GPS, with the communications those airplanes should be able to communicate to the government or to their airlines exactly where they are, exactly what's going on.

And we shouldn't have to be going to the bottom of the ocean to get a black box to know what happened. Are you included -- and also the airplane is clearly a weapon of the terrorists. 9/11 is of course the most dramatic example, but they could put a bomb in a commercial airplane and have it land in one of our airports and then blow up or blow up before it lands. Thank you.

MR. FANNING: Bob, good seeing you again. Hey,

I'll start up, but I'm going to turn this over to somebody who knows something else.

MS. SHERWOOD-RANDALL: It's -- we need additional --

MR. FANNING: A transportation guy.

MS. SHERWOOD-RANDALL: -- members of this panel.

MR. FANNING: But here's one of the challenges. So when I say the big three, right -- and so telecom. What is telecom? Is it a telephone? Is it a IT device? Is it -- what is transportation? Airlines, trucking, railroads, ship -- going vessels. They all have different characteristics, different threat environments, all sort of things. Trying to harmonize all of those activities is an enormous challenge.

And so what we're working on right now in the private sector is to prioritize kind of what are the most important things, and in my view, to protect against the biggest threats, and that is the existential threat -- the ability to laws --- to execute commerce or to govern our wonderful nation. I don't know -- anybody wants to tag --

MR. ALLEN: Let me take a stab at it too.

MR. PETRAEUS: Well, what you've laid out is again a requirement for defense in-depth. You look at the thousands of employees that could actually have access to something that goes on that plane or even to the catering system that ends up on a plane and you've got enormous challenges as we saw on the wake of the Egypt Air as they've done the forensics and the investigation there. And then you get to the issue that is somewhat perplexing that we can't have real time streaming of data from planes.

In some cases there are limits to the architecture of the satellites, to be sure, but not when you're over the Mediterranean. Why you have to dive down to get the data that couldn't be streamed is again something that airlines should have long taken on.

SPEAKER: (Off mic.)

MR. PETRAEUS: Yeah, I've --

MR. ALLEN: Yeah, I would only add --

SPEAKER: (Off mic.)

MR. PETRAEUS: For a price.

MR. ALLEN: Yeah. I would only add that this gets back to the public/private partnerships and --

SPEAKER: Yeah.

MR. ALLEN: -- discussions on how you solve complex problems. The last place you want to solve an Apple problem is in court.

SPEAKER: Yeah, yeah.

MR. ALLEN: Okay. The technology is there for continual contact with these planes. The original equipment manufacturers have a way to monitor the performance of their equipments that are on the plane. The question is what's the regulatory practice, what is required, what is the best practice by industry, and how do you manage risk of the platform that's flying out there. And I would suggest to you that conversation hasn't been as robust as it needs to be, given the incidents that have incurred because I don't think it's a technology problem.

SPEAKER: Yeah.

MR. ALLEN: Over here.

MR. CARMAN: So the --

MR. ALLEN: And you sir are?

MR. CARMAN: Oh, I'm Bob Carman (phonetic) from Boston. So we see that America has been safe for a long time, still is, except for cyber threats, cyber attacks, basically. And when we try to find an analogy Israel is a

good example -- they're being attacked all the time. And what they developed was a very robust deterrent system with regard to specific attacks that deters aggressors from wanting to do that a second time.

So my question is since physically I don't think America's going to be attacked -- let's hope so -- but the cyber attacks will continue, it's really a technology question -- my question -- which is what capabilities do we have or that you envision where these attacks are against private companies or they may be against the -- you know, the public grid or what have you where the response is response where that person's computer burns up. You know, it's a deterrent response to the immediate aggressor, which seems to have been very effective for countries that suffer these kinds of attacks. And we don't have that model, and is that the model?

MR. FANNING: Fire back capability is exclusively the purview --

MS. SHERWOOD-RANDALL: Yeah.

MR. FANNING: -- of the federal government. We --

MS. SHERWOOD-RANDALL: But that -- but as you said, the doctrine has not been evolved too. That extent, it's an ingenious idea.

MR. PETRAEUS: Well, without getting into any details other than what's in David Sanger's book or other columns and so forth -- I mean it's publicly known at least according to David Sanger that we certainly have some extraordinary cyber kinetic capabilities. According to him, allegedly these capabilities were used in partnership with Israeli and other countries' intelligent services and signals intelligence to put sticks in the spokes of the Iranian nuclear program, et cetera, et cetera, et cetera.

Now, without again confirming or denying all that I'm recounting that he says has been done, what I do want to come back to is the sense that this is an extraordinary Pandora's box. And when you head down this road, you

better have thought about the destination. And the destination could be a place in which we suffer much more than do those against whom we're using the extraordinary capabilities that we have. Rest assured that what we can do is really very, very considerable. There are legal mechanisms that underpin all of this. It's a very, very careful review processors, red teaming, there's everything else.

But again, when you head down that road you better have a sense of where it's going to take you and noting that we are more vulnerable than any other country in the world and have more at stake than any other country in the world. You've got to be careful about taking that next step. There's a lot of banks, by the way, that want to hack back.

SPEAKER: Oh, yeah.

MR. PETRAEUS: And again, there's a lot of CEOs that have come to me and said, why can't we do this, why can't we do that. And I would argue that there are good reasons why we can't do it, having thought through some of those when assessing the capabilities that we had and when they might be used.

MR. FANNING: Here's -- I'll give you another example that we're wrestling with right now. This is real grey area stuff. So let's say I put a digital umbrella over some of my critical infrastructure. And I can basically survey the whole landscape to look for threats. And let's just say a drone is starting to approach my critical infrastructure. The technology exists today to identify the drone, identify the payload and everything else.

Now, I can shoot a beam back at that drone, shoot it out of the sky, or I could shoot a cyber beam at it to turn it around and go back to sender or a whole sort of other things. But man, I have now impacted a whole set of other publics beyond my critical infrastructure. These are very tough issues.

MR. ALLEN: Question over here. We have time for

this one and one more -- just to give everybody a --

MS. PORGES: Hi. Shelly Porges from Washington, D.C., Entrepreneurs for Hillary. You know, we're talking about these cyber threats and of course they're very serious. But cyber threats also represent an opportunity for entrepreneurs and innovators. And I just came from the panel about the future of our economy. What do you see on the threshold now in terms of some of the biggest innovations? And is innovation nation here in the U.S.? What opportunities do we have to not -- (off mic) --

SPEAKER: Oh. We need to innovate around the microphone.

MS. SHERWOOD-RANDALL: This is an area in which, as I've noted, Shelly, partnership between government funding and universities and labs and the private sector is an opportunity for our country. We are putting a lot of money into innovation in cyber and innovation in other domains having to do with resilience of the grid. But this is a place -- for example, we're putting more than $200 million over the next 3 years into innovation that will be about partnership with the brains in our country, with the private sector to try to generate those solutions that can keep us ahead.

And that's something that we can't do alone as government, but also those outside of government can't do alone. And so we're trying to build that ecosystem in many of the great research universities partnered with our labs in the private sector around the country to make that a reality. It's also an area of huge opportunity for jobs. And we're seeing such growth in the energy economy broadly. This is a part of that energy economy and contributes to our energy security.

MR. FANNING: Let me give you a great example of that as terrific partnership with DOE and the labs. But -- so we have a system now. What we're looking for is every company that's signed up evaluates data coming across your servers. Imagine if anybody's ever been a trout fisherman, you know, you're standing on the bank or in the shallop on the river and you're casting out, but you're always looking

for little swirls -- that the water flowing through the river should represent all of the data flowing through the servers in the United States.

And you're always looking for little perturbations in the surface of the water where the fish may be. In fact our system evaluates right now all of the data coming across, and we're looking for those little -- what's going on here that causes us to raise a question and evaluate. And in real time basis now machine to machine, we get that back out to say, hey, we may have something going on here and we take steps.

The next level of innovation will be to connect those types of capabilities with essentially now a bathtub of data and connect now not only kind of what's going on in the energy space, but in all these other commercial sectors and all the other three-letter agencies. Really interesting stuff, and the government's doing a heck of a job here.

MR. PETRAEUS: And let me just put a capstone on that as someone who has now come to believe that among the highest callings in life is the private equity industry.

(Laughter)

MR. PETRAEUS: If you're a partner at KKR you'd feel the same way. No, the -- look, there are -- with all due respect to the $200 million that the government's putting into that one area, we're putting tens -- hundreds of billions into startups, scale-ups, growth in all the rest of this. And I think that is one of the areas that continues to be an extraordinary strength of our economy is that we have very, very agile capital markets and we have small and medium enterprises and startups that can build out the technology that the geniuses in places like Silicon Valley, Silicon Beach, and Silicon Alley develop.

And it's really quite a special attribute that has maintained our country's leadership and so many of the ongoing, really revolutions that are shaping this. It's not just the IT and the energy revolutions, it's life sciences, it's manufacturing. Every single sector is being

transformed. And in many cases the real engine behind that again is this capital with these entrepreneurs who are building up really great ideas.

MR. FANNING: Hey, and let me just add, though, when Liz talks about $200 million, please understand that's a contribution.

MS. SHERWOOD-RANDALL: Exactly.

MR. FANNING: We pick it up as --

MR. PETRAEUS: Yeah.

MS. SHERWOOD-RANDALL: Yeah.

MR. FANNING: -- as companies and it gets leveraged up many, many, many folds, so.

MS. SHERWOOD-RANDALL: I'd like to put in a plug for public service --

(Laughter)

MS. SHERWOOD-RANDALL: -- right -- since you've had a distinguished career in public service that has positioned you now to be in the private sector. For all those of you who care about these issues, we need great talent. We need people who care and who want to roll up their sleeves and work hard.

(Applause)

MS. SHERWOOD-RANDALL: Please join us. We can't solve these problems alone. And we face myriad challenges. You're listening to us discuss some. There's so many more. But to all those of you who are looking for some way to contribute, ask how you can serve.

MR. ALLEN: And we have time for one more question -- the gentleman in the red hat.

MR. BAKER: My name is Don Baker (phonetic) from Washington, D.C. We've spent a lot of time talking about

public/private partnership in the United States. We haven't heard much about partnerships between the United States and other countries and where it's working well and where there is really room for improvement.

MR. ALLEN: Liz, you want to take that?

MS. SHERWOOD-RANDALL: There is an enormous amount of work with other countries. Of course, we start with our close allies. And you've mentioned the work we do with Israel. There are many, many partnerships with countries in Europe and Asia to enhance cybersecurity capabilities. We work with partners around the world as well to help them identify threats and think through how they will meet them. You've done the rebuilding of grids.

You have many international partnerships with the private sector where you're working on this combination of efforts to make grids stronger in the face of new threats, but also stronger in the sense of using energy resources more efficiently and meeting our goals in the face of climate change. And so the international dimension of this is hugely important. If we had more time we could go around the world and talk about a number of these initiatives. But we certainly can't solve the world's energy problems alone, the climate problems that we face, the resilience issues without working in close partnership with other countries.

MR. PETRAEUS: You know, maybe a last word on that would be that even when there had been political challenges between countries, there had been maintained the extraordinary relationships between, if you will, the professional bureaucracies of those countries. The intelligence communities, the armed forces, the energy sectors, all of these different areas have tentacles and ties that are just really resilient, doesn't matter what's going on politically.

They're going to keep working together because they know the importance of it. And it really is sustaining a lot of the progress that's been made.

MR. FANNING: Well, I know I got to say this.

MR. ALLEN: Tom, you're going to have the last word here.

MR. FANNING: By definition, when you think about a financial system protecting itself or collaborating -- financial systems are by definition international in nature. There's almost no such thing as a domestic financial system especially from the Fed, right. So these things are happening. The -- we don't talk about them a lot.

SPEAKER: Yeah.

MR. FANNING: Sometimes you're better off working quietly to prepare, to respond to. Please understand that's happening. Don't believe in the hysteria -- important, tough issues. America is taking a leadership role here, and I'm very proud of the progress we're making.

MR. ALLEN: Let me thank the panel for their extraordinary insight and some tough questions out there.

(Applause)

MR. ALLEN: Thank you very much, folks.

* * * * *