Preparing for a Cyber-Enabled Economic Warfare Attack

A Conversation with Ted Craver, Steven Chabinsky, Scott DePasquale, and Suzanne Spaulding , moderated by Samantha Ravich

MAY: Political and military strength, while we haven't yet seen a wide spread rolling coordinated cyber-attacks, director of national intelligence Dan Coats testified just last week. That China and Russia, North Korea and Iran are advancing their cyber capabilities which are relatively low cost and growing in potency and severity. When a large scale attack occurs, the U.S. government and private industry will need to work together to allocate resources, mitigate the effect of the attack and share timely information. Help assess areas of divergency between what the government and private sector will require of each other and to help develop mechanisms and coordination now FDD and The Chertoff Group conducted a table top exercise, performance in your government officials and private sector leaders.

The findings of that exercise are what we are here to talk about today. Samantha Ravich CCTI chairman and visionary behind this exercise will moderate today's conversation with a few of the exercise participants. Samantha also serves as the vice chair of the President's intelligence advisory board and a member of the newly appointment cyber space and solarium commission. But first let me introduce David London of The Chertoff Group to set the stage. David was the lead designer and facilitator for the exercise and services of the senior director at The Chertoff Group working with some of the world's largest companies, managed cyber risk, build effective security programs. Previously David designed high profile cyber exercise and war games or government information sites.

By ways of housekeeping, I should note that today's event will be, is being live streamed, I hope and I encourage you guys here and online as well to join in on today's conversation, particular on Twitter that's @FDD, I'd also ask that you silence your cell phones. With that, David, thank you, over to you.

LONDON: Thank you.

Thanks to FDD and to Cliff for the introduction. At The Chertoff Group, we view cyber enabled economic warfare largely from the perspective of American companies, who we work with on the front lines who are looking to separate the noise and the nuisance from the vest that could down lifeline services across America. The services that Americans rely on, on a daily basis. CEEW and our exercise puts that dynamic on steroids. Sophisticated actors exploiting systemic vulnerabilities to cause debilitating consequences. And as Cliff indicated, government and industry coordination mechanisms do exist, but it was far from clear, from the exercise whether they are agile enough to respond to CEEW conditions. Especially when time is of the essence.

This is an essential truth that was a key driver for the October event and is why we enlisted some of the most engaged and thoughtful minds for our exercise and for our panel discussion to grapple with these issues. Last week the Wall Street Journal published a piece by Andy Kessler entitled *Strike Back Against Every Cyber Attack*. Provocative for sure. But it does capture the sentiment of many American companies and people who feel powerless and outmatched as America's most critical infrastructure and our own identities are targeted and exploited. And while Cliff indicated full blown CEEW cyber enabled economic warfare has not transpired in the U.S. yet. The steady drum beat of nation state attacks that we read about in the news, that we seek to defend ourselves against on a daily basis, remind us that this risk is persistent and it's pervasive and it's highly disruptive to our way of life.

General Michael Hayden who's a Chertoff principal and who was a key contributor to the exercise in October, crystallized a consensus view that came out of the session in October. That view is that there is a need to review and reshape the division of labor between the U.S. government and the private sector in addressing CEEW events and conditions because the current status, the current status quo has been out voted, both by our adversaries and by the ambiguous technology that we interface with every day. At The Chertoff Group we work with clients to build resilient enterprises and effective security programs and we believe that resilience is a key pillar for countering CEEW conditions.

Cyber resilience is often defined by the ability to anticipate, withstand, recover from cyber-attacks and then evolve from them as our adversaries evolve. And we believe these principles are, interesting organizing principle both for broader CEEW issues and also for some of the insight that came out of our session in October. Anticipate can we look around corners and we maintain informed preparedness. Now this is a joint proposition of course between government and the private sector in order to coordinate response and also to enrich threat intelligence. Mechanisms like the Cyber Security Information Sharing Act is a great start, it's in place and it is working to reduce legal impediments but other barriers still remain. Can organizations maintain the essential functions in the face of adverse conditions? In other words can an enterprise bend without breaking?

It starts with a unified understanding of critical or as financial service's sector calls, must run functions and the commitment to protecting those first. But it's also about coordinated efforts to maintain public confidence while sever conditions and life line sectors are threatened. Particularly in this fractious political climate. Recover, can we restore quickly? Understanding the interdependencies, not only the critical functions within sectors but the interdependencies across them are key to prioritizing CEEW related recovery efforts. And we must also evaluate the adequacy's of existing government functions and authorities to address the unique cyber conditions that we may face.

And finally evolve, are we learning? Are we adapting? Adversary tactics and objectives of course as we all know in this room are not static and so our ability to counter CEEW conditions is going to be contingent on our capacity to evolve as well. And events like this, building coordinated muscle memory between private sector and government and other advanced planning activities, we believe to be essential. The most important finding that Cliff touched on earlier, emerging from the event is that unless the government and the private sector begin making and developing CEEW specific procedures, we will be caught flat footed in the face of cyber enabled economic warfare. On behalf of The Chertoff Group I'd like to thank our counter parts at FDD and I'll turn it over to Samantha and our panel to unpack our insights from that exercise. Thank you.

RAVICH: That's great. Thank you, thank you David. Thanks for The Chertoff Group. You know as David and Cliff mentioned and our reports on the table on the side, can be explained further for cyber enabled economic warfare is the use of cyber means by an adversary to undermine key components of our economy in order to weaken us strategically. Alright so it really puts the private sector on the front lines of this battle space in a way that perhaps we, the U.S. government and the private sector themselves haven't really thought through. Thought through the roles, responsibilities, expectations in the event of such a catastrophic type of attack. And that's really why we convened the exercise in the first place.

To kind of level set what each side thinks responsibilities, roles are of the other and also then to come out of that, how do we prioritize what type of planning activities need to be taken? And that's what we'll be talking about with this very astute panel. We really gathered some of the leading lights in the private sector and in the government to attend in October and we are really fortunate to have four of them here today. So starting from the far right on the table, Steve Chabinsky is the former deputy assistant director of the FBI cyber division and served as the FBI's top cyber lawyer; Ted Craver is the retired chairman, president and CEO of Edison International and he now serves on the board of Wells Fargo and Duke Energy; Suzanne Spaulding served as under secretary for national protection and program director at the department of Homeland security and she's now a senior advisor at CSIS; and Scott DePasquale is the president of the financial systemic analysis and resilience center which coordinates activities to mitigate systemic risk to the U.S. financial system from cyber security threats.

So I'm going to start off with Suzanne and you know Suzanne at the table top exercise you saw the scenario which and large scale rolling cyber-attacks across our economy, across different sectors. So assuming that the U.S. government designated it as a significant cyber event incident, who at the White House would be brought around the table, you know who's in charge in the U.S. government and how would the private sector get their voices heard in such an event?

SPAULDING: So the way in which the government responds is laid out in presidential policy director 41 and which captured what was an ongoing practice. So you have both a cyber-response group which is really looking at policy and strategy and that's going to be the players that you would expect. So you'd have folks from DOD, both the officer of the Secretary of Defense but also, almost always somebody from the joint chief of staff. You're going to have the intelligence committee there, probably ODNI and almost certainly someone from NSA. You're going to have DOJ there and almost certainly somebody from the FBI as well. You're going to have DHS at the table, State Department, Treasury, almost always is going to be there and there's SSA's, so the sector specific agencies.

So DOE if we're talking about impact on the electric grid, communications is almost always implemented, DHS is the SSA for coms and for ten of the different 16 sectors but there are agencies out there for the others. So that's really the primary group that you would have coming around the table and then the context that was playing out very quickly in the scenario were you've got also geo-political tensions and a potential effort to mobilize the military federate, you're going to have those meetings at very senior levels and it's going to be indistinguishable from an NSC or a deputy's committee meeting, I think initially on those issues.

At the same time though, you've got, so that's policy and strategy. At the same time you're standing up a unified cyber coordination group, the UCCG. And that is to focus really on the operational pieces. Who can bring what to the table? And how are we going to coordinate our operational activities? So again all the same players but much more operationally focused, so DHS for example at that would be represented primarily, probably by the NCCIC. Our national cybersecurity and communications integration center. So it would be more of an operational focus and that is where explicitly there is a provision for the private sector to be at the table.

Which is vitally important. Not only because it is the private sector that is likely the victims here, the targets of this cyber-attack but also because they are going to have the tools and resources for responding to that in conjunction with the government. That is going to, a lot of it's going to fall on them. They're also there, I mean at the CRG, DHS and the sector specific agencies center enrollment are going to be turned to, by policy makers to say, what is the impact here? What do we know? What's our situation awareness? And what can we anticipate? NCHS has stood, I stood up a cyber and infrastructure assessment group, it's now the national risk management center that works with the private sector to look at these inter dependencies cascading consequences, what should we expect? What is the – not just the consequence today but what's going to be the consequence in the next few hours, days and months?

And that's what the policy makers would look to. At the coordination group it is who has what levers to bring to bear to mitigate those consequences? Alright and so that's, again a huge part of the resilience, and it's not just going to be your IT folks. And so very quickly Ted can talk about this, when we did these big grid X exercises for the electricity sector, the CEO's are very quickly talking about where can we get, can we get this much copper wire? How are we, you know, how are we going to get things back up and running? In a degraded fashion? So those are the – and then of course we are going to be getting that situational awareness by being in direct contact with our private sector folks. Some of them sit on the NCCIC floor, on our operations floor at DHS, we have seats for the financial services ISAC, for the electricity ISAC, for the multi-state ISAC so that we're getting on the ground, what's happening all across the country? A number of private sector folks as well as the inner agency that are going to be right there on the ops floor, getting what we're getting at the same time we're getting and providing that same real time information.

And then we get folks on our phone, Caitlin Durkovich, their group was able to get sectors and the cross sector groups on the phone within a very short period of time, you know, sometimes less than an hour. To get folks on the phone to say what do you need? What's happening?

RAVICH: That's great. Thank you. Ted, you may, you've been a major figure in the electric power industry for many, many years and you know, sitting as you do in the private sector and at the scenarios there were other members of the private sector. Some you know, not as perhaps well versed in the language and speak of Washington with all of the letters and the acronyms. But you know when you think about this, first from the electric utility standpoint, what mechanisms exist, you know in and amongst yourselves and then as you saw in the scenario, other sectors that rely on electricity, up and down the pipeline. What comes to mind in terms of what concerns you? What keeps you awake? Or you know where you think we're in pretty good stead.

CRAVER: Yeah so particularly with the electric grid, maybe self-serving or self-importance but we tend to think everything relies on electricity which is actually in our current society pretty accurate. Can't move water without electricity, most of the transportation networks don't work without electricity, so on and so forth. So a lot of time and attention has been spent on how do you protect the grid as much as possible. And in fact, enterprise systems, so whether it's accounting systems or people related systems, those things are important and well protected but they're kind of secondary to the operating system that manages the grid.

And indeed it's largely isolated from the enterprise systems that use the companies. So heavy focus on that part. I will say that one challenge is that the electric system is not made up of, you know four or five big companies and maybe a few smaller ones, it's made up of over three thousand companies. Some of those are state owned, some of those are county or municipality owned, some of those are what we call co-ops about 45, 46 of those are owned by what we call investor owned utilities, which Edison was one is another. And about 70, 75 percent of the assets and the customers are within that investor owned group.

So one of the challenges is how do you manage a grid that has over three thousand people, three thousand entities rather that have a connection into it? And that have a part in managing that? Starting in around 2012, late 2011, 2012, a huge effort was put in place to try to bring all of those CEO's from the investor owned utilities plus the municipal and co-ops together with government, DOE and DHS as examples, is very much involved in the effort to really start that coordination process, so that we could get good information sharing between the government and these three thousand plus entities and we could coordinate resources and be able to share resources across all of those pieces that touch the grid.

I think another strength actually is that the grid is this large multi path network and it has a lot of built in and engineered resiliency and the fact that there are so many islands that are interconnected probably creates a strength if in fact a serious attack was mounted on the electric system. We can talk more about that maybe a little later but I think that's actually a strength, although it can be a challenge just trying to coordinate all of the pieces. And there's a culture within the industry of mutual assistance, we've had for decades mutual assistance programs really for addressing natural disasters, so hurricanes, earthquakes, wild fires and so on. And this is where all the utilities across the country and actually in Canada and little bit in Mexico as well, will jump in and help a utility or group of utilities recover.

But one of the natural disasters that occurred during the time that Suzanne and I were working on this was Hurricane Sandy and we had, in fact Edison trucks and people were airlifted from California into the Northeast to deal with Hurricane Sandy. So obviously a cyber-attack is a different animal than a natural disaster but the focus is the still the same. That's trying to keep the grid up and running, trying to isolate the problems, trying to speed recovery as much as possible. And I think one of the greatest strengths is the industry is very used to working with each other in these mutual assistance acts to quickly restore.

Where we're spending more and more time now is on the cross sector piece which Suzanne just mentioned and there are really five sectors that are most involved in this. Communications, finance, water, natural gas, transportation. So all of those pieces are inter-related and trying to ensure that we have that same type of mutual assistance and working together to try to manage the issues and really restore the grid but also restore the other inter connections that make it all work. So I would say kind of in sum on that, I think there's a good culture and a good background for working to protect and maintain and restore in severe outages, but it is a complicated group of industries and companies that have to work together and work with government in order to share resources and share information to be able to really keep the systems, the life line systems safe.

RAVICH: You know, that's a great point, and I think we saw during the table talk that you know different sectors who have different experiences working with the government, different expertise, longevity working with the government had different expectations, what the government could provide to them as well as what would be expected from an, and there was a kind of a robust discussion in this particular point on the need for attribution. If this, if a type of attack occurred would the government, how would the government go about making attribution? The importance of attribution to the United States government as they proceeded along in the wake of a large scale, malicious attack and what the private sector kind of thought about that.

And there was different, a bit of a robust discussion amongst the private sector participants about the value of attribution to their own mitigation efforts and you know Scott, talk a little bit about, you know that in terms of the financial sector, does value attribution, they understand it and why they understand the importance of it and how defenses can actually be strengthened by anticipating the attackers playbook and perhaps how other sectors – it would be good for them to understand this as well.

DEPASQUALE: Yeah, I mean, I think it depends what seat you're sitting in and at what moment in time, right? If you expect the US government to suppress activity that's persistent in your use of DDoS attacks of Ababil back in 2012 and in 2013. If you expect the government to do something about it, the government is going to need to refine its understanding of attribution, it's going to need to understand the impact the atmosphere is having a key piece of critical infrastructure. And so the question is what might the private sector have in its possession because they operate that critical infrastructure, they have the most robust and highest fidelity information about what's happening on that front line.

What kind of partner can we be to the government to allow them to make a better decision around that threshold of impacts so they can take an action? So if the answer as you expect to play some roles, a partner with the government in that, that attribution is pretty important. If you’re on the frontline of defending the network, which you hear about at that moment in time is, what is the malicious activity look like? How do I find it in my system? Who in this sector can help me understand the quickest way to eradicate that because it's likely happening across dozens if not hundreds of other entities, right? So the information sharing community becomes the important first line for that. As a network defender you want to know binary's and hash values, and you want to know what to look for.

You don't need to know at that moment whether that's Iran or North Korea, you need to know how do I get it out of my system and clean it and produce business as usual for my stakeholders? So it really, it's not a one size fits all shoe. It depends what seat you're sitting in.

If you want to go look at the long pole in the tent and get ahead of these things, I think it's really important to understand, what geo-political actions, whether it's a breakdown of GAC, OPA, or what the environment is that's creating, the type of attacks or at least the type of reconnaissance that might impact you in a couple of weeks. So from a strategic standpoint, if you're a pretty strong case to be made that you're going to partner with government, going to have to be able to contribute to that out. I mean, particularly if you want to government to take an action on the other side of and event or during the event.

RAVICH: Yeah, Steve, certainly even as the US government has gotten better at attribution, there's still some information that is critical for attribution that resides with the private sector. There was actually a very good conversation as well about what the private sector, what kind of data can the private sector to the US government?

Some misunderstandings as well. It seems that the legal and reputational concerns, breaking those down into two kinds of baskets, so let's start with the legal side and in terms of liability protection to the companies, but then also how do we – Maybe the harder question is how do we deal with the reputational concerns that companies would have providing such data during times of crisis to them?

CHABINSKY: That's a lot to unpack. I'll try my best. First, let's start with the attribution of why we're even having conversations. What does the government need? Why is information sharing even a thing? I'm not the strongest advocate of talking about information sharing as though it is the end goal, right? There should be some strategy that if it requires information, that's great, let's figure out how to share it, but there's a lot that can be done without anyone passing any information to anyone because there's a lot out there.

I do agree, turning off with that proposition that if you don't know who the actor is, a couple of things, you don't know if they're coming back after you get them out of your system. Is this a opportunistic attack or is it a targeted attack? Of course if we're going to have any deterrent value, it's important to know who's doing it. So where is the information for attribution so you can make these decisions? By and large, it's internationally acquired because hackers don't just start where their boxes and then go straight to the victim, and so it's going to be routed through a lot of places and that creates an enormous ecosystem of tracing back where activities come. So you have an infrastructure that's being used by attackers, that's one thing.

Then you have the methodology itself, which tends to be in a couple of locations, one on the actor's side, but then on the victim side, seeing what the malware is, what commands are being entered on that?

When you pull all that together that you have this environment that's architecture where people are using their purchasing domains, they're using email addresses to do so, they're setting up servers, they're breaking into servers, they're extending their reach from there. They're doing the same thing to possibly a thousand victims at once from one central location. Then at the end point, right, you're seeing the same types of malware.

What's interesting when you put all that together, a lot of folks think that attribution is, well this malware was used by this country, and therefore we see that malware. You can't say that that's that country, anyone could use it. That's true of course, anyone, but when you pull together all of the areas that we're talking about, right, when you pull the string on this totality where you get to say, "Well, this is interesting. The architecture that's being used, the IP address, the domain a year ago it was being used to target this events of this one country and now it's aligned against companies that actually have the exact technology the country is looking to acquire and next week is having a summit on that."

You start saying to yourself, "Okay, you've got a motive. You've got not just the tools that are being used but the exact architecture. What are the odds that some other party could actually acquire all of that and then use the exact same trade craft to do it?"

Not only that, but to actually have the motive to do it? I mean, tell me what the community thinks this way, right? You have this red team analysis where you're saying, "Okay, could it be somebody else?" We have all the reasons why we think it's this country, let's come up with some alternative competing hypothesis of someone else that it could be and that's how you start gaining this high level of competence about who's doing it. Then you try to take your action. So the first question is, what are those information pieces that are needed and who has them that information be shared?

What's been remarkable, at least in my career, I've been doing this since 1998 on the cybersecurity side, is how often companies say that there are impediments on the legal side to sharing information when none actually exists. It's really a nice way of saying to the government, "We don't really have any motive to share. We don't want to share if it's either going to be a cost against business or it's going to be somewhat difficult for us to get the approvals." So what we're going to say is, "We would love to share, but we can't and it's your fault because the laws don't permit it."

The way we know this to be true is every time some – I guess there are two reasons. Every time there has been some discussion about, well, what are the laws FOIA, antitrust, liability, civil liability, someone will sue us.

What ended up happening is the government met private sector and said, "Okay, we're going to give you a letter, we're going to give you a law. We're going to say this isn't an issue." Then the next point will come up. Well what about this? There got to be the meeting, the letter of the law, and most recently in 2015, the Cyber Security Information Sharing Act of 2015 now three years old, which basically said, "You'll still retain your attorney client privilege. No one can sue you if you're just handing over threat information. It's not an antitrust violation. FOIA doesn't apply to the state. The regulators can't use it to regulate against you." The list went on and on and guess how much more sharing we got? So it's a canard, right? That there are these legal impediments, but you asked another important question about, well, what about reputational risk?

I think that there are a couple of things of what is the motive to share, right? One of the motives to share is what's the point of it, right? Why does anyone need this information? Does the private sector needed it to have a better defense, does the government need it to help the private sector or to take actions against you? That case really still very seldom gets made upfront. Meaning we're got a couple of gaps and those gaps would make a difference to our strategy and that is seldom articulated and so the rationale for why it's needed has to really be the beginning point.

The other issue is now it's gotten to the point where a lot of companies make it a marketing right decision, that they're about privacy, right? That there may be attention with sharing data with us between private sector companies or with the government versus this public statement of saying to the private sector, "We won't share any of your data."

I think that it's a bit simplistic because the data that would need to be shared isn't about the customer, but it could indicate information that is acquired, right? That the private sector companies have. It could indicate access capabilities that the private sector may have, that even though in that instance the information that is being shared as clearly for cyber security, national security purpose, it implies something greater that the company doesn't want to be part of. Whether it's working with another nation or just showing what the capabilities are.

I think that when we were talking about, well, what's the strategy, what's the rationale? Why you need it? If that could be more aligned with what is actually being shared and how is it protective of civil liberties and human rights? That we can make a lot of progress here, but it's not legal issues that are the challenge.

RAVICH: We'll kind of circle back as he was saying was absolutely took up a good chunk of what we're talking about at that table talk, what was the private sector already understood? What was the canard as Steve was saying? This sense of, you know, US government don't just say you need everything. Tell us specifically what it is and will be used for. So in some ways the prioritization of the ask.

The other piece of the importance of the prioritization of resources, it goes to stockpile of parts of the most vulnerable and important critical pieces of our supply chain. So Ted, I want to ask you about this question on supply chain and how it figures into cyber risks? To talk a little bit about what you were thinking as we were going into this table talk of about do we need to start prioritizing resources differently in the event so that we're prepared and can have the resilience and can constitute if need be, if there were a catastrophic cyber enabled economic warfare attack?

CRAVER: This is a really complex area and a lot of dimensions to it. I'd say probably the starting point is on the supply chain, I think we tend to think of it as mostly a potential vulnerability. We have most of the utilities, so I'll focus primarily on those industrial utilities that manage about 70% of the assets.

They don't make or build a lot of things directly with their own boys, they use a lot contractors to do this, so the supply chain, both on product and service is quite expensive. A lot of those companies are significantly less sophisticated in terms of cyber issues, in particular, so a lot of effort over the last four or five years has been on how through your contracts can you get in a sense audit rights? The ability to come into these firms and get a better sense for what level of protections they have on software and particularly where they're connecting into parts of your system, so that's one element of the supply chain.

The other part always major parts, spare parts and so on, that I think is actually in pretty good shape. That's again been something that the industry has been doing for decades around responding to grid outages and natural disasters. Just put a little point on it, one of the most important pieces of the grid are called AA Transformers and these things weigh tons, they are huge. In fact, in order to move one transformer often will require four or five days to get it a small business. So getting those transformers and strategic locations in the grid and lining up the transportation that's going to be required, they have these things called, Toppers which have anywhere between 15 and 20 axles just to be able to carry these things, it takes up a whole road in order to move it.

So things of this nature have been focused on for many, many years and I think generally speaking, we're pretty good shape on having strategic spares and strategic locations around the grid.

The final part comes back to that cross sector party. We rely on natural gas in order to get generators up and running. We rely on the communications network to get the system going. When you have to get a grid back up and running, you don't just go over and flick the switch, you have to go through a whole complicated black start process. Then you have to be able to synchronize all of these grid assets, it's a phase angle and all of this stuff that engineers talk about. Being to get the grid back up and running a multi-day process if it is a significant outage. Being able to ensure that you have people really trained on how to do the black start process, folks just going through the simulators, but really understand how that piece works is, again, something that I think the industry is continuing to focus on.

RAVICH: Yeah. Suzanne, we had talked about how the electricity industry is probably leading the way on as, as Ted was talking about stockpiling of certainly a critical spare parts, but when you look at kind of the broader risk assessment, risk management of the economy as a whole, what are your thoughts on where we can really kind of push ahead?

SPAULDING: Yeah. Well it's really interesting. I mean Ted is absolutely right that the electricity sector, like the financial services sector, a few others, spent a lot of time at the CEO level and I met three or four times a year with 30 or 40 CEOs of the Electricity Subsector Coordinating Council. Really focused, like a laser beam, really on resilience really at the CEO level, what they really focused on is how do we keep providing a good or service that we provide to the public? How do we keep that going? Just terrific, there was some great progress made, but it is also, there was also a recognition that some of these things that they rely upon, for example, for natural disasters, like these mutual assistance arrangements may or may not work in the context of a cyber-incident that is cascading across the country.

So in the case of something as huge as Superstorm Sandy that was up and down the entire East Coast, it was the East Coast and it came through and it was gone. So you could air lift things from California. You could bring stuff in from Ohio, etc., to surge resources because they weren't going to get hit next. The challenge, listen I remember these conversations in the context of a bio terrorism and bio warfare, an emerging outbreak of emerging disease, even natural outbreaks. This notion of sharing pharmaceuticals and what have you from one state to another, if you don't know how it's going to spread and whether you're going to be next, you're going to be reluctant to airlift your supplies and there is a recognition of this. So sort of how do you adjust them, your normal plants for a cyber-incident?

In addition to understanding that one of the most important assets that you're going to want to share and surge is the cyber workforce. Transformers have traditionally been that long pole in the tent. But in this time, in this instance, it might be where do we find some more folks who can actually get into the IT network and figure out what's going on and helping us bring it back up?

Then one of the other interesting things that came up in terms of interdependencies you might not think about. As Ted said, you can think about all of the industries that rely on and all of the things in our lives that rely on electricity. All of the things that rely on communications, etc.

What was it immediately obvious for example, was that if the electricity is out for an extended period of time and the electricity companies are trying to, whether it's put out copper wire or move big transformers or wherever they might be trying to do, that requires money. They're not collecting revenue from customers who are not getting electricity and so that interdependency on the financial services sector to finance the work that needs to be done, and we are not where we should be, where we will need to be in that understanding, all of those interdependencies.

It's why exercises are so important. It's why cross sector exercises are so important to really begin to understand those cascading consequences so that we can plan today, how are we going to do that? What are the contractual relationships that you are going to need to have in place? When we did the Section Nine Catastrophic Consequences List that the President asked us to do under Executive Order 13636.

Look at all of the entities where a successful cyber-attack, could have been expected to have catastrophic consequences. Almost all of those were catastrophic economic consequences and the focus then needs to be not just about, okay, how do we prevent this from happening? But how do we mitigate the economic consequences so that if an adversary, because using the threat of economic warfare to freeze us in place, to deter us from doing something in our national interest, we are not so brittle and susceptible to that kind of extortion?

RAVICH: Yeah, before I put up the questions from the audience, I want to put one more thing out there for Scott and Steve to comment on. Suzanne, you know, by saying adversary, right? So this is not a natural disaster that we're talking about. This was an adversarial attack. Again, with the private sector at the cross hairs of this, whether it's the banks or large international companies, they're very involved in the international economy. They have clients, they have board members, they have C-Suites that are involved in either they're not Americans to begin with or they are very involved in international commerce. Just some thoughts on how do we begin into open the aperture to think through this very tricky aspect of what happens in the event of a cyber-enabled economic attack, not a natural disaster in that respect?

DEPASQUALE: We sort of break the world into two parts, right? What happens as you approach or you're at boom and to the right of boom from the recovery and how do we stop the pain perspective? Then left of boom, how do we maneuver better long before it, so we avoid it, right?

On the right of boom scenario, I think what we found out is soon as you were moving PII from the equation and you're talking about TTPs in specific observations about how the network was compromised, what the tools were, were they observed in other places, Why shouldn't we have seen that happening? I actually don't think there's a lot of sensitivities for the financial institutions to be able to share that with our government partners.

I think the gift to get a relationship with FSR, was built around this idea that, hey, we will educate our government partners in particularly in the defense community and cyber command about how our critical must run functions operate. What's the interconnectivity between the business processes, the market functions, the specific technologies that support them? The return on investment is if we have a bad day and we're under attack, that you have a contingency plan and you've done some homework based on various thresholds of impact that you thought through how you're going to react to this and what you need from the private sector to enable you to suppress that activity before that bad day happens. So we formed a lot of our projects around doing that.

Now what you learn really quickly when you start working with your government partners in that space is that if you get out of that the defense, world we get into the intelligence community more on the Title 50 side, the more we work together and unify our understanding of the threat with the government, the better. The more we look at strategic warning meaning that, you know, hey, if there's tools development being deployed in the Ukraine and we see outcomes, the intelligence community might not understand that those tools can be used to hit at the heart of something. To Suzanne's point that is a critical must running system that may not be obvious to our partners in the intelligence community. So I think, far left of boom we need to be working on educating folks about what the impact could be, so we deal with it and maneuver before we have to go deal with cyber command to suppress it, right?

We kind of start to separate those. Let's have the contingency plan, let's work through that with the defense community, let's keep PII out of it. It makes it less difficult to deal with. But let's keep pressure on the intelligence piece of that to get further and further left of boom so that hopefully over time the intelligence community can harmonize this collection practices consistent with what really matters for the financial sector or the power sector.

The last thing I'll say is what we learned is you don't actually start this whole thing on the threat side of the equation. You start this by looking at your building and saying, "Before we figure out, you know, how to forecast hurricanes better, how can we make sure that building withstands a Category Five hurricane?" What you find out is, if you focus, and what we did at

FSARC as a sector, what are those 14 things? What are the top three ones? How do we make those withstand more? You have to basically deconstruct the building and rebuild it. That's where you really learn the things, the intelligence and defense community can then mobilize to be more effective in their response to it.

It really is back to the business processes and to Ted's point understanding your system better. I think the sectors have some work to do to make sure they, among themselves, work on the interconnectivity because I think we have to bring that back to the government and then suggest way for our government partners to deal with it.

CHABINSKY: Two brief points here to your question. One is the geopolitical implications of cyber enabled economic warfare where countries might be able to retreat to their geographic boundaries but most companies cannot retreat to a particular country's geographic boundaries.

As a result of the fact that even large American headquarter companies have equities throughout the world and the architecture and infrastructure and where data is stored in cloud environments. They cannot retreat in the same way that a government, consider it government versus government, that's not how the private sector views it.

The second point is you talked about the private sector being on the front lines. I think if I were to say the largest problem with all of cybersecurity is that we recognize that the private sector is on the front lines, but we have not empowered in any way, shape, or form economically the private sector to do what needs to be done with the government to resolve this at a higher level so that it's not getting to all these people.

Every person, every business should not be on the front lines of a national security problem. It's crazy. We have allowed that to occur instead of figuring out what is the higher level through an internet ecosystem where the government and the health communications services, the internet providers, the domain services.

How could they all work together so that this threat doesn't reach every end user? We've instead said that we need more workforce, crazy response to a problem. It's like having an arsonist in the neighborhood saying we don't need to get the arsonist, let's get more firefighters. Or looking at another analogy if you look at what happened in Flint, Michigan where you have water that is not potable. No one can drink it. Is the response let's have every business and home have a filtration system and the capability to use it? Of course not. You go to the reservoir on the pipe level. You don't make everybody responsible for it.

We are approaching this problem backwards and as long as we approach it backwards, we leave too many people in order to resolve it instead of making sure that we're doing it efficiently and that we're paying those who need to be on the front lines of cybersecurity to have that national security approach and to pay them for being on those front lines.

RAVICH: That's absolutely fantastic. Let's open it up to discussion. Please use the mic. Introduce yourself.

WEBER: Hi, Rick Weber, *Inside Cybersecurity*. So the report does a very good job of describing what's a stake and the recommendations, 20+ recommendations, sweeping recommendations. Redefining government's relationship with the private sector. How does this get implemented? Is this something that congress has to do? What are the next steps?

RAVICH: Susanne I'm going to turn to you since you were on this when you were in government pushing things ahead.

SPAULDING: Well, it helps me to get back to your original question which I never really answered, who's in charge? All right? Because normally these kinds of recommendations, if they're really taken seriously by administration would be handed to your cybersecurity coordinator or perhaps your assistant to the President for homeland security because they would be working on a daily basis will all of the players on the government side, who would also then be working with the private sector folks on this on a daily basis. They would pull together a task force and they would look at which of these do we want to accept and how would we implement them.

So it makes it all the more unfortunate that today that would really have to fall to Bolton. Who would also have to be effectively chairing the cyber response group and the unified cyber coordinating group in the event of an incident. So I think it's another – Effective implementation of these recommendations will be hampered as so much of our cyber coordination –

RAVICH: Are new laws needed? Do you think we have the laws that are needed? Does it point to congress that we actually need to be able to do the prioritization of what we had talked about? Or does that exist and now we've just got to get to it?

SPAULDING: I don't think we need new laws to do the prioritization. As Steve said, a lot of this, the prioritization is going to depend on your ability to analyze particularly consequences. Then as we've talked about these interdependencies cascading consequences, that's going to be the key input into how you prioritize your activities, and the nation risk management center that's been set up at DHS is set up to do exactly that. They are moving from an asset based focus and prioritization. After 9/11 we had this list of assets and buildings and structures across the country that – and prioritize those in terms of which are most important.

We've moved to a recognition that it's really function. Where are the key functions? Where are these key nodes that are at a higher level where if we focused our efforts on building resilience and risk management there we could stop a lot of the harm? Making that happen does not require a new law. It does require making the business case. It requires making sure that all the folks that come to the table understand why they should come to the table, what they get back.

RAVICH: I think both Scott and Steve want to just –

DEPASQUALE: I'll make a minor comment. I agree in the foundational work that the NRMC done, the nation risk management center, it's created a coordination capability for this work that didn't exist across the government. The one thing I think that we struggle with as a sector is that it is when you're working with the defense and intelligence community which we do through DHS now that there's a mechanism to do that. I think there's a conflation of what is legally acceptable and then what has been adopted as policy among the executive branch agencies. Our hope is that through NRMC now and through DHS's new cease program where you've got it consolidated cyber agency that we can get the intelligence and defense community with the sector specific agencies working more side by side with the sector in a way where maybe the intelligence and defense community wasn't comfortable doing before.

DEPASQUALE: I think we've actually had some successes in doing that. I haven't perceived, I think we've been at the front line on this effort, we haven't perceived a legal constraint to doing that. But you've got to have a whole lot of executive policy discussions about who's doing what. That takes up a lot of sector bandwidth. I'm not sure we've got it perfectly right yet, but we're –

RAVICH: Did you want to include some –

CHABINSKY: Well, I think we've had a market failure so I agree with Scott that we don't have any legal impact setback before. But if I can think of a law that's needed, it was interesting to me to find that when we wanted to bring telephone service and broadband service into rural America there was an economic purpose for that, we created a Connect America fund to fund that. I didn't realize, we don't have a Protect America fund so we keep rolling things out without any idea for security. How are you going to fund at the higher level this new strategy where the fewer corporations can do for the greater good more?

So make a Protect America fund, take 10% of the military's budget for all I care, and have requests for proposals of what would it take, for example, to get rid of all botnets in three years. These are the command and control platforms that grant somewhere is being used that all the economic espionage campaigns are being used from. Eliminate them in three years at the higher level so no one has to deal with them. It's an economic issue.

NELSON: I am Bill Nelson, CEO of Global Resilience Federation, formally FS-ISAC. I took part in that exercise, it was fantastic. What I noticed though that week, two days after that exercise which was targeting a nation state attack against transportation, energy sector, and the financial services sector. Two days later we saw an attack against Poland. We'd just signed a deal with United Kingdom to buy natural gas then attack your transportation and their energy sector. Do we have a playbook to defend ourselves? Because this stuff's happening all the time. We saw it in financial service sector 2012 and '13. See it with other countries, South Korea, Saudi Arabia. I mean, are we ready? Do we have a playbook, cross sector playbook, private sector, public sector playbook in response to something like that?

CRAVER: I'll take just a piece of it. I think probably in the last year and a half, two years, there's been more effort on exactly those cross sector dependencies. We have had, as you were explaining, some exercises that I think start to identify where the gaps are and where the weaknesses are. I guess I'm a big believer that you need a few core pieces in place, but trying to get too specific with playbooks for this or that or some other thing you're never going to really guess the attacks or the circumstances.

We haven't talked about it here, we did a lot in the table talk exercise a few months ago, I'm actually pretty confident in the informal network that exists. I saw this in the electric sector, you get below the CEOs and so on and as you get to the engineers in the field and you get to the folks that are in the cyber command centers they're quite free about sharing information. They band together quickly, pick up the phone, "Hey what are you seeing? This is what I'm seeing. How's this going to work?" So I think it's some combination of having this top down piece, but I wouldn't want us to forget the importance of that informal network. A lot of that is getting people together through these exercises. They've established those relationships they bring a lot of those relationships from things that they did before. I think that's actually one of the restraints that we really get hit with a serious cyber-attack, I think that informal network is probably going to do more of the work then a lot of fancy top down efforts.

SPAULDING: So I would just add that the relationships are really important. And saying, and this is one of the reasons that the private sector is going out on its own and trying to create some cross sector organizations and relationships. So when my friend, Tom Banning CEO of Southern Company a company we worked with 10, 9, so many others over the years, working very hard on a tri-sector group to bring in electricity to start with. Electricity, finance, and communications. They feel like the government's come along but the private sector recognizes that these relationships at the CEO level will be important.

RAVICH: Before we go to the next question, I just want to use my moderator privilege to say we didn't, at this table talk, we did not forget that third after that is out there which is the citizen. There was a robust, again, discussion on do we have, if not the playbook, but who is in charge of telling the citizen if the banking system is under stress during a time of cyber economic warfare or electricity outages or shelves in stores are starting to go bare. That was a key component to that discussion as well.

LYNGASS: Hi, Sean Lyngaas with *Cyber Scoop*. I wanted to ask about potential blow back of US government going on the offensive. Imagine that topic came up during the round table with government officials and industry executives at the table. What was the specific concerns that were raised with the private sector side and how did the government folks try to, reassure is not the right word but, bring their perspective into – How did those diversion views get consolidated during the exercise?

RAVICH: If you want to-

CHABINSKY: What's interesting about the question is I think there was more of a sense of the Government is not going to step in and have affirmative actions that will make the pain stop for private sectors in the reverse. Really, I think, during this table talk exercise at least, that tended to be the focus and the private sector expect that the Government will be able to help in any number of ways. When you say offensive, we consider the full range of diplomatic information on military economic, law enforcement, this whole Dino league, elements of national power that the country can bring to bear on any situation. Or is the private sector on its own? That tended to be the stress factor as was already mentioned with the DDoS attacks in financial services center. That was, I think, a big lesson learned.

Where does an event continue with at least a pure inch of the private sector that the government is not stepping in to assert its strength against potentially another nation state? When is the point where the country is going to come in at the national level, at the government level, and say we are going to use your information to have that type of reaction? There's little precedent I think right now for considering your question other than the fact that I went to national strategy, just say that an attack against our public or the government that depending on what the effects are it could be treated as a military incident. But we've shown a lot of capability at the Government level of these economic sanctions, law enforcement sanctions to go against other nations.

SPAULDING:To Shawn's point, I mean I think there was, my recollection was that there was a recognition that depending on what offensive actions the Government might decide to take that it was important to have representative at the table when those decisions are being made. Private sector perspective that understood they could bear the brunt of any retaliation. So even the attacks on the banks in 2012 and 2013, the DDoS attack, were in theory a retaliation for the role they played in implementing sanctions against Iran. So again, I think we certainly, when I was at DHS, we were very mindful that as we came to the table in those discussions part of what we were there to do was to try to bring that private sector perspective into that conversation and not to freeze action, but to understand that private sector might bear the brunt of the retaliation and how do we mitigate that?

RAVICH: That was the foundational question concept at the start of our project on cyber enabled economic warfare that threw pressure on the private sector, cyber means in this case, that it could change the direction at the national level for national strategy because the pain that the private sector and citizens were bearing at some point they say just make it stop. What would that lead to in terms of our national strategy?

A few more questions.

MARKS: Hey, Jim Marks from the Washington Post. Steve, when you said earlier that say co nard that legal liability's an issue for the industry. So, how the heck do we get them to actually do it if they haven't yet? Then Susanne, obviously you worked on this and I'm sure have some thoughts on that.

CHABINSKY: So one thing I think Ted pointed out is in areas where it really matters, and when there are active investigations or active incidents that there's a lot more sharing going on for people to see. And that's without all of these protections, right? Meaning that those weren't required, they were assurances that were given through legislation, but then even prior to legislation that information would've been able to be freely shared. I think that it gets back to what we said earlier, that if there's an actual need and there's an actual gap and getting that information is going to make a difference, that there is a lot of sharing going on.

MARKS: Thank you.

CRAVER: I perceived there to be a little bit of difference with the electric sector than perhaps some of the others. The electric sector is uniquely domestic it's not owned by foreign companies. Those companies, at least the investor owned utilities, very few of those holding companies own utilities in other countries. It's really, for all intents and purposes, it is a domestic industry. So the pressures of, well do we really want to share this information or are we worried about how our foreign owners or board members or whatever may feel? I think that's largely absent. It does not exist in the legislative. It may sound a little overly patriotic but my opinion, if we had an issue that attack in a significant way attacked the electric sector it would be all hands on deck, it would all be about how do we work with the government?

Frankly, it would probably be a fair amount of settlement of the like some shooting back because it's too hard to defend this entirely on our own. I think that sector would be very much lashed around trying to get the electric system restored as quickly as possible with very little other consideration.

CHABINSKY: It would be fair to note there as well there a couple sectors that are highly recognized including energy and financial that they have to share certain information.

SPAULDING: So I think the issue is at all – Long before the intense focus cyber going back to the physical days of responding to storms, etc., terrorist incidents for example, what we have always known is in the event of an incident that's not where your information sharing problems are going to be most intense. Because almost always people rally around, everybody's focused on trying to solve this urgent problem. Intelligence community and law enforcement are much more likely to be willing to share information with victims and potential victims, folks who have information that they think could help are much more likely to come forward with that information. Really the challenge is on the day to day, always, and cyber is no different.

Because it's harder to make that business case as Steve represented. Yet, it is that day to day activity that pinging those millions of attacks all across the country on critical infrastructure, that data that can be so incredibly valuable. I think increasingly the private sector gets it. We've done a pretty good job of convincing people that if you share data you're going to be better off. So now they're sharing with ISACs, they're sharing within their own private sector organizations, not necessarily with the government. At DHS, the system that we constructed, basically sort of says that's okay. If you're more comfortable sharing with each other and not directly with the government you do that. Those ISACs are nodes in this automated information sharing and they will still get the information and they can send information that's been anonymized. It doesn't all have to be a hub and spoke going right to the government.

RAVICH: Very quickly, very quickly.

PELSON: Sure. Jon Pelson from Spotlight Software. In the weeks after 9/11 all the talk was that the next major attack would be cyber. Here we are, why have we gone almost two decades now without a massive attack in the US?

SPAULDING: I mean I would defer to some of my private sector, we've had some pretty significant attacks.

CRAVER: If you're one that's been attacked it's pretty ugly.

RAVICH: You're talking hundreds of millions of dollars for specific companies after not touch alone.

CRAVER: Pharmaceuticals, some of those have been hit where they have lost production capability. There's been some pretty serious events. In any event I think you always have to be – What is that potential and let's make sure we're really as well protected and it's well organized as we can be.

CHABINSKY: I would just say that the attribution has gotten better. Most major states have a better deterrence factor against the United States. Up until recently private sector economic hacks have wanted the systems to remain up and we have now started seeing more of the hackers for profit using destructive attacks. I think that has shown a rise. Then we've seen incidents where destructive attacks have spread but not intentionally that could be nation state sponsored. Both of that would be my response to you.

SPAULDING: I think really having a significant impact on operational, and sustained impact on operational activity through an attack on industrial control systems is harder than people think. It's just getting into the industrial control network is not enough to have a sustained and significant physical impact.

RAVICH: I think our time is up. But first of all, I want to really, I want to thank the panel so much for participating in October and for today. So thank you, thank you. On your way out, please take the publications and the one from this table talk it does have a list of recommendations. So now we have to put our shoulder to the grindstone and actually think through how to operationalize this thing. So thank you again.

SPAULDING: Samantha's going to make it happen.

RAVICH: There you go.