THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2016

THE VIEW FROM THE WEST WING

Aspen Meadows Campus
Greenwald Pavilion
Aspen, Colorado

Saturday, July 30, 2016

LIST OF PARTICIPANTS

CLARK ERVIN
Executive Director, Homeland Security Program
The Aspen Institute

WALTER ISAACSON
President and CEO
The Aspen Institute

LISA MONACO
Assistant to the President for Homeland Security and Counterterrorism

* * * * *

THE VIEW FROM THE WEST WING

(2:15 p.m.)

MR. ERVIN: All right everyone. We will get started, if you could make your way to your seats, please. Well, as I think you all know by now, I am Clark Ervin, the Executive Director of the Homeland Security Program here at the Aspen Institute and the organizer of the Aspen Security Forum. I want to thank all of you for being with us for these past three days.

Every year, it seems as if world events conspire to underscore just how important the Aspen Security Forum is. And I want you all, please, to join me in thanking our sponsors and thanking our speakers and moderators for three absolutely riveting days of conversation.

(Applause)

MR. ERVIN: It's very appropriate that our final conversation is moderated by our President and CEO, Walter Isaacson. So Walter, take it away.

MR. ISAACSON: Thank you very much.

(Applause)

MR. ISAACSON: And it's not only a great honor to have Lisa Monaco here, but it's a great personal pleasure. Most of the people I've met working in government, great servants, really diligent, but nobody is like Lisa who combines being both nice, level-headed, smart but also very diligent, so diligent that I said, "What did you do today?" She said, "I spent three hours on a secure conference call," so while the rest of us were hiking, so.

MS. MONACO: It's okay.

(Laughter)

MR. ISAACSON: So thank you and welcome.

MS. MONACO: Thanks very much. It's great to be here. It's a credit to you and to Clark and to the whole team for putting on yet another great event. It's also a rare privilege for me to get outside of what is commonly referred to my cave or bunker in the White House which has no windows, let alone a beautiful tent. So it's great to be here. Thank you.

MR. ISAACSON: It's great. If we could start with Syria, we've heard today --

(Laughter)

MR. ISAACSON: -- or the threat of bears, we could do that. But we've heard at this conference that we really are making headway against ISIL in Syria. Do you worry about a resurgence of Al-Qaeda if that happens?

MS. MONACO: I do. I do, and I should say, you know, we've talked rightly a lot about the threat from ISIL and I am sure we'll get into more of that here and the hybrid threat that it presents. But I think any discussion of the terrorism threat that we face today has got to also underscore the threat, the continued threat we face from Al-Qaeda. Now John Brennan talked about this yesterday that Al-Qaeda core while greatly decimated, Al-Qaeda remains a lethal organization with its affiliates like AQAP and others.

But what I think we really need to underscore is the fact that Al-Nusra, which is in fact Al-Qaeda in Syria, is a threat to us. It has established a growing safe haven in Syria and they have taken advantage of the chaos in Syria. People will remember that in 2014, when we began our military operations in Syria and Iraq, we did so against ISIL. But we also simultaneously undertook actions and strikes against a group of Al-Qaeda veterans who had moved quite deliberately from the Afghanistan-Pakistan region to Syria for the expressed purpose of taking advantage of that ungoverned space.

MR. ISAACSON: How closely are they aligned or they're competitors, ISIL and Al-Qaeda, in Syria?

MS. MONACO: So they're competitors at this stage. And you got into this a little bit with Dina did with John yesterday. And I think we have to constantly be watching that relationship, but we should not be take our -- we should not take our eye off the ball and let any success against ISIL, which we are having substantial success and we've got momentum against ISIL in both Iraq and Syria. But we should not, and we should be very careful that that success does not also create a vacuum for Al-Qaeda in Syria.

MR. ISAACSON: How are the threats between -- from ISIL versus Al-Nusra, how are they different?

MS. MONACO: So I think -- and this has been also been talked about to some degree, but I think it's important to remember ISIL presents what I call a hybrid threat. It is at once a terrorist group most -- most assuredly, engaging in directed and complex attacks like we saw in Brussels and Paris and other places. It is an insurgent army undertaking military tactics and operations and taking swaths of territory, although less now than before, but it is also a social phenomenon. And it's this last piece that I think is -- makes it a distinguishing -- is the distinguishing factor in the threat that it poses. Its ability to utilize the online space and frankly to digitize the threat that we face is -- makes me believe that we have -- we have now confronted and are in a new phase of the threat that we face. We're in a moment that's different from one that I've seen.

Now ISIL at once is trying to do directed attacks and complex attacks as we've seen, but they're also extolling their followers and their adherence to undertake attacks wherever they are, and to do so without needing to travel, to train, to become vetted or undergo any type of discipline, but rather to undertake terrorist attacks wherever they are using the tools of our everyday life. We saw Mohammad Adnani extol followers to undertake attacks where they are, to use a gun if they have a gun, to use a knife if they have a knife, to use a truck if they have a truck.

MR. ISAACSON: Which is what they did in Nice.

MS. MONACO: Exactly.

MR. ISAACSON: So we then have to fight them in a different way, meaning a bigger threat from ISIL comes from the homegrown self-radicalized at times terrorists who may be like the guy in Orlando, just totally confused about many things, but then decides to say, "I was an adherent and I'm doing this for ISIL." Does that mean that we have to have closer relationships with our domestic Muslim communities? And if so, I think General Clapper said earlier at this conference, that it's very dangerous, the rhetoric that you hear in many places about demonizing Muslims.

MS. MONACO: Look, I think we have to have greater relationships and greater connectivity with the Muslim-American community, with communities of all stripes around the country because the distinction, I think, in the moment we are in now is that we are confronting this threat, as you've noted, that is more diffuse, it's more unpredictable and it is, I think, maybe less sophisticated attacks that occur, but they are certainly deadly and they bespeak a level of unease for people that I think is quite reasonable. So I think what we're doing and what we have to continue to do is constantly recalibrate the tools that we are using.

So, for instance, after 9/11 we set up, I think, across the last administration and this one, an architecture that was focused on building up our intelligence capabilities, breaking down barriers, breaking down walls between law enforcement and the intelligence community, taking what we call on all-tools approach to disrupt threats, whether it's military intelligence, law enforcement, diplomacy. And that architecture has been created and has been, I would argue, quite effective at discerning, detecting, disrupting complex attacks that are based on a networked structure, that are based on a hierarchical model such as the one that Al-Qaeda and core has employed.

But the threat we're facing now is both -- assuredly that and so we have to continue to use those

tools and continue to foster the partnerships we have with our international partners between law enforcement, intelligence agencies. But the Orlando example or the individual who is self-radicalized online, our net is not designed and is, frankly, not capable of detecting that. How do you detect when something goes wrong in somebody's mind and something resonates within them to commit a violent act? That means we're going to have to rely a great deal more on our communities, on giving them the tools to intervene, to identify and work with individuals who are on a path to radicalization.

It means we're going to have to work in greater numbers and with greater urgency with the private sector, with those who have developed the platforms that are frankly being misused to peddle this venom and really brutal messaging from ISIL. I think we've got a lot of those tools that we're developing. I think we're going to have to continue to recalibrate and because some tools that we used for the post 9/11 era aren't always going to be applicable for the threats we are facing going forward.

MR. ISAACSON: Well, let's drill down on the two things you said, work more closely with the Muslim community, work more closely with the private sector tech community. Starting with the Muslim community, how harmful is it really when people are demonizing the Muslim community?

MS. MONACO: So look, I think now this -- this debate about what do you call radical Islam, et cetera, violent extremism, this has taken on a political resonance and has gotten into the -- a very heated political debate, and I'm not going to get into that. From a purely counterterrorism professional perspective, the enemies we are fighting, the groups like ISIL and Al-Qaeda that are trying to recruit, radicalize and mobilize individuals to violence are doing so on a message that we, the American people, the United States, are at war with Islam, that we are trying to promote a clash with civilization. So why would we do anything to further that?

Now, there is no denying that a tremendous amount of violence from these groups, all of the violence

from these groups, has been undertaken and perpetrated based on a perversion of Islam, there's no denying that. But we need to focus on the goal, which is why are and how do we stop radical jihadists or violent extremists of all stripes from trying to kill us.

MR. ISAACSON: But Secretary Jeh Johnson, Homeland Security Secretary, sort of your counterpart since you're the President's Chief Advisor on Homeland Security, says he's actually now been going into Muslim communities and finding it harder. And the first things I say to him is, "Why is everybody in America demonizing?"

MS. MONACO: Yeah, it's -- that it does not help our ability to reach out to maintain relationships with the Muslim community. I hear a lot, I sit down with representatives from across the diaspora, from across the civil society, and what I hear is a concern not only about rhetoric and labels, but about a sense that the U.S. government should not securitize the relationship with the Muslim community, which makes complete sense.

MR. ISAACSON: Explain what you mean by securitize.

MS. MONACO: So that all interactions between the Muslim community and the government should not be done through the law enforcement lens, which of course is right. We've got to broaden that and our strategy for countering violent extremism recognizes that, right? So this is a strategy that is based on enabling communities from the ground up, whether you're teachers, whether you're medical professionals, whether you're community organizers, whether you're state and local government, or whether you're local law enforcement, to be able to come together and build your own recipes, your own strategies for whatever is going to work in your community for helping individuals, usually young, lost and troubled souls, from not becoming, frankly, soulless killers.

MR. ISAACSON: We should give credit because the George W. Bush administration started that process.

MS. MONACO: Absolutely. Absolutely.

MR. ISAACSON: Now you talked about the tech community. As the President's Chief Homeland Security Advisor, you helped lead a delegation not too long ago out to Silicon Valley, I'll call it, although you were all around California, I think. If you had to just request right now and say, "Here is three things the tech community could best do for us," what would they be?

MS. MONACO: So, some of it is already being done, which is broadening the conversation beyond the encryption conversation, which I think is a very important one for all the reasons that John Brennan talked about yesterday. But we have the best innovative minds in this country, I'm clearly biased, but not to say there isn't great entrepreneurs and -- and inventors and engineers elsewhere in the world, but I think we've got the best innovative minds in the United States. And they have built the platforms that have become the tool of choice for terrorists to both peddle their propaganda, but also to use for operations.

So it starts in the open lane, it starts on Twitter, it starts in the open source community, but then goes to the darker side of the web. What we need to do is enlist the private sector's help in having those tools that they invented not to be used for this purpose. I firmly believe that the innovators in this country don't want their -- they're patriots, they don't want their platforms used for this purpose.

And how do we help them enforce their own terms of service? Every tech platform I've ever talked to has got their own terms of service about what's permissible on their platform, but they -- what they have said is they want information to be a two-way street, what are we seeing from government -- from the government perspective about how terrorists are using their platforms that might help them enforce their own terms of service. So that's one thing.

The second thing is they are sitting on a lot of knowhow in terms of marketing and branding and getting messages out that frankly the USG is not particularly

expert in. You know, anything that has a U.S. government stamp on it that is trying to counter ISIL's message, I would submit, is probably not going to be the most resonant with the target audience. So what we have done is alter our counter-messaging approach, and we've done this at the State Department with something called the Global Engagement Center, and we've gone -- shifted from the approach that says the U.S. government should be tweeting at terrorists and undertaking our own U.S. government stamp to counter-messaging and rather bringing in experts who can advise us on why is ISIL's messaging getting so much resonance.

And Brett McGurk talked about this yesterday, they're not drawing people in with beheading videos, they're drawing individuals in, and mostly young people in, with messages that have themes, and this we had some experts explain this to me and it was really interesting, with themes of strength and warmth and belonging. And how you counter that is a different proposition than trying to get into a religious debate with ISIL, which we in the U.S. government should not be doing.

MR. ISAACSON: You know, you kind of shunted aside the encryption question, but CIA Director Brennan yesterday on this stage just went at it really strong and said we should not be celebrating technology companies that are purposely building devices and systems to be out of the reach of the law and valid court's subpoena power. Do you believe that?

MS. MONACO: So I come at this as somebody who spent, before I came to the White House, 15 years in the Justice Department as a federal prosecutor, as a career prosecutor, as the Chief of Staff at the FBI and then as the leader of the national security prosecutions in the department. So I believe strongly that we are a system of laws and the system that we have built that has served us so well for many years and has dealt with technological innovation and our courts and our rule of law system has enabled us to balance that. So I believe we ought to be using that same approach here and that should serve us well.

Now, the fact of the matter is nobody has a stronger interest in strong encryption than the people operating classified systems, the people looking at the nuclear codes, the people who have a responsibility to make sure the air traffic control system is -- stays upright. So there is no scenario, as the President has said, that we in the U.S. government don't want really strong encryption. That said, what has been frustrating, I think, in this debate is there has been a series of discussions where there's a perception that both sides have an absolutist position. We got to get away from that. And I think that's what John Brennan was saying, I think, quite well and quite eloquently yesterday that we've got to move off the absolutist positions, and maybe we've got to break up this problem and make it a little bit smaller.

There are some issues that confront state and local and federal law enforcement when it comes to getting evidence to put the terrorists to the -- to put the pedophile, to put others in jail and make a case. There's a separate problem when it comes to data that's in motion. So how do we address both of those issues, they're separate, they present different challenges. But I'll tell you something, we, in the U.S. government, aren't going to be able to do it alone and there's no one-size-fit-all solution. We're going to need the innovative minds that have built these platforms to help us.

MR. ISAACSON: And what does your conversation say with Tim Cook or others been like recently on that?

MS. MONACO: So, you know, you talked about the delegation that I was a part of out to Silicon Valley earlier this year. You know, there is, I think, a real sense amongst -- and I think these are firmly held and legitimately held views -- that the greater good maybe in having strong encryption that is not accessible in any way to law enforcement and there are some people who have that view. I think that from the standpoint of somebody like myself and others with a responsibility with the public who expect us to stop terrorist plots, to enforce the law, hose come in real tension and --

MR. ISAACSON: So you still have that tension at the moment?

MS. MONACO: I think it's fundamental and it's not based on, I think, anybody not wanting to do the right thing. But people have, you know, people on this issue unlike any other, I think, I've confronted in my recent history in government, this is a really, really tough issue.

MR. ISAACSON: When the hack on the Office of Personnel Management happened last year probably by the Chinese, the Director of National Intelligence, General Clapper was on this stage and he kind of shrugged in a way and said, "You know, score one for them, this is the way spying works, and we're upset, but it's the way -- the way things happen." The hack on the Democratic National Committee, is that different, fundamentally different?

MS. MONACO: So I don't think we know enough yet. And obviously, as has been said I think from this stage and others many times over the course of the last three days, it'll surprise none of you particularly those of you in the press that I'm not going to comment on that specific investigation.

(Laughter)

MS. MONACO: But look, I think the debate at Hellespont is a worthwhile one. The debate about what does it take and when do we attribute and how do we attribute an intrusion, what is that all about and we can talk about that. And then once you discern that, what do you say about it and what do you do.

Now the process by which we've -- and we've evolved in this in the cyber security realm and there are some examples of it recently; the Sony hack the North Korean attack on Sony Pictures. That I think allowed us to utilize a series of best practices that we've built up and it kind of came together in the Sony situation. And what we did there was rely on the investigative agency. The FBI was on the ground working with Sony Pictures to investigate the incident, pool their knowledge with the

rest of the intelligence community, work very rapidly I think both to -- and this is important, share very quickly I think within 24 hours of them being on the ground in that investigation they were able to and we as a government were able to share information back out about the malware that had been used.

And so that is a very important cycle that we have to get into as a government because so much of the infrastructure is in private networks, right? So if the government isn't protecting every individual computer we've got to enable when we see threats to it get that information out just like we do in the terrorism context. So the FBI was able to do that very quickly.

MR. ISAACSON: Oh, boy, that's the only time I can think of that you named names. Meaning the Chinese -- I mean, you won't -- may not say, but Chinese everybody has said did OPM, Russians got into the White House and State Department a year ago and yet the administration has been reluctant to point fingers.

MS. MONACO: So I think I would challenge the premise of that question, although it was more a statement and less a question. So we did it in Sony. And we did so based on as I said, bringing the intelligence community together, looking at this, reaching a level of confidence, which is an important thing. You have to have a certain degree of confidence and ability to prove it, right? Because you're putting that out there and it's still drew some fire from some quarters.

And importantly though, to marry that attribution about the who did it, with what they did, right? And here in the Sony case, we discerned that this was activity that was unacceptable. It had crossed a threshold. It was both destructive, it fried the computers of Sony Pictures, took them offline and it was coercive. And those two things along with the -- our confidence in the attribution and our ability to talk about it in a way that would not disclose sources and methods and hinder our ability to make such attribution in the future, all combined to say you know we're going to call this out.

We called out the Chinese military members who hacked into a number of industries and I know because I started that investigation. When I was the Head of the National Security Division I started that investigation with great prosecutors up in Pittsburg and prosecutors from the National Security Division. And I remember going over and briefing my predecessor, John Brennan and sitting down in the now my windowless office and laying it out and saying this is what they're doing, these are the individuals we've identified, this is what we think is happening.

MR. ISAACSON: That was the National Security Division of the U.S. Justice Department?

MS. MONACO: That's correct.

MR. ISAACSON: Has the DNC hack been referred to the National Security Division of the U.S. Justice Department?

MS. MONACO: I'm not going to talk about that investigation.

MR. ISAACSON: Okay.

MS. MONACO: But my point being that this -- that in that case, we started the investigation when I was the Head of the National Security Division. It developed and what you saw a couple of years ago was indictments against five members -- military members of the PLA for cyber-enabled economic espionage against our companies. So what did we have there? We had strong intelligence, great investigative work rooted in a very high confidence level that these individuals were the ones who did it, that they did it at the behest of the state that we could prove that. We could disclose that without hurting our intelligence tools and their conduct was violative of both criminal statute and a norm that says you're not going to steal from our companies for the enrichment of yours and for your state.

MR. ISAACSON: So you started by saying you

first need the high degree of confidence?

MS. MONACO: Sure.

MR. ISAACSON: -- that you have it right. Approximately how long would it take on any hack like recent ones, I mean we don't have to go into any specifics, but if like -- if something happened in the sheer does it take weeks, months or a year to figure out -- I mean why does it take so long to?

MS. MONACO: Yeah, so the cyber security experts in the room will not be surprised to hear me say it's really a case by case situation. And it's really -- you know look, these actors some of them are more sophisticated than others. I would note that Russia apropos of nothing in particular is a particularly sophisticated actor. And they use very sophisticated tools. Different actors use different tools, whether it's state, sub-state actors. So there's no timeframe you can put on it.

But I think the point I'm trying to make is the framework we look at this through is first and foremost, an investigation that brings the government together, brings the intelligence community together rapidly. What do we know? How do we know it? What's our confidence level? And what have they done? So what I would say here is that the debate around this if this is an attribution that separate -- we need to separate the questions around this issue which is attribution and who did it is one question, what did they do and for what purpose is another.

And what I would say is, if there -- if this is an intrusion for the purpose of stealing information not to inform intelligence or inform their own governmental decisions but in order to coerce and take coercive action and undertake information operations and influence operations that is a different type of activity.

MR. ISAACSON: Okay, then let's stipulate, we're not talking about any one --

MS. MONACO: I hear you.

MR. ISAACSON: -- particular hack or whatever, but you just said something very interesting.

MS. MONACO: I hope so.

(Laughter)

MR. ISAACSON: -- which is what is the purpose and that there is a difference in purpose between trying to take that information for commercial reason --

MS. MONACO: Sure.

MR. ISAACSON: -- for spying reason, and take that information to coerce or influence a political system. Something else that John Brennan said, that this is a -- it would be theoretically a different order of magnitude if it were leaked simply to influence our election.

MS. MONACO: Without a question of doubt, that there are -- there are different reasons that we see intrusions. You may see an intrusion for the purpose of an intrusion, for the purpose of exploring, for the purpose of stealing information, for the purpose of simply understanding what that system looks like to be used for some purpose later.

You could see an intrusion for purposes of destruction as we saw in Sony or in the Saudi Aramco case or see an intrusion for purposes of stealing commercial secrets for the purpose of commercial gain in another country. These are all different approaches which I distinguish from traditional espionage.

MR. ISAACSON: And walk us down through what would happen -- what happens when you sort of have attribution? You're 95, 99, 99.9% sure of attribution, you're the person who has to coordinate then to get into a room with the President and say, do we or do we not name who did this. Walk us through that process, please.

MS. MONACO: So again it's going to be a case by case basis. It's going to be a question of the confidence level. It's going to be a question of what are the tools that are in place. And then what is the follow on, right? So naming and shaming is one thing, the responses that we have at our disposal maybe another. And I think something that this administration has been extremely clear about that all tools are going to be on the table, whether it's the terrorism approach to identify, detect and disrupt threats to the United States.

Similarly we've taken that approach in the cyber realm. So you've seen us employ sanctions as in the case of North Korea. You've seen us employ law enforcement tools as in the case of the China PLA case and frankly the Iranian indictments that the Justice Department did against Iranian actors for attacking and committing DDoS attacks against our financial sector as well as an intrusion into the Bowman Dam in New York.

So there is a range of tools, some of them maybe stated, some of them maybe visible, some of them may not be, some of them maybe diplomacy. All of those things are on the table when that discussion happens.

MR. ISAACSON: David Sanger, who is here, has a piece he just posted, which I know you've read. There's David, in the New York Times this afternoon online, which talks about this very issue of when do you name, what do you do sanctions, whether it's economics do you have, secret things you sometimes do maybe but also public things. In a case that involves a critical infrastructure which is our American political system; not talking about -- this could happen many times whether it's -- so I'm not just talking about DNC, I'm just talking about for politics, do you owe more to the American people to come forth?

MS. MONACO: You know, I think it is a -- I think John Brennan was right, it is a serious, serious issue, a serious thing if there is deliberate intrusion for the purpose of coercing and influencing the political process. I think one of the things this discussion is -- has important implications for both the scale of this if

this is a new technique, right, having using cyber means in yet another new way. And this is we've seen this across the board, right?

MR. ISAACSON: I'm sorry, what do you mean in a new way?

MS. MONACO: Meaning using cyber theft for the purposes of coercion or influence, right?

MR. ISAACSON: Got you.

MS. MONACO: So that is -- that could be we could be in a new world in terms of that as a new tool. Seeing yet again the cyber realm and the digital domain being a place where new tools are used for kind of old types of operations, whether it's stealing, espionage, influence campaigns. And the implications are I think very important. The scale, right, so the barrier to entry for something like this is really quite low. The ability to get in unseen doesn't -- may not take a tremendous amount of overhead costs.

Then the other thing is I think it makes us consider what is critical infrastructure. Everyone knows the power grid is and you know the air traffic control system et cetera, but how should we be thinking about critical infrastructure in a broader way.

MR. ISAACSON: So in other words, the electoral process maybe a critical infrastructure. Would that even mean you're trying to protect voting machines and stuff like that?

MS. MONACO: Sure. I mean there was a good piece recently I saw about what is the level of vulnerability to those types of industries that and also may only get used periodically. But it's all the more reason why I think the President has been very clear from his first days in office, the cyber threat is one that poses not only a national security, but an economic security challenge for us.

And we have seen a tremendous evolution in the

tools that are being used, the tactics, the vectors, the actors from nation states to sub-state actors to criminals or hactivists to of course terrorists. And the attack surface which cyber security experts talk about is so vast and getting bigger with the Internet of Things that it is really has to be a shared responsibility.

I am fond of using the terrorism model to apply to the cyber threat and I think there's a lot we can learn from applying a lot we can learn from how we changed our organization as a government to combat cyber threats -- I'm sorry to combat terrorism threats.

MR. ISAACSON: Right.

MS. MONACO: I think we can learn a lot and apply that to the cyber challenge, there's a difference though. 80, 90% of the networks in this country are in the control of the private sector or state and local actors. It is not the federal government. So we need to rely on that information exchanged with all levels of government and between the public and private sector if we're going to be able to defend ourselves.

MR. ISAACSON: Well, I hope you can protect us against the digital Chad's crisis for this coming election when it happens. One of the things that Aspen Security Group is almost modeled on the Aspen Strategy Group, if Clark won't take offence of that. And the Aspen Strategy Group began with Brent Scowcroft and others to do deterrents but deterrents when it came to strategic deterrents meaning nuclear weapons and that sort of thing. And one of the ideas and thoughts they came up with over the 40 years of this thing is that in order to have strategic deterrents, you have to be a little bit open and talk about your offensive capability. You have to say, here's intermediate range nuclear forces based here that will do this. Will there come a time when you think it's worthy -- worthwhile to talk about our offensive cyber capabilities?

MS. MONACO: I think -- I think there's some truth to that and I think there is a -- there is a framework that we are building that draws on exactly this

concept of deterrents and what are the signal-- what's the signaling that we have to send. Because in the cyber realm, as you say, what's acceptable, what's not acceptable, we haven't developed a set of norms around that. So the danger of escalation, misinterpretation is such that I think you know we have to be responsible about; but we should be very clear as we have been very clear that we will respond to those actions whether it's cyber or otherwise that threaten our interests.

Now the other thing we have discussions about with is that cyber effects don't always necessitate cyber responses. They should be on the table, but you don't always have to respond --

MR. ISAACSON: But are we developing a doctrine? I mean, we would know what to do precisely if a North Korean missile had hit the Sony lot, but we don't quite have the doctrines yet, how do we develop the doctrines and then work with the Chinese and Russians do, what would be the counterpart of assault talks in the '60s and '70s?

MS. MONACO: You know I think we do have a doctrine. I think it's the same doctrine in many respects that we apply in the physical world, right? Respect for sovereignty or taking into account sovereignty, we recognize an international law applies in the cyber realm. We have been working very hard over the last several years to bring the international community along to a set of peacetime cyber norms. Countries, nation states should not impair another country's critical infrastructure.

MR. ISAACSON: So in other words, they -- that norm which I've obviously read about and you gave a talk about means that in peacetime, it's generally now agreed upon amongst nations that you don't take somebody's electricity grid down or it's an act of war?

MS. MONACO: And or it's also a way to isolate those nations that do.

MR. ISAACSON: Right.

MS. MONACO: I mean, this is what --

MR. ISAACSON: But so you've created that one, do you think interfering in a political process should be at that level?

MS. MONACO: I think it's a serious question. I think it's something that if there is coercion, if there is destruction, the other thing I think we need to talk about is manipulation of data, right?

MR. ISAACSON: Right.

MS. MONACO: Which is --

MR. ISAACSON: In other words, stealing data, manipulating it, faking it and then releasing it to somebody?

MS. MONACO: Or intruding in a particular data system and manipulating that data and undermining the integrity of that data such that the owner of that may not know and may not be able to rely on the integrity of that data. I think that is a near to mid-term concern that we should be very, very focused on.

MR. ISAACSON: But we have offensive capabilities, do you think we should be -- I mean can you talk it all about hinting at what are -- what we could retaliate with offensively?

MS. MONACO: Well, we've been very clear about the use of cyber operations on the battlefield in the campaign against ISIL, right? Now I think we should be clear that we're willing to use that that we are using it, but I also don't think we should be telegraphing our punches. So I think there is a -- there's a reasonable distance between articulating norms, trying to bring the international community along, isolating those actors just as we do in the physical realm and in the physical space; isolating actors who violate international norms with a whole range of tools, whether it's sanctions, whether it's diplomacy, whether it's law enforcement, whether it's militarily. We should be building up those norms and we should be quite clear as we have been for instance in the

counter-ISIL campaign that cyber operations are part of the suite of tools that the commander has at his or her disposal and they will be used. But I'm not going to telegraph where we should be dropping the cyber-bomb anymore than I would be directing the F-16.

MR. ISAACSON: You will be happy to know, I am going to end with two friendlier questions about things that seem to be going right. We hear a lot about the border and how we can keep the border safe and people pouring in, and yet I have some the presentations that in the past year that's really gotten under control. Tell us how you got the border with Mexico situation under control, you and Jeh Johnson.

MS. MONACO: More importantly, the wonderful people in the Department of Homeland Security and the Border Patrol working with partners. Look, it's true that border apprehensions are kind of the leading indicator of those trying to cross the border or down. It's also true as we have seen over the last couple of years that the flow of unaccompanied children and families has increased over time. That is a function of a number of things including tremendously difficult and dangerous situations in Central America.

So what we've done is because under our laws if a child comes across the board, we've got a responsibility to provide care, provide an understanding as to whether or not that individual has an asylum claim et cetera. We've increased our capacity to address that flow of unaccompanied children and families. But importantly, we work with the Mexican government to help them control their southern border because it's their southern borders which impacts their northern border, our southern border, so we've worked very hard with the Mexican government to help them including giving them tools with experts from the Department of Homeland Security and Customs and Border Patrol to help the Mexican's control their southern border.

But importantly, to work with Central American nations to address really what is the root cause of some of these kids and these families making an incredibly

dangerous journey and working with them and working across the law enforcement and intelligence community to crackdown on the smuggling network. So you saw just recently, Costa Rica has agreed to provide a place where Central American refugees can go and not make that dangerous journey, but see if their asylum claim has merit even before they make the dangerous journey. And so we are doing more of that. So, all of that has combined I think to try and be first and foremost not sacrifice our safety, but to do so smartly.

MR. ISAACSON: And the other headline we read at the beginning of this summer was that it was going to be an absolute TSA nightmare that lines in airports were going to be, you know, what -- that didn't really happen, what are you doing technologically and in other ways, I know Peter Neffenger is here, that's Peter, they had a -- I shouldn't say that people will be coming up to you --

(Laughter)

MR. ISAACSON: -- trying to get TSA pre-clear. But Peter Neffenger gave us a really good briefing about three days ago on some of the things that have been upgraded, the technologies, everything from Atlanta to New York to Chicago airport and prevented and even bringing people back to work and TSA full time instead of part time to prevent this. How did that work in the White House and TSA?

MS. MONACO: Well, let me just say I am very glad you recognized Peter Neffenger, who is the administrator of TSA who -- this is the guy who runs into a problem, right, and does not shy from the problem. And when you've got all eyes on you and you know the world and the TV screaming that the world is falling, Pete and his team have maintained incredibly cool heads and really attack the problem. And you have mentioned a lot of things. I think Pete has applied his skills and his leadership as the former commander of the Coast Guard that he was, to bring a level of innovation, management reform and partnership with the private sector, with airports, with airlines and importantly, the state and local governments who by the way are responsible for those

airports.

So, all the things you said, innovating, creating a management structure and an incident command post at headquarters in -- at TSA to say what's happening in the system, how do we surge resources and address problems before they become acute. So all of the reforms that you talked about I think have combined to a point where I think 99% of the traveling public this summer has waited less than 30 minutes. So, focusing particularly on these top seven airports that really create some of the backlogs, it's been a tremendous credit to Pete.

MR. ISAACSON: I am going to go to the audience for questions. Why don't you bring a mic? Pete, did you want to say something on that? No, okay. I really wanted to give you some -- some little credit.

MS. MONACO: He is worried everyone wants to get their pre-check application approved.

MR. ISAACSON: Right here, yes and then -- okay. They will come running.

MS. HOWARD: Ma'am, thank you for being here. Well, the DHS has a --

MR. ISAACSON: Do you want to say your name?

MS. HOWARD: Oh I am sorry, I am just so excited. Andrea Howard, I am at King's College London right now. DHS has identified 16 critical infrastructure sectors, what do you personally see as most specific catastrophic target for a cyber attack either in the United States or elsewhere?

MS. MONACO: So, as you have shutters going through the crowd, look, I think what we have to understand is we've identified those 16 critical infrastructure sectors as a way to organize our efforts and our work with them. So, whether it's the financial institutions, the telecom networks, the power grid, the energy sector, I think what we need to recognize is because we are so intertwined, the attack in the power

grid may have a cascading effect or more importantly, the attack on one financial sector element may have a cascading effect. So, I am not going to sit here and give the terrorist actors a roadmap to where they should most effectively point their efforts. But what you've seen us do is try and organize our efforts and prioritize them.

MR. ISAACSON: Yes ma'am, right there and I will get to the back in a minute and then, yes.

MS. BRIGGS: Rachel Briggs from Hostage U.S. Thank you for your comments and for your leadership in this area. I wanted to ask you about the support available for the victims of terrorism. We have heard over the last few days that we are facing the very real prospect of more attacks here in the homeland in the way that we have unfortunately seen in Europe. Do you think at the moment that the U.S. government currently has the right level of provision for those victims who face really complex health and mental health problems over a very prolonged period of time?

MS. MONACO: It's a great question. And I think we should recognize Rachel Briggs who has done great innovative work at Hostage U.S. taking what is a very effective framework from Hostage U.K. and bringing it here to help families of hostages who have been killed or taken abroad, so just tremendous work by Rachel and her team. You know, I think the victim services, for lack of a better word, are what we are doing now from a federal perspective is really only one small piece of the puzzle, right? It has got to come at the local level, but we need to make sure that we have made available as much in the way of federal resources as we can.

So what happens in real life and I will tell you having spent time about three hours with the President when he was in Orlando meeting with the families of that devastating attack is what we try and do is have the victim services in that case from the FBI, really provide kind of a backstop and provide a network of resources that they can plug into the local communities. That's where I think we are best not coming in and big footing a local communities approach, but rather giving them tools, giving

them additional resources, but letting them say what's going to be the most effective thing for the communities that are devastated.

MR. ISAACSON: Yes, I think that was in the back, yes. Whoever it is, yes.

MR. WALDT: Very quickly before I have to catch my plane, I am sorry. I am [Eric Waldt], D.C. Metropolitan Police Department. As you've probably read or know Ted Koppel had a book out earlier this year called *Lights Out* that talks about the dangerous nexus between the cyber attacks and the vulnerabilities in our electric grid and he points some criticism at DHS and FEMA in particularly for lack of plans to handle a long sustained electric grid failure. Perhaps you could comment on what you see his criticisms, whether you believe them to be valid and what plans you see either in place or coming?

MS. MONACO: So, I have to confess, I haven't read Ted Koppel's book, although it was given to me as a gift for the speech I just gave at a cyber security conference. But --

MR. ISAACSON: So, you will read it or try it.

(Laughter)

MS. MONACO: In my copious free time.

MR. ISAACSON: Yeah.

MS. MONACO: Look, one of the things we are doing is working with what we call the sector specific agencies, right? So, the Department of Energy has undertaken I think a very focused and very good effort under the leadership of Erne Moniz and Liz Sherwood-Randall to bring the leaders of the power sector, the leaders of the electric grid all around the table to make sure that there is a place to intersect in terms of information sharing where we get information about cyber vulnerabilities, about malware that we are pushing it out both through DHS, but also through this -- through the sector specific agencies.

One of the things we've done to try and buck up that effort is create something called the Cyber Threat Intelligence Integration Center, CTIIC. Again building on the terrorism model, we have NCTC that is -- brings all of the elements of the intelligence community together to be aware of all the terrorist threats that we are facing and then make sure that the policymakers and operators have that information.

We've now done the same thing with CTIIC. Before last year, there was not one single place in the government even though we face such a big cyber threat, there wasn't any single place in the government responsible for integrating all that information. So, now CTIIC is doing that. And importantly part of its mission is to downgrade or declassify information that can then be shared by DHS out with industry including the electric sector.

MR. ISAACSON: And the electric sector is one among many that's partly private, sometimes public-private companies, you have both CTIIC and you've -- one of the few laws that got passed this year was to enable information sharing and even reduce the amount of risk you would have from antitrust --

MS. MONACO: That's exactly right.

MR. ISAACSON: -- that you have shared with other people.

MS. MONACO: Yeah, we've --

MR. ISAACSON: But how do we get people to share more because we kept hearing his week that still industry isn't sharing quite enough?

MS. MONACO: So, look, I think this is going to be a bit of a cultural evolution. One of the things about the cyber threat is it's not all technology, there is a lot of human behavior involved, right. The seatbelt analogy I think is instructive. There was a time when we didn't all get in our cars and reflexively put on our

seatbelts. But we have to over time change our behavior around common cyber security practices. So one of the things that we did in passing bipartisan, yes, bipartisan cyber security information sharing legislation last year was to put in place a framework that said, if you share information about the breach that has occurred in your company, you do so through the Department of Homeland Security after you take appropriate privacy protection measures on that information, you, company X, will have liability protection for sharing that information.

I think companies were both very fearful of sharing information with the government for fear that their customers or shareholders would sue them for that and they were I think fearful of sharing with each other on the theory that there will be some allegation of collusion. So two things that we did was make very clear what the antitrust rules of the road were and that a company would receive liability protection for sharing information with the government.

MR. ISAACSON: But they say this taking for example Centers for Disease Control, if somebody gets Penicillin anywhere, gets bit anywhere by a mosquito, it all goes into a big database and they have huge amounts of data and they analyze it. We get hacked at the Aspen Institute two or three times a month, we don't have a database we can just send it to. Why isn't there a big national database like the Centers for Disease Control has where you can have experts and even the public looking in and trying to figure out the pattern?

MS. MONACO: Well, so I would argue, that's in large part what DHS has done and Suzanne Spaulding is here somewhere, she and her team at DHS under and I am going to throw yet another acronym at you, bear with me, it's called the NCCIC, the National Cyber Communications Integration Center and what that does is, this information whether you're a company, whether you're a state and local government, whether you're from a particular industry, share that information into NCCIC which has all of the government alphabet soup present in it, but it also importantly has industry present. So, it has representatives from industry sectors sitting side-by-side

understanding what that information is. So that really is the type of --

MR. ISAACSON: Yes, but let me push back.

MS. MONACO: Sure.

MR. ISAACSON: In the minute it took us to discuss this, let's take Citicorp, probably got twice hacked and attacked and they caught, they didn't send that information to you, did they? They are not doing it yet.

MS. MONACO: Well, I hope -- I hope that they are going to avail themselves of what this legislation put in place, which is it said, DHS needs to have a automated indicator sharing system, so to make it a lot easier for companies and frankly for government agencies who also have been victims to share that information.

MR. ISAACSON: Yes sir. Okay. I can't see because of lights.

MR. BLUM: John Blum is my name. Isaacson has been pushing you all evening to try to get you to talk a little bit more about our aggressive side. And when I hear public officials talk about our morality and how moral we are, it scares me. We are not dealing with moral people, we are dealing with people in Russia and especially in the Middle East that don't have the same kind of moral structure we do. So, can you give us some kind of sense of what aggressive positive things we are doing, can we hear what's going on, the top officials in the Kremlin, can we hear what's going on in the Middle East when two guys talk together who are officials and important, or don't you want to comment on that at all?

MS. MONACO: If you're asking me to disclose what our intelligence methods are and where they are, I will decline your kind invitation.

MR. ISAACSON: Well, you assures that we're at least being aggressive.

MS. MONACO: In the cyber realm, in the military

realm, in the law enforcement realm, absolutely and I don't think that there is or there should be a whole lot of debate about that. When you look at the number of terrorists that we have taken off the battlefield, with the amount of territory that ISIL no longer controls, with the 14,000 strikes that have occurred in the campaign against ISIL in Iraq and Syria over the course of this --

MR. ISAACSON: Okay, let me -- hold it right there, you just said 14,000 drone strike or strikes, whatever, some drones, some not, again why don't you say what cyber attacks we have done, if can say what drones and other strikes were done?

MS. MONACO: Well, because I think it's a lot more difficult to say, look we can lay out the list and we have laid out the list of the leadership of ISIL and Al-Qaeda that we've killed with drone strikes, with Special Forces operations and the intelligence that has yielded that, which has led to yet more operations. That is something that you can see and you can describe. But the cyber methods that we are using, I personally don't think it makes a whole lot of sense to describe that for our adversary who can anymore than it would make sense for me to say, tomorrow we are going to strike the oil infrastructure at these coordinates next to Damascus, that doesn't make a whole lot of sense to me.

So I am not sure why we would transmit what cyber effects we would have in that realm either. That said, we should be very clear about the norms that we are applying. So, for instance, in the kinetic world, when we are dropping bombs, we do so under a set of laws and norms, the law of armed conflict which you and the rest I hope of the citizenry can have confidence that we are doing so adhering to the laws, adhering to proportional collateral damage as has been talked about and that we are doing so consistent with our values. I don't think anybody should shrink from that, I don't think it's something we should apologize for, that's what makes this country great.

We should I think have the same confidence and you should be able to have the same confidence that we are

applying that framework in a way that is effective and protects our interests and aggressively under the same framework in the cyber realm.

MR. ISAACSON: Yes, back there and then I will catch you next. Sorry.

MR. BLATZ: Hi, [Bob Blatz], Cincinnati. Could you comment on a recent article in the Wall Street Journal where they were reporting or German intelligence was reporting that Iran was acquiring nuclear materials?

MS. MONACO: I can't comment on that, although I would refer you to, I don't know if you here for John Brennan's --

MR. BLATZ: I was.

MS. MONACO: -- comments yesterday about the monitoring of the joint comprehensive plan of action and his description of Iran's compliance thus far there.

MR. ISAACSON: And so basically not to get in the specifics, we should feel assured that there has been in general compliance with the joint plan of action.

MS. MONACO: Thus far, and again I would say, I think John's comments about that hit the mark.

MR. ISAACSON: Yes ma'am, in the white. Yes.

MS. LEMMON: Thank you so much. Gayle Lemmon from Council on Foreign Relations. And I just had a quick question. I was speaking with military folks recently who are doing counter-ISIL messaging and they talked about the frustration and the challenge of doing that when you're up against people who are really nimble, really flexible, don't have a 12-step process of approvals to go through before they get their messaging out. And I wonder if you could talk about the challenge and the mismatch there.

MR. ISAACSON: Good question.

MS. MONACO: Yes, I've heard and we have talked about this in terms of DoD's operations on this score. I think the counter messaging that we are talking about here and I that was referencing earlier really is about enabling, amplifying other voices, right? So, the individuals or the voices, the credible voices in the Gulf and across the Arab world where 90% of ISIL's messaging is done, that needs to come not from us, frankly not from DoD, not from state, not from anybody else again with the U.S. seal, but from voices that are going to be credible and targeted at frankly the target audience. And what we've been trying to do is build up those voices, working with for instance the Sawab Center in the Emirates, doing the same thing that we are going to be doing in Malaysia. So, that's really where we are trying to target our counter messaging.

MR. ISAACSON: Yes. Kimberly, yes.

MS. DOZIER: Kim Dozier at the Daily Beast and CNN. Lisa, do Americans need to get used to the concept of terrorism like they got used to the concept mass shootings. We've heard this week that in the near-term there might be a military defeat of ISIS on the battlefield, but that the generational fight to come will be against ISIS, Nusra, Al-Qaeda in smaller forms.

MS. MONACO: So, it's a good question. Look, I think the spate of attacks particularly that we've seen over the last say six to eight weeks when you're talking everything from Istanbul to Orlando, to Dhaka in Bangladesh, Saudi Arabia, you name it, I think people rightly have a sense of unease and I think it's because it is so unpredictable. So, I often get the question, are we in the new normal and I think that's really the point of your question. And I hesitate to agree with that premise because I don't think the type of carnage and depravity that we've seen for instance in something like Nice, that should never be, we should never consider that normal.

If we've gotten to that point, I think we've lost our way. But I do think that and this gets back to the start of the question that Walter asked me, we are in a different moment and we are facing a threat that is much

more unpredictable. And what I think Americans need to recognize is that they got to be part of the apparatus that enables us to prevent these, right? So it has got to come from the communities, law enforcement and intelligence as we talked about earlier is not going to necessarily be able to identify the person who radicalizes very quickly, has no contact with Al-Qaeda, Nusra, ISIL, Boko Haram, you name it, has no outward direction and we are going to have to engage more with communities to divert that individual, keep them from going down that path, but divert them if they get on that path, that very dark path to violence and but at the end of the day, we are going to have to rely and I'm heartened when I think about this because I think this is something that we have readily in our toolkit, which is the resilience of the American people.

We've seen it time and time again from Boston to San Bernardino to Orlando, we are going to have to remember and continue to draw upon the resilience in our communities because we will continue to face violence from deranged, radicalized extremists of all stripes and we are going to have to continue to summon the resilience to address it.

MR. ISAACSON: Yes, now we have gone a bit long and I appreciate it Lisa, your willingness to stay. Well, there are a couple more questions, way back there, I have been discriminating against the way back.

MR. MARTIN: Thank you. Todd Martin from Aspen. I am not sure this is a question directly in your current responsibility, but I am sure you are close enough to answer it, which is how is strategy determined at the very top level in the zone of ISIL and the Middle East because there is political issues, there is military issues, there is history, there is cyber. How is strategy determined so that President Obama or any other president would have the smartest way forward through that mirage of difficult factors?

MS. MONACO: You mean U.S. strategy, you are talking about, yes. It starts from the top, from the president based on discussions with his National Security

Team and I'm at that table. So actually your question is more on point than maybe you think. And it starts with his direction and what you see reflected is evident in the counter-ISIL campaign, which is that strategy is not solely a military strategy, it is not solely a humanitarian effort, it is not solely a diplomatic strategy, it is a comprehensive approach first and foremost to squeeze ISIL where it is in its twin capitals of Mosul in Iraq and Iraq and Syria and as Brett has very capably talked about and has been leading this effort to go after its networks, whether they're financial, whether they are foreign fighters, manpower, whether they are network of messaging and then to go after the branches that they have been able to have take root in and now eight different provinces.

So the strategy comes from the president's leadership that this has to be a comprehensive approach that relies on and is done in concert with a stable of partners across the globe. We now have 67 partners in this coalition and that comes from the president's leadership that our strategies got to be one that's done with partners, that is comprehensive, that cuts across and is built on the notion that we are not going to ultimately have a solution to the problems in Syria and Iraq solely militarily, but it has to be one that's built on a political foundation.

MR. ISAACSON: Lisa, you are about to end your term in a few months. Let me let you end by reflecting on what it's like to be sort of right in the center every morning at 5:00 a.m. to be hit with things that you are going to have to brief on in a couple of hours. Tell us a little bit about how you feel just a career prosecutor who suddenly ended up in a situation room.

MS. MONACO: You know, it's unbelievable I think sometimes when I reflect about how incredibly fortunate I have been to be able to have a series of roles where I hopefully have been able to contribute, whether it's being a career prosecutor which as an assistant U.S. attorney, it's the best job in the world to get to stand up and say Lisa Monaco for the United States, to helping FBI Director Mueller transform that agency from a law enforcement,

solely law enforcement organization to a national security organization, to leading a group of incredibly professional prosecutors at the Justice Department to now sitting in the Oval Office every morning with the President talking to him about the challenges we face, I think I'll ultimately get over the fact that he basically refers to me as Dr. Doom because nothing I bring to him is ever positive.

MR. ISAACSON: Whenever he sees your name on phone ID, he knows something bad has happened.

MS. MONACO: Yes, it's usually not good news. But that's an incredible privilege. It is absolutely unrelenting, but it's an incredible privilege to contribute and to have as your job to help the National Security Team, basically the job description is to help keep the country safe. It doesn't get any better than that.

MR. ISAACSON: Yeah, that's what we've heard all week, whether it's Jeh Johnson, Peter Neffenger. We thank you for your service and thank you for being here.

(Applause)

* * * * *