THE FOUNDATION FOR DEFENSE OF DEMOCRACIES HOLDS A
DISCUSSION ON CYBER WARFARE IN THE NEXT ADMINISTRATION

NOVEMBER 18, 2016

SPEAKERS: FORMER CIA AND NSA DIRECTOR MICHAEL HAYDEN

SAMANTHA RAVICH,
CSIF BOARD MEMBER,
FOUNDATION FOR DEFENSE OF DEMOCRACIES

CLIFFORD D. MAY,
FOUNDER AND PRESIDENT,
FOUNDATION FOR DEFENSE OF DEMOCRACIES

[*]

MAY: Good morning, everybody, and welcome. You all know where you are and I think you know this organization; this is the Foundation for the Defense of Democracies. I am Cliff May. I am the president. I think you also know, we've been in business since just after the attacks of 9/11/01. We are a policy institute, we are non-partisan, we try to avoided politics as best we can, you all know how difficult that can be in this town, but we try.

Today's conversation is Cyber Warfare in the Next Administration. FDD is pleased to host this conversation in coordination with the launch of our Center on Sanctions and Illicit Finance project on cyber enabled economic warfare. We're looking forward to sharing our research from this project in the coming weeks and months.

While you hear a lot of discussion in this town about cyber war and the cyber battle space, the cyber domain as General Hayden has called it, and was the first to call it, recognizing it as a domain of warfare along with land, sea, air and space. There is far less understanding of how U.S. Adversaries are using cyber as a means to engage in economic warfare against the United States and other countries as well.

Too often we dismiss individual attacks as cyber crime or cyber espionage, or cyber vandalism, without understanding our adversary's strategy, and the broader campaign.

Thanks to Samantha Ravich's thought -leadership in the growing challenge, we at FDD are looking at what our intelligence community needs to be examining and what policy makers need to understand in order to craft smart strategies to succeed in this new environment.

Samantha will be leading this CSIF project we're pleased to have her moderate today's conversation with General Michael Hayden, who has been a tremendous resource to FDD for a very long time, he serves on our leadership council. Before I hand this over to Sam -- which I'm gonna do right now -- please silence your cell phones and make sure that you have no listening devices that you aren't aware of on your person.

Thank you very much Sam.

RAVICH: Thank you, thank you.

And, thank you all for braving the morning commute and I want to introduce General Michael Hayden. And, for those of you who may have commuted from Mars and don't know the good general, I just want to go quickly, a little bit over his background. Of course, he's a retired U.S. Air Force four-star general, former director of the National Security Agency, director of the Central Intelligence Agency.

He is also, as some of you may know, an avid Pittsburgh Steelers fan. He's had a bit of a rough season. And speaking actually as a Giants fan, I was disappointed in the Steelers' loss to Dallas last week, but I have to admit on December 4th I won't be cheering for Pittsburgh when they play the Giants.

OK, but -- but -- but back to business. Let me say that Mike is really one of the most cogent and thoughtful leaders and thinkers in our time on the evolving threat of cyber. I'm honored to have him on the advisory board of our Project on Cyber-Enabled Economic Warfare, which is focusing on a very specific part of the cyber-threat domain.

You'll be hearing a lot more about our -- our research over the next year, year-and-a-half, as Cliff has discussed. But I just want to introduce you to that term, "cyber-enabled economic warfare," and the definition of it, which is -- it refers to a hostile strategy involving attacks upon a nation via cyber technology with the intent to weaken its economy, and thereby reduce its political and military power.

All right. So we have structured this conversation, the general and I will -- will talk for about 30 minutes, then we'll open it up to Q&A. So I want to get this part rolling with a -- with a question and get your thoughts on the evolving battlefield of cyber.

But I want to hearken back to-- you recalled where you were and what you did on the morning of September 11, 2001?

HAYDEN: Right.

RAVICH: And how you called for all nonessential personnel to leave NSA, leaving about 5,000 people in place; and how in the days that followed, you were asked by the president and -- and the leadership: Was there any more you could do? And how you went to the White House and recommended to President Bush that there was more you could do if given the proper authorities. And in those days, that meant understanding the evolving terrorist threat with new applications of signals intelligence and new analytic capabilities around big data.

So I ask you this: So that we don't suffer a cyber 9/11, is there more that we can do now? Do we need new authorities, new technologies, a new organizational structure? Or do we have most of it in place and we just have to have to maybe have the new will or -- or thought to go forward?

HAYDEN: Yeah. No, I wouldn't assume we have it all right and we're fine and we can throttle back. But Samantha, when I went to the White House and the president says: Can you do more? I said I've got a couple things I can do, but I don't have the current authorities to do it.

I was asking for authorities within a broadly agreed framework of American law and policy, and frankly, political culture. Now if you read the outcome of the program called Stellar Wind (ph), you know, it wasn't universally agreed. All right? It was -- it was very, very contentious.

But at least I was asking the question within a well-developed framework. And people can disagree whether we're leaning left or right, but then who were left and right were. The issue with this is we don't have that developed framework. All right?

I am fond of saying that the most powerful limiting factor right now on our cyber capacities -- offense, defense, espionage -- are questions of law and policy, not -- not questions of capability; not -- need a lot more technology; always use more talented people. But fundamentally, the big issues, what we call LIMFACs (ph) when we do planning -- limiting factors -- are law and policy.

What is it we -- 320 million we -- what is it we want? And more importantly, what is it we will allow our government to do in -- you heard the description of cyber as a domain -- what is it we want? What is it will we allow the government to do up here to provide us the same kinds of services we have roughly agreed on how they will provide them down here in physical space?

So I -- that's getting really metaphysical, but it really comes down to that.

And so when I was in government, now this is eight years, but we couldn't do anything up here without having a meeting the situation room. I mean, there were no precedents. Every -- every issue was -- was new and had to be -- had to be decided at the highest levels. And so that -- that's where we are.

So a little additional to what Samantha described as their work, cyber-enabled economic warfare, we had a dinner not very long ago with folks like us talking about it. And -- and it resembled a bunch of Jesuits and a bunch of Dominicans trying to decide on the ample description of the Trinity. All right? Right?

(LAUGHTER)

Because it was those kinds of fundamental questions.

I can see what it is. What should we call it? Because, you know, how we think through things is to abstractly put them into categories, and we don't have clear categories -- offense, defense, exploitation, economic warfare, cyber warfare. And so we're struggling with that.

And so I do agree the organizational structure has to evolve. I'll give you one example and I'll stop.

So the -- the -- the ancestor of the Cyber Command was something very clumsily named Joint Functional Component Command Net Warfare. And -- and I was the commander. All right? So I was the first director of NSA to actually have a Title X war-making chain of command that could tell me to tell the guys: Turn your hats around and go do something NSA is not allowed to do.

America is allowed to do it. NSA as NSA is not allowed to do it. In other words, I was using war-making authorities coming out of the Title X chain of command. All right?

And so we were explaining that, Jim Cartwright and I were the -- he was my commander. And we were explaining to the Chairman of the Joint Chiefs Dick Myers at the time. And General Myers and I, we go back long time, Air Force guys, kind of going back and forth. After Jim leaves the room, he says "Mike,

come on, straight on: Is this going to fix this?" And I go, "Oh no, no, not at all." I said, "But we will be back to you in a couple of years screwing this up at a much higher level than we're able to do now."

And you know, he was a friend and I was being flip, but it was true. You know, this -- this was a step process in terms of getting the correct intellectual framework for this new domain, new form of combat.

RAVICH: So let's turn to one of our greatest challenges, adversaries in this space, Russia.

We've seen them be very active in a lot of these so-called "bear attacks." I don't know with the DNC hack, if it has a bear name attached to it...

HAYDEN: Yes, I think it does.

RAVICH: ... but it probably does. But the Fancy Bear attack was against the Olympic committee. Then, of course, there's been a discussion about Russian attacks on -- on Ukraine power grid.

HAYDEN: Yeah, power, yes.

RAVICH: Power grid. And a whole slew of other -- of other -- other events and attacks. So where -- talk -- talk to us a little bit about how you see that threat evolving. How we begin to think about deterrence, if there is, against what the Russians are doing.

And where they may be vulnerable. If we're starting to think about how do we understand the Russian escalatory ladder in this...

HAYDEN: Right.

RAVICH: ... space, part of it is understanding where they're vulnerable.

HAYDEN: Yes. So, to review, in my personal view -- by the way, it's rare that our government actually goes and dimes out a cyber aggressor. We've done it twice in my memory; the North Koreans and now the Russians. So when we do it, I think you can take it to the bank, all right? We're -- we're sure.

All right, so the Russians penetrating the DNC and stealing e-mails, all right, I've said publicly and I will repeat for you, is honorable international espionage. It is what nation-states do to one another. And so if I'm going to pass any moral judgments here, shame on the DNC for not protecting their information, not shame on Russia.

If I could have penetrated -- not that it would do any good to penetrate United Russia's internal e-mail system to learn about the future of the Russian state. But you realize that intelligence services' highest priority is to divine leadership intentions of potential adversaries. And if I've got a big geostrategic adversary and I have sources of information that would inform my government's judgment about their intentions. Hey, game on. I'm going after it.

So I -- again, I -- I -- I've got to separate this issue. And so the theft, honorable international espionage. The weaponizing -- the weaponizing of the information is something different, all right? And here, you've got the Russian Federation -- I think -- I think everyone agrees these are Russian criminal

gangs acting on behalf of the Russian state, stealing the information, giving it back to the Russian state. Then the Russian state is actually washing the data through WikiLeaks and then you've got this relentless drumbeat.

In essence, an attempt to corrode, erode confidence in American political processes. Quite different than just honorable international espionage to learn about what a potential future president might do about X, Y or Z. What you've got is the Russian Federation trying to erode confidence in the political processes of the most mature democracy in the Western world. Ouch. That -- that's a big deal.

So when I think about that, the first thing I -- I think, Samantha, is do not drop this into "we've got a cyber-problem" box. My first instinct is drop this into, "we got a Russia problem" box, all right? And so I'm going to get to the cyber response in a minute.

But I -- but I do think, if I'm -- if I'm advising, if I'm going to the meetings in the small room down the street and talking about this, my counsel would be do not narrow your focus to this cyber attack. Put this inside the box with all the other things that the Russians are doing, all right?

So the appropriate response here might actually be defensive arms to the Ukrainians. The appropriate response might be building LNG ports on the east coast of the United States and the west coast of Europe so that we undercut European dependence upon Russian gas.

Now, if you want -- if you want to have a part of your menu be cyber, all right, Jim Stavridis, former SACEUR, has written about this. And I'm copying Jim's words because I think they're very good. One thing you could do is doing a bit of naming and shaming about, let's say, Russian oligarchic kleptocratic financial transactions. Which one -- one could do.

A second would be fundamentally just attempting to disable the platforms used by the surrogates. Not bad. A third, and what is really attractive to me, is to do everything in your power to push into the Russian cyber-sphere as much anonymizing technology as you possibly can, because nothing will get the attention more of the Russian leadership than threatening their ability to monitor their own population.

And if -- if, you know, you want to pull the chain and say, "You know, you might not want to play this game so aggressively." That looks to me like -- like a -- number one, it's actually a good idea in its own right. But it also plays to the needs here.

So we're not without tools. I don't know what we have done. Jim Clapper said yesterday in his farewell address in front of Congress that they did see a change in Russian behavior after the announcement and after the warning from our government. But that's all I know.

RAVICH: That's interesting. Some have suggested that at least some of the hacks and exploitations and then the publishing of the information was as much to validate and normalize certain Russian behavior...

HAYDEN: Yes. Oh yeah, yeah.

RAVICH: ... as it was to undermine us. So -- so on the DNC hack, Putin's facing an election coming up...

HAYDEN: Yeah.

RAVICH: ... and "Oh, there's corruption everywhere so my corruption in Russia is just part of the international norm."

HAYDEN: No, I think -- I think that's right.

RAVICH: Same with the Olympic committee. "Oh, sure they're coming after our athletes for taking drugs, but look, everybody else is taking drugs as well."

HAYDEN: It -- it -- it is a perfect image of what happened after the shoot down of the Malaysian airliner several years ago. I mean, the facts in that case are so obvious they scream for -- for some sort of international response that RT, Russian television and the Russian State, pushed so many alternative stories out there that a lot of people said, "Oh man, this is just really hard to figure out."

They -- they -- they created a sense of equivalency for other false narratives, just like they did here.

RAVICH: Yeah, yeah. And one other point on this I'd love to get your take on, there's been some suggestion that these different bear attacks -- so-called bear attacks are actually different Russian intelligence agencies going after each other.

HAYDEN: Yeah.

RAVICH: There's a competition...

HAYDEN: Sure.

RAVICH: ... you know, just as -- just as here where lots of agencies are competing for resources. You know, we look over there -- they're competing for resources as well. Does it strike you as reasonable and...

HAYDEN: Yeah, it does. Yeah, very much so.

RAVICH: ... probable?

HAYDEN: Very -- very much so. Perhaps even more so inside the Russian Federation. I mean, we -- we -- we get marked down for the lack of sharing. But -- but frankly, we're pretty actually pretty good at.

RAVICH: Yeah.

HAYDEN: I mean, if we're marking on the curve, we'd actually be honorable, all right? But we don't mark on the curve. And so if you look at another intelligence structure where the sharing is less, where the compartmentalization is stronger, even more of a case for that.

RAVICH: Let's talk about international norms for -- for a moment.

HAYDEN: This will be a brief conversation.

(LAUGHTER)

RAVICH: Yeah, right. Well that's -- that's what I want to get your take on. I mean, is it -- is it possible in this space -- you know, some have suggested that we should -- you know, be working -- if not full cyber alliances, but certainly stronger cyber partnerships. We -- we have something we signed, obviously with the Brits. We work within a lot of other nations more quietly in sharing of technologies, sharing of information.

But is there something beyond that, at least amongst the friendly nations...

HAYDEN: Yeah.

RAVICH: ... that we can kind of work towards norms, leaving out those that are truly in the adversarial camp?

HAYDEN: So, hard work. All right? Hard work because we've got to do our own internal thinking as to acceptable and unacceptable behavior. So, to return to an example I gave earlier, the hack into the DNC, we would have done the same thing. We do not view that to be inconsistent with accepted international practice.

The OPM hack -- and this time, the government didn't say it was the Chinese, but I'm telling you it was the Chinese -- the OPM hack, that's also consistent with international practice. It's offensive, all right. And in our language we -- we -- we lump those things in with the Sony North America attack from the North Koreans, which we all agree is not accepted international practice.

So, the first thing we've got to do is to really make our language very, very precise, all right, in terms of what it is we think should be normalized in the sense of creating norms. So, we -- after the Edward Snowden thing came out, it was in high dudgeon -- I'm actually in Hong Kong being briefed by South China News, microphone in front of me -- and says, "Edward Snowden's documents say you spy on China."

I go -- and my answer was, "I certainly hope so."

(LAUGHTER)

And I said, "But we self-limit." We have -- we have a definition of accepted international espionage, which is we'll go steal other people's stuff to keep you safe and to keep you free. We will not steal other people's stuff to make you rich, all right? That -- that -- that is American normalized behavior.

And -- and to be modestly optimistic, a year ago, Xi Jinping was in this city and signed a document with President Obama that accepted our definition of legitimate state espionage.

So again, I guess my point is we have to be very, very precise with our language, be very careful in our negotiations.

Now, to really answer your question. How do you create norms and go forward? I think you work from the inside out, all right? I think, number one, we get our own act together. What is it we think's

acceptable? So, we think breaking into a foreign political party might be justified in some circumstances. I think we all agree there are no socially accepted reasons to have a botnet.

So, we can begin to sort that out. We get our own ideas clear. And here I'm making it up, but I think then the next conversation is amongst the Five Eyes. You know, like-minded folks; common value, common history, shared secrets. So I think we would begin to get a pretty good consensus from that group.

And then maybe the next is G-7. OK. Again, people of like-minded values. And then, G-20, people with skin in the game, people who might look at this in the same way you do to create broad international understanding of accepted and unacceptable practices in the cyber domain. Not treaty language beyond...

RAVICH: Right.

HAYDEN: ... anything I can imagine.

RAVICH: Right, and of course one country that isn't in -- in those categories, but has some of the best technology outside of us...

HAYDEN: Yes

RAVICH: ... and the Brits and a few others is Israel.

HAYDEN: Yes. Sure.

RAVICH: So, certainly a player potentially in a new type of framework or -- or partnership arrangement.

HAYDEN: But again, you're establishing norms. You're -- you know, you are -- you are -- you are a citizen in good standing in the cyber domain or you are a renegade in the cyber domain. Look, this is halting and slow. But you know I've got no secret sauce that we're going to use and get this -- what's the right word -- put into law and statute and...

RAVICH: Right.

HAYDEN: ... hard and fast, black and white, right angle norms, all right?

So, I -- I'll give you an example. All right. There is a biological weapons treaty, I know, I know that. But fundamentally, if you got biological weapons, you're bad. We -- we don't want to -- we don't want to hear about your arguments. We don't want to hear about your big next neighbor. We don't want to hear you're only going to use them in defensive purposes and extremists. You got bio, you're bad.

I think we can begin to build some of those sorts of -- you host botnets, you're bad. That is unacceptable behavior.

RAVICH: Before I turn it over, one -- one other question. So, new administration coming to town.

HAYDEN: I heard.

(LAUGHTER)

RAVICH: Yes, you all heard? You all heard about this?

And so -- so, thinking about the priorities that the new administration should set on -- on the cyber domain -- and let's talk broadly, I mean, you know, in terms of cyber R&D to cyber norms to cyber deterrence. How should those folks start thinking about what to prioritize with obviously as resources always are, they're limited? Limited in personnel, limited in money, limited in time.

HAYDEN: Yeah, so, I think instinctively, everyone in this room thinks it's a big deal. This should be near the top. All right. But it is not something that either campaign really campaigned on.

RAVICH: Right.

HAYDEN: And when the question got asked at the debate, Secretary Clinton gave it an undramatic, but somewhat coherent answer. And President-elect Trump -- really this was very unfamiliar turf for him. And I get asked, "So, who -- who in the incoming team is the cyber guy?" I -- I don't know that, all right?

And so, that -- that -- that I think is a promise to be kept that the incoming team is going to have to express its views on cyber and to organize a team of the right kinds of folks.

Can I give you a slightly different thought that I think answers your question? So far, we've been talking about what the government ought to do, all right? And I would just suggest to you that we need to widen the conversation. That -- that cyber defense -- even the creation of cyber norms may actually have a stronger private sector quotient than say Herman Kahn's on thermonuclear war had when he was trying to solve the last time when we had this kind of problem.

And so, I -- in the long form, when I give these presentations to trade associations, I talk about the first line of American defense in the cyber domain is the private sector, it is not the government. And for most questions, it's only the private sector, all right? And so, when we have these kinds of conversations, we need to be sure we start tugging in the private sector thinkers.

I'll give you I think a true modestly troubling thought; one of the things we haven't figured out in the cyber domain is the 21st century definition of reasonable expectation of privacy, right? That's -- we're still dribbling that ball at half court. I would offer you the view that Mark Zuckerberg is going to have more to do with where we land than any act of the United States Congress.

And so, we might want to weave him into the broader conversation. So that during the campaign -- and I think this was instinctive and not thought through -- but during the campaign, when Mr. Trump said, "Don't buy Apple. Throw away your iPhones and they should open the damn phone in San Bernardino."

When you decompose that, all right, there is clearly a legitimate need for law enforcement to get into that phone. But I have serious doubt as to whether or not it trumps the broader national need for high-end unbreakable encryption. And so, I guess what I'm saying to you is to date, the incoming guys when they talk security, seem to talk about it in a linear, industrial, physical sense. And there are ways of doubling down to create that security here that actually might make it harder to do this security here. And so I hope as they go forward, the horizons get broadened. One other ray of light, after the OPM hack, the

president threw $17 billion at the problem and said, go do more of what you're doing to make us safe, which is OK.

He didn't say, go do different, but he did launch a private-public commission. And you've got some very bright minds on it. Keith -- I think Keith Alexander's on it, I think Eric Schmidt's on it, all right? And those guys are due out in December. So you've got the $17 billion to go do more, I think the charter of these guys is go think different. And so I would really like the incoming administration then, because this was obviously designed for them, to pick up what these guys are saying. To incorporate that, accept, reject, sentify, vilify, whatever, but at least bring it in and make it part of their thinking for the next steps.

RAVICH: That's great -- that's great. And I would add, I think there's been an underappreciated role for the states.

HAYDEN: Yes.

RAVICH: You know, we talk about the public-private partnership and it's always thought, especially in this town, that it means Washington and the private sector, but of course the private sector happens in the states and there's a great role for bringing them up to speed and having them be in the interlocutor with the people they know best which are actually living and working and creating jobs in their states.

HAYDEN: Yes, let me double down on that because in my second life, eight years out of government, I actually kind of mixed with this and so you've got the research triangle in North Carolina, you've got the Silicon Hills West of Austin, you've got the Silicon Bayous outside of the gates of Barksdale Air Force Base at Bossier City. Every one of those sponsored by their governors, all right? Trying to bring cyber industry, cyber education and re-purposing National Guard units when they have their A-10s and C-130s taken away and making them cybersecurity units to defend dot-NC, dot-TX, dot-LA. Great idea.

RAVICH: Yes -- yes, that's great. Great, I'm going to open it up now to questions. Please. I'm going to put on glasses, I can't see. You're all fuzz.

QUESTION: Michael Gordon, New York Times.

HAYDEN: Here it comes, Michael.

QUESTION: Michael Gordon, New York Times. It's been confirmed that Mike Pompeo is going to be the next director of Central Intelligence Agency...

RAVICH: There you go.

QUESTION: He doesn't seem to have a background in -- a deep background in intelligence or cyber issues. What's your reaction to this selection?

HAYDEN: I know the Congressman. In my second life we've shown up at dinners together, we've had conversations. I -- frankly Michael when I saw the choice, I was heartened. I think this is a serious man who takes these questions seriously and who's studied these questions. And so like I said, I'm heartened by the choice.

RAVICH: Jim.

QUESTION: hey, every time I put cyber financial warfare in a game theoretical context, I don't get very far. Looking back at the Cold War, you have sort of two rational actors and an escalatory ladder and if you blow up New York, we'll blow up Moscow, et cetera, and there were ways to avoid that by thinking through that step by step.

In the financial context, the problem is you have a great asymmetry of target sets. So if Putin shuts down the New York Stock Exchange, we shut down the Moscow Stock Exchange, but who cares because the market cap of the Moscow Stock Exchange…

HAYDEN: It's like my point about attacking united Russia.

QUESTION: …is irrelevant so we have to sort of go somewhere else. We also have multiple actors, maybe five or six major players instead of two, not all of whom are maybe rational.

So isn't that an almost insoluble problem in terms of putting it into a, as I say, game theoretical context as a way of working backwards to a solution?

HAYDEN: In our current state, yes. And that's why it just keeps coming and things seem to get worse. But we've been in this domain, what, 30 years? And I'm old enough to remember the Law of the Seas Conference back in the '70s where it took a decade to set down rules of the road for domain in which we've literally been operating in for millennia. And the thought, I don't want to be so pessimistic that let's wait a couple thousand years, we'll sort it out.

But again we just need to, as we were just suggesting, putting good minds on it, creating international norms, acceptable, unacceptable behavior, legitimate, not legitimate targets, again made far more complex by the low cost of entry.

By the multiple actors, by the non-state actors and so one thing -- two thoughts I'd give you, James. One is obvious, do not begin to transfer your thinking here over to here. You've really got to put it through a filter to decide whether or not it applies in the new domain. The second, I'm a historian by academic discipline and so I look for examples.

And then the best one I can come up with is 500 years ago, the European ages of discovery, the creation of empires, the great age of sail, the linking together of civilizations that had grown up autonomously and so on, gave us the greatest explosion in human learning, commercial development, scientific advance we'd ever seen up to that point.

It also gave us global epidemics, the global slave trade and global piracy. And it also was an era in which private actors seemed to act like sovereigns, Hudson Bay Company, East India Company and so on. There may be merit in studying that period and how that finally worked its way out. If you recall, piracy was put in its place, slavery was put in its place because the British Navy decided to do it.

QUESTION: Isn't an accidental launch in the meantime...

HAYDEN: I'm sorry?

QUESTION: An accidental launch, meaning that in terms of probing systems you actually set something off that you didn't intend.

HAYDEN: So -- so you bring up, and I'll try to be efficient here James, but you bring up one of the real dilemmas of the cyber domain and how thinking here doesn't work over here. So that in physical space, you do reconnaissance before you do the operation. You gotta know the target before you do it, you know, you know, Jeb Stuart's got to find the army of the Potomac before Robert E. Lee can do something about it, right?

In almost all cases in the physical domain, the reconnaissance, even though it might be real hard, is an easier task than dealing with the Army of the Potomac once you find it. In the cyber domain, it's the same. You've got to reccy in that before you can do anything to it. But in the cyber domain, and this is where it really gets troubling -- in the cyber domain, the reconnaissance is actually the more challenging task. The actual operational act, wipe the data, manipulate the data, destroy the data, steal the data. The operational act is actually a lesser included case of the reconnaissance, all right?

And so that in physical – in the industrial era, I've got a Soviet satellite overhead taking pictures of my ICBMs. Well, I don't like it, but I know that satellite's not going to destroy the ICBMs. In this era, I've got somebody in my power grid who may just be doing what intelligence services do, preparation of the battle space. But what's so troubling is that by doing that reconnaissance, he already has the ability to do something far more malicious.

And so, this -- it becomes the devil's own problem trying to sort this out because -- because we will not give up our right to do reconnaissance.

QUESTION: Caroline Vicini from the European Union.

Very interesting to listen to you, sir, and I recognize the whole story you are telling us here. And we certainly have had our differences on -- on privacy, but my question is -- is a different question. It's on the incoming administration. You mentioned Russia as one of the primary foes in this.

What about -- what we know about the incoming administration is that they want to take out ISIS. I mean, in a big way and we will see if that happens. But already ISIS have been pretty clever in social media, in -- and they have, apparently, access to people with sort of modern thinking in parallel to their very old-fashioned thinking in other fields.

What do you think about their capacities to go into cyber warfare if they are pressed out of their territory?

HAYDEN: So, the real answer is I don't know, all right? But that won't stop me. I'll -- I'll continue.

(LAUGHTER)

They are very cyber-smart and they do an awful lot of operational things in the cyber -- they recruit, they train, they direct, they proselytize, they fund-raise in the cyber domain. And so, I -- I've been saying this for years, but I don't know of a terrorist destructive cyber attack yet and I -- and I can't tell you why. I mean, I can speculate that it's not religiously pleasing destruction, it's somehow not manly destruction of a warrior -- I mean, they -- they complain about us with targeted killings as -- as being unworthy of a warrior because it's remote and so on, so may -- I don't know.

I'm making that up entirely, but they haven't done it and I can't explain why. One would think they would and -- and I take your point that as you squeeze the stateness of the movement down to zero, which is going to happen, these destructive energies are going to have to find expression somewhere else, so we could see it in -- in the cyber domain. And I would tell you, look, I mean we -- flash, we got cyber weapons too, all right?

And remember, I said we always had to have those meetings downtown? The single most prickly issue that took the longest to resolve whenever we would attempt to use an offensive cyber capacity was the question of collateral damage. It was in our mind the most difficult thing to convince a policy maker that no, we can do this. We can -- it will be proportional and it will be discriminate, all right? And so that actually kept us from doing things that were otherwise technologically feasible and maybe even policy-wise, right?

Now we've got an enemy who is indifferent to being discriminate and proportional. And so if this enemy were to choose to do things -- again, I don't know why they haven't -- it -- it could be very problematic for us. And -- and our power -- James, back to your how did this work. This is one domain in which a preponderance of offensive power doesn't seem to do anything for your defense. It doesn't translate into making you safer.

RAVICH: And then we'll go over to this side of the room.

QUESTION: Thank you Indira Lakshmanan from the Boston Globe. And you can -- and this is partly a part two to Michael's question.

You know, the national security adviser, we've heard, is going to be General Flynn and I'm curious because this sets up an administration where at least some people have not been worried about Russia or have been very positive towards Russia. You've talked a lot about Russian cyber attacks. The president-elect himself said that he did not believe U.S. intelligence agencies or trust their work, that they were not to be believed because of the mistakes made in Iraq and elsewhere.

So, I'm curious. Knowing that, what are your thoughts about an incoming President Trump who said that the cyber hacker of the DNC could be a 400-pound person sitting on his bed and having people who seem to be pro-Russia within the national security establishment?

HAYDEN: Yeah, so I've actually written about this and I've been very clear that that was particularly off-putting for me, given my background as an intelligence officer that you would disregard the judgment, not because you had contrarian evidence, but frankly -- and I don't think this is unfair -- because it didn't fit the macro narrative that you wanted to have, all right?

Look, this is the story of intelligence when it works, all right? We get stuff wrong, all right? But when intelligence works, we're the fact-based, empirical, inductive world as it is gang talking to the visionary, deductive, world as we want it to be gang. And so, you always have this -- this tension between intelligence and policy, all right? It really gets tough when the intelligence cuts -- cuts across the grain of the policy, all right?

And so, I guess what I'm trying to say is this is not an unknown problem. We -- we've been on this road before, but this is an important one. And in my judgment, American interests and Russian interests

are not convergent, all right? And -- and therefore -- and therefore, I hope the fact-based, world as it is, inductive guys lay out their case as clearly as possible to the incoming administration.

I also recognize that intelligence isn't the only input to legitimate decision making. There are other things a president can use to calibrate where he wants to go, but when it works -- when it works, intelligence isn't a syllogism that compels action. Intelligence does, though, create the left and the right hand boundaries of legitimate policy.

I hope that's what happens, but you raised the single most obvious issue during the campaign where I thought the positions taken by policy were at most variance with the world as I knew it to be.

RAVICH: And let me just add on -- on -- in the realm cyber and cyber-enabled economic warfare, I think the analytic tools are still being created for the fact-based folks because it's very difficult at this moment to do the kind of traditional cost/benefit analysis to present option A versus option B versus option C the way policy analysts usually do their recommendations up when it's still evolving, when we're creating new analytic methods to understand, well, what are the costs and what are the benefits if we take this action against an adversary who has engaged in a cyber attack upon us.

HAYDEN: And -- and to reinforce this, this is about the complexity of the cyber domain and maybe a comment on speed of government too, all right? So President Obama, after OPM I think, turned to Jim Clapper and said "you know, I'm a little tired of getting the DHS assessment, the DNI assessment, the NSA assessment. How about you do something to get me an agreed upon position here for cyber attacks?"

HAYDEN: And so they created...

RAVICH: CTIIC

HAYDEN: ... Yeah, Cyber Threat Intelligence Integration Center.

All right? It took longer to set up this two-dozen person office than it took the American Army to get from Normandy to the Elbe. I'm just saying.

RAVICH: And a lot, because they had to decide where to place it...

(LAUGHTER)

... where they had to place the office. That -- that was a big -- a big thing.

HAYDEN: And so, you know, it's just not the enormity of the cyber task and its complexity. There are -- there are elements of our governance here that aremaking this even harder than it should be.

RAVICH: Yeah. I feel badly. This side. Sir?

QUESTION: Elias Groll with Foreign Policy. Speaking of intelligence and a fact-based world view, the incoming CIA director is somebody who was deeply involved in the Benghazi investigation. And that was an investigation that was marked with a certain conspiratorial mindset. What do you think the implications are of somebody of that kind of mindset or outlook entering the CIA?

And before you answer that question, I want to ask part two of that -- that similar question. When it comes to Mike Flynn going -- coming into the administration as national security adviser, he's somebody who has flirted with Islamophobia and a wide range of controversial statements, which I'm sure you're familiar with.

As a veteran of the war on terror, what do you think the implications are of somebody of that type of mindset entering the White House? And what was your experience with General Flynn as a manager during your time in government?

HAYDEN: Yeah, I -- I didn't have a lot of contact with Mike in government. All right? I -- I maintained a little contact since I've been out and he's been in. Really bright, incredibly hard-working.

I do think most of his life experience has been at the tactical level where he has been incredibly successful in the fight – in the fight against terrorism. And so I think this job is going to -- is going to extend him. It's - it's going to demand that he up his game to be more broadly strategic than -- than just tactical.

I'd also offer you the view that my vision of the job, the national security adviser -- is less theologian and more process chief that -- that the job of the national security adviser is to make sure that the views of the government are harnessed and aggregated and presented to the president in a way that the president has the benefit of the full range of views.

And so that's also a function that's a little bit different than being Stan McChrystal's J2 and being remarkably successful every night for hundreds of nights. And so I do think that'll be an additional challenge for Mike as he goes forward.

With regard to the congressman, I understand the background with Benghazi. All I can tell you is in my conversations with him, I found him to be very well informed and very, very serious. And as I said, to Michael, when I first heard the choice, I go, "Yeah, that's OK."

I'd offer one additional view. All right? Not that the congressman has asked me any advice. All right? When you go to Langley for the first time, get out of the car alone. All right? Don't bring your own ecosystem. Go into the agency and embrace the agency.

(CROSSTALK)

QUESTION: Jim Prince, Democracy Council.

You mentioned about the tactic of shoving a lot of circumvention technology, anonymizers, VPNs into Russia. This has been tried with limited success in other areas, Iran being one target area, can you speak a little bit about the negative consequences of bad guys, lone wolves, criminal gangs using such technologies, tools and applications for nefarious things.

HAYDEN: Sure, so during the Arab awakening, it was American policy, to push as much of that as forward as possible into the Arab world, to protect people who were saying things that made us excited, from repressive regimes. And, I commented at the time, and we're doing that in the face of network anonymity, being the most serious issue we've faced in conducing adequate cyber defense.

I get it, all right. These -- these are -- these are going in different directions, but you know life is that way all the time. You know, privacy, security I want them both. I want them both in full measure; life doesn't let you do that. Life makes -- makes you trade. I think the same thing -- the same thing applies here as well.

It's a little bit like the apple story, all right. On balance, I think America is a safer place with the availability of unbreakable encryption, even though as a former director of NSA, that's not my perfect universe.

(LAUGHTER)

QUESTION: Hi sir. Megan Eckstein, with U.S. Naval Institute News.

I thought it was interesting that you framed the DNC hack as more of a Russia problem than a cyber problem. And, I was wondering with the President-elect expressing interest in improving diplomatic relations with Russia, do you think conditions are such that a better diplomatic relationship would result in fewer negative cyber behaviors or do you think that there are too many actors that play at this point where that may not help at this point?

HAYDEN: Well -- I mean -- if you believe the intelligence estimate that the Russians did this and they did this to mess with our head. I mean we didn't talk about it, I don't they were trying to pick a winner, I think just the erosion of confidence and their ability to go you see, these are the guys who preach at us, look at them. All right, I think that was enough for him to do it to. So, if some sort of relationship with the Russian Federation makes that less likely, that's good. It doesn't have to solve world hunger, just dampen this one aspect.

What troubles me is that the push for wouldn't it be great if we could get along with Russia, seems to be without condition. I've -- I've -- I've just -- I've just not seen anything in the rhetoric and to make that happen, this -- these are the things that we're going to have see. And, I just don't see that, and so I -- I am not enthusiastic so far about what I see as an agreed policy objective, yes it would be better, if we had better relationships with the Russian federation. But, to get there by suppressing legitimate American interests, is very off-putting to me.

RAVICH: I think we're going to take one or two more questions and then I'm going to grab the last question for my self.

Yeah, please.

QUESTION: Sean Carberry, Federal Computer Week.

And, a little bit bigger picture, you're talking about norms and challenges of defining this. The U.K. recently released their revised cyber strategy with a couple of notable differences from the way the U.S. is approaching it, in terms of their more centralized approach and also more of-- emphasis on retaliatory cyber capabilities and basically saying, they will respond in kind.

Can you sort of compare and contrast a little bit their strategy to U.S. strategy? Are there things that the U.S. should be adopting from theirs or are there things that are concerning about their strategy?

HAYDEN: So let me also throw in the Australian strategy, a recent product. In both of those other Anglo-Saxon democracies, there is a higher tolerance for state intervention than there is in the United States. I mean, the Snowden stuff -- I mean, got a little traction in Great Britain and Australian, nothing like it got traction here. These are -- we're friendly nations, we all come out of the same historic arc, but there are different political cultures.

So one distinction is a higher tolerance for a more robust state presence, even at the expense of some perceived loss of privacy, in order to get enhanced security. So that's one. Your question is more offensive action.

You know what? I don't know. But let me tell you something I have thought of. I would like to know more about what it is we're actually doing against the Islamic State. I mean, for the first time we've actually said we're playing ball. For the first time, we've actually said we're going after them.

I actually think as that becomes more public, we will learn more about the -- the value of response and retaliation and reduction of capacity, because right now, our deterrence theory in the cyber domain is based far more on resilience than it is on retaliation. And so now we're actually -- we've actually got a little petri dish going on here, as our -- we're actually trying to reduce the capacity of someone to operate in the cyber domain.

Before we did it, some people said that's not going to work, that's going to be whack-a-mole. Maybe not. So, I'd like to see it, and then that might inform my judgment to answer your ultimate question is -- so is going offense a better thing to do? My instincts, yes. But I'd like to have the data to demonstrate.

RAVICH: Last question from the audience?

QUESTION: Will Carter, CSIS.

There's been a lot of focus in the cyber debate -- there's been a lot of focus in the cyber the last few years on cyber physical attacks and threats of cyber action that have physical effects, but if you look at some of the most damaging impacts of cyber attacks that we have seen, it's been the theft of data, the dissemination of data, the partial dissemination of data. And in many ways, that -- that ties to your point that why haven't terrorists launched destructive attacks in cyberspace.

Maybe it's just not a very efficient way to blow things up or break things. And you know, as NSA director, you know about the infrastructure and human costs that go into effective cyber operations. Do you think that there has been maybe an over shift towards cyber physical as a concern? And do you think that...

HAYDEN: In terms of expressing concern?

QUESTION: Yeah, and maybe we should be focusing more on data and information warfare, which has arguably been more damaging so far?

HAYDEN: Thank you, that -- that's a great question. I'm just going to give you the points of light here, rather -- something coherent.

So what -- what -- when I wave my arms and talk about cyber danger, I don't quite get to the place where Mike McConnell and Leon Panetta get. I mean, Mike's -- well Leon, his last couple months as SECDEF was up on the Intrepid in the Hudson talking about digital Pearl Harbors and cyber Armageddons, and so I don't go there. In fact, my standard line when I do the long speech at the trade association is that the Chinese are turning out the lights on the eastern seaboard. It's not the first thing on thePDB, OK? That's a subset of something else.

And so I -- and so I don't need to go to the catastrophic physical attack. I think I'm agreeing with you, say we've got real problems over here. When I look at -- at cyber weapon creating effects in physical space, I can get Stuxnet and I can get the Ukrainian power grid and maybe a factory in Germany that was threatened and (inaudible), all right? I don't have it.

So this actually might be harder to do than -- than we think, OK? And so I don't -- again, I don't need to go there.

And then finally, people who know this far better than I, say do not confuse defending OT with defending IT. OT is and should be easier to defend. We shouldn't make it as hard as we seem to be making it. IT is harder, but defending operating technology, operating systems should -- should -- should be easier.

I mean, for example, a massive big data machine, creating an analog backup is not an option. It is on a whole bunch of things over here so that you can prevent stopgap, watertight door, catastrophic loss. I can't resist temptation to go into the world of science fiction and remind everybody about Battlestar Galactica. You know why the Galactica was the only starship in the fleet to survive, right? Because it hadn't been modernized. It was analog.

(LAUGHTER)

All the other ones were digital, and when the Cylons attacked, they all went down.

(LAUGHTER)

RAVICH: That's great. So...

HAYDEN: So, let me just finish.

RAVICH: Yeah.

HAYDEN: So -- so -- so that -- I guess three quick points. I don't need to go catastrophic to make this a real bad problem, so I don't. Second, the examples of physical destruction are limited, I wonder why that is. Third, protecting operating systems, we shouldn't think it's as difficult as protecting information technology.

RAVICH: So we only have two more minutes, so I want to ask the last question, kind of aligned to our discussion or maybe underpinning it.

So throughout your career, you have led small groups of people to very large organizations. You have recruited, you have selected, and so I turn over in my head, you know, what makes -- what makes a good cyber warrior? And how do we even begin to think about cyber teams?

And I'll just say on this, I remember doing a little bit of work on how do you even select for the appropriate cyber teams, and I thought, I'll go ask the Navy SEALs how they put people on teams. Not how they select, but how they put people on teams. Truth or not, I was told by height. And I said "excuse me?" And they said by height, because we all want to be of equal, you know, height because if we're carrying a boat above our head, we don't want the really tall guy and the really short guy.

(LAUGHTER)

OK, probably not a cyber analogy. But have you – you know because in this new world, we are going to need new types of warriors and also new ways to put them on teams. So final thoughts or -- or maybe another discussion.

HAYDEN: Probably legitimately another discussion, because I was back -- when this is embryonic, remember Joint Functional Component Command Net Warfare, I didn't have enough people put on a team, all right? In fact, the reason they're both at Fort Meade is that we didn't have enough people to get under the canoe to carry it. I mean we had to use the same people to do the exploitation that we would use to do the attack because the resource was so limited.

Now, we made great progress. I mean, under Keith and now Mike, we've got cyber teams being organized at 130 or something up there. They have reached initial operating capability. I mean, these are all good things going forward.

Now the trick is not just, to my thinking it is not just that small little group and how do you create the synergies within the team, but how do you integrate that team with the fire and movement of other friendly forces? That's a really interesting one.

RAVICH: That's right. So another discussion.

HAYDEN: Yeah

RAVICH: Well, I want to thank you so much for taking the time out of your morning and I want to thank you all for coming.

(APPLAUSE)

HAYDEN: Thank you.

END