FDD's Center on Sanctions and Illicit Finance
Securing American Interests: A New Era of Economic Power
February 6, 2017
Panel: Shoring up Our Defenses against Emerging Threats of Economic Warfare

JOHN CARLIN, Former Assistant Attorney General for National Security

ZACK COOPER, Board of Advisors Member, Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies

PETER HARRELL, Adjunct Senior Fellow, Center for a New Security

JONATHAN SCHANZER, Vice President of Research, Foundation for Defense of Democracies

JOANTHAN SCHANZER: I'd like to ask everyone to please take their seats. We're gonna get started with our next panel.

OK, the title of this panel is, "Shoring Up Our Defenses against Emerging Threats of Economic Warfare." My name is Jonathan Schanzer. I'm vice president at Foundation for Defense of Democracies and -- and I've been part of the CSIF team; honored to be part of it.

Look, the U.S. has spent the last two decades developing an economic warfare playbook. I played a small role in that as an intelligence analyst at Treasury, dealing with sanctions. But sanctions are the tip of the iceberg and we'll hear about those other tools throughout the day.

Our adversaries and enemies have learned. They're taking pages out of our playbook. We are looking at actions that would include sanctions, strategic investments, cyber activities, the use of alternative currencies, and even non-state boycott activities, as well.

The U.S. and its allies must now formulate defensive strategies to protect the U.S. and its allies. And just as we created an offensive architecture now, it's time for a defensive one too.

So we've got a terrific panel here this morning to talk about these issues.

We've got John Carlin. He's the former assistant attorney general for national security at the Department of Justice. And currently the chair of Morrison & Foerster's global risk and crisis management practice.

Welcome. Thank you for being here.

Zack Cooper is a member of CSIF's Board of Advisers. He's a fellow at CSIS, and a former White House staffer, reporting to someone named Juan Zarate.

(LAUGHTER)

And we also have Peter Harrell, who was a former deputy assistant secretary for counter-threat finance and sanctions at the State Department. And he is now an adjunct fellow at CNAS.

Welcome, everyone. Let's dive right in.

I think maybe, if I could just take a quick poll, a lightning round, up front, what were the top economic threats that you saw against the United States from your perch in the U.S. government? And perhaps maybe who were the top enemies? Maybe, just get started.

JOHN CARLIN: Yeah, so I -- I think I'll start there by focusing on what was a threat that was newly categorized -- or relatively newly categorized. And that's the theft of our intellectual property, of trade secrets, of trade negotiations, strategies on scale. And it's been categorized by the former head of the National Security Agency as the largest transfer of wealth in human history.

And that's the theft through cyber-enabled means targeting U.S. companies directed by military and intelligence services overseas.

And although we moved to address that threat, I don't think we've addressed it satisfactorily yet. And primary on the list of countries that engage in that activity would be China, but it's not China alone.

ZACK COOPER: Yeah, that's a -- that's a great concern, and another one related to China is some of the strategic investments they've made which have the potential to limit U.S. involvement in a military contingency in the western Pacific.

So something that doesn't get a lot of attention are Chinese investments -- business investments that are in most cases legal around U.S. military bases: Tinian, Saipan in the Commonwealth of the Northern Mariana Islands, as well as even on the continental United States; there have been issues on the West Coast, in particular, and in foreign countries, allies of the United States. One that got a lot of attention recently was the Port of Darwin in Australia.

And these Chinese investments, we don't know exactly what the purpose is, but you see time and time again that there are major strategic investments being made, often in dollar amounts that don't seem to make a lot of sense, around U.S. military bases.

And this is something that I think we haven't paid enough attention to. As a former Defense Department official you know, this is something you worry about but it's

not quite in the Defense Department lane. And so it can be difficult to figure out exactly who should be managing it.

So that's -- that's one that I would continue to look at.

PETER HARRELL: I'd just echo the -- the two comments already put on the table, I mean particularly, John's comment about the first.

You could -- you could really see when I started in government in 2009, the Obama administration, 2009, early 2010 -- you could see this was on the uptake. And really by 2012, 2013, it was completely out of control, the volume of cyber-enabled theft of our USIP, to the point, you know, as John said it was actually beginning -- is beginning to reach a macroeconomic level of risk.

And I think we, as a country, have begun to respond. But like John, I think there's quite a bit more to be done on that.

SCHANZER: So, Zack, let's talk about China for a minute.

You mentioned the strategic investments. I should probably note there are also reports of the Chinese investing in Hollywood, perhaps trying to manipulate the way that we even message about China in -- in the entertainment industry.

I think, obviously, defensive measures are required. What can we do to prevent these strategic investments?

COOPER: I think that's the big question. And one challenge here is that the Chinese make these investments in very different ways.

So we have a very -- a legalistic approach to how we manage sanctions, right? You know, many folks in the room have dealt with these challenges. And the Chinese approach this entirely differently.

So, let's take the case of a dispute between China and the Philippines that occurred in 2012 over Scarborough Shoal.

Well, what the Chinese do is they're not going to formally announce sanctions, but it happens that tropical fruit exports from the Philippines which are going to China suddenly end up sitting on shore in China and that they can't be sold, right?

So -- and there's no clear evidence about in that case, for example, that there wasn't something wrong with the shipment. But it just happens that all tropical fruit exports from the Philippines at this exact moment happen to, sort of, be cut off.

And so, I think one of the challenges is it's not just how we manage U.S./China relations on the economic side. It's also how we work with allies to manage them.

So, you know, one idea that I think some folks have talked about which would be potentially helpful with allies and partners is the idea of actually having a fund where when allies and partners are under pressure from the Chinese in this way, that the U.S. or others could step in and try and buy some of these goods.

Another area of concern that has -- has attracted a lot of attention was rare earth minerals. And this is another area where there's a lot of work that needs to be done defensively so that we limit our risk to Chinese coercion.

SCHANZER: Peter, lemme just ask you, we recently heard that China may have ordered quietly state-owned companies to boycott South -- South Korean businesses because Seoul allowed U.S. air defense -- defense systems to be installed.

Zack was obviously talking about this. What -- what do you think the U.S. response should be to these sorts of activities specifically?

HARRELL: I think this is another example of what Zack was just -- was just talking about. I mean, I heard from a couple of South Korean companies last fall, South Korean government officials, then later got in the press that, you know, their sense was the Chinese, not formally, you know, there are no sanctions on South Korea out of Beijing, but we're talking to some of their large SOEs, which are very large producers -- consumers of South Korean components for things they're manufacturing of, you know, maybe it's time to kind of ramp down our purchases and source elsewhere.

And this is actually tremendously impactful. It can be tremendously impactful given the scale of China as a -- as an economic center today. I think like Zack, we need to be thinking about some ways to, you know, either through trade or through, you know, kind of shared risk pool fund kind of things, mitigate this.

I also think we -- this is not a near-term solution, but over the mid-term, we need to be thinking through how we would signal and deter this kind of a strategy. You know, what kind of markers can we lay out about what is and isn't acceptable of China's use of this kind of sanction from -- from our perspective to begin deter them from doing it.

SCHANZER: John, when you were at the Department of Justice, you prosecuted a number of cases against cyber criminals, including Chinese, Russians, Iranians, responsible for attacks against U.S. institutions. How is the U.S. government's thinking about cyber attacks in its cooperation with the private sector, activities inside the government itself, how has that evolved?

CARLIN: Let me -- before I pivot to that question, I just wanted to follow up on one thing that -- that Zack said because I think one important area to look when playing defense against the possible exploitation of strategic investments is an obscure committee in Washington called the Committee on Foreign Investment Inside the United States. And this is one that came to public attention and the statute was strengthened after the Dubai ports issue.

Since then, though, rather than looking necessarily at areas of physical threat to national security, like supply chain to the Department of Defense or purchasing property right next to a military base under -- for suspicious reasons. What you're seeing is a different use of that committee and it's based on the change in the threat. And one thing I wonder as we shift administrations is how the new administration is gonna broaden its sense of national security to include economic security as a national security event.

President Obama already did that moving to your cyber as the basis for the first executive order of its kind regarding sanctions, which declared essentially that we're facing a national emergency -- a national security emergency because of the theft of economic information on scale. That was the basis for the first executive order that allowed for the use of sanctions against actors purely because of their cyber-enabled activities, including theft of intellectual property.

Is that same understanding of what the national security threat going to mean that when a foreign company attempts to acquire U.S. company and goes before this committee, the Committee on Foreign Investment in the United States, are they gonna block transactions and say they're blocking them for national security reasons, but it's because they think this is a purchase on scale that could affect national security?

And maybe at the time of the transaction, they acquired -- didn't have the intent to -- they're making it for purely business related reason, but because -- because in China, it's linked to a state-owned enterprise, they know that the government could exploit that purchase at a time of tension between the two countries. And so you need to mitigate that potential national security risk.

The advantage of that type of approach, I think, would be that it would send a message that if you -- if you want to be able to do business on the international stage, if you want to be able to profit, you're gonna need to demonstrate that you're not exploiting your economic investments for -- to affect the national security of other countries. And until you show that, we're going to view it as a national security risk.

That, I think, is a good segue to our change in approach on cyber which was based on that same all tools thinking, which is we need to follow what the intelligence shows the threat to be and then we need to work to disrupt it. And when it came to cyber, as someone who had been in government through multiple administrations, when I was a prosecutor prosecuting computer hacking cases, there was a squad that was doing the intel side that I worked with in the FBI, they're behind a literal locked, secured facility door.

And the whole time I did criminal cases, I never banged on that door to get in. Occasionally, an agent would switch squads and they just disappeared and I never saw them again, I didn't know what happened on the intel side.

When I went over to be chief of staff to FBI Director Mueller, I saw the intelligence side and what I saw was both an amazing intelligence feat but also

horrifying because we were able to map in real time with the help of the other intelligence agencies theft on scale. You could see in real time -- you'd watch Chinese actors hop into universities, hop into corporations and then you would watch the intellectual property flow out of the country. Billions and billions of dollars worth in theft.

So when I came back to the Justice Department to say hey, how are we applying the lessons we learned post-9/11 that led to the creation of my division of bringing down the wall between intelligence and law enforcement when it comes to cyber, and the answer was we weren't at that point. So we were still treating that as an intelligence problem, that it looked more like espionage than theft.

So the change that we started in 2012 was we retrained hundreds and hundreds of prosecutors across the country to become national security specialists, to learn on the one side the bits bytes Electronic Communications Privacy Act, Computer Fraud and Abuse Act. And the other side, get read in for the first time to that intelligence, have the highest level clearances so they can work together to disrupt.

The FBI issued an edict that said, "Thou shalt share what had formerly only been on the intelligence side of the House to all of their field offices," just like they do in terrorism cases. It's that change in approach that led to the first indictment of its kind, the indictment of five members of the People's Liberation Army, Unit 61398.

An important about using this approach, I think, is first it shows we can figure out who did it because if you don't make public that you can figure out who did it, I think a lot of enemies were -- our adversaries were wrongly assuming that we couldn't do it. Secondly, by making it public, it helps to educate the private sector and get their support in coming in to bolster this approach. And without their support, there's no way that we can bring these cases.

And in that case, we showed what's going on with China is not -- it's things like you're about to do a joint venture, and instead of paying for the lead pipe that you were going to lease to them, they steal the design specifications or for a solar company, they steal your pricing data -- these are both in the actual case -- and then use that to price dump, and then to add insult to injury, when that company sued, they stole the litigation strategy out from the company...

(LAUGHTER)

... through cyber-enabled means. So that's why we brought that case, that's why we changed approach to start trying to bring deterrence to the table.

SCHANZER: Zack, you -- you follow China, you follow cyber. What -- I mean, can you give us just a couple of pages out of this playbook, give us a sense of what -- I mean, what does China do day in and day out? We understand they're really probably the most active country in this regard. How are they doing this?

COOPER: Well, you know, as John said, Unit 61398 is one of the leaders in the Chinese system in pushing this kind of intelligence gathering activity.

I think one of the questions that many people on the outside who don't have access to the kind of intelligence that you see inside government often ask is exactly how connected is this to say, state-owned enterprises, right? How are the Chinese then using this intelligence that they gather and how direct are the connections between the intelligence gathering activities and say, private corporations or state-owned enterprises?

And that is one thing that many folks on the outside, especially in the China community, often raise questions about, is exactly who in Beijing is running these kinds of activities. So that -- that's one thing that I think there is a lot of interest in within the China community and I would expect that the new administration is going to spend a lot of time digging into this issue and they've made quite clear that on the U.S.-China economic relationship, that they're gonna put a lot of focus into making sure that it is a fair and balanced relationship. They've been quite consistent about that.

Now, one question is how -- how much the pressure that we've put on so far has been effective. You know, if you read a lot of the press, there's been I think a lot of optimism that perhaps leaders in Beijing have pulled back a bit after the indictments, that they did see this as a strong message that the U.S. was going to take some risk in this area, and in fact, that it was willing to put real pressure on China to pull back some of these coercive economic activities.

Now, whether that continues, especially if U.S.-China economic relationship gets more tense, I don't know. That's -- that's going to be one big question.

SCHANZER: Peter, you recently left the U.S. government, working in -- in the field of sanctions, working at the State Department. I think most people think about the -- the work that you did as being sort of offensive, right? It's about targeting bad actors in the -- in the -- around the world, whether it be for proliferation or for terrorism.

Has there been any real thought? Is there a doctrine about defense? Is there -- is there infrastructure right now in the U.S. government that can be deployed for defensive measures, as opposed to only going on offense as traditionally conceived?

HARRELL: Well, let me -- let me first actually say I'm sorry if my voice is a little scratchy. In addition to getting over a head cold, I'm from Atlanta, so this whole morning's just been kind of -- kind of rough at many -- many levels.

(LAUGHTER)

But to get -- to get to your question -- and I should actually say, I think this is an incredibly important area and I'd actually give you, and frankly, a number of your colleagues, Mark and Juan who I see right here among others, credit for beginning to

nudge, you know, probably about 18 months go the U.S. government begin thinking about this.

And its great to see in the report, some more systematic thinking about exactly this issue because -- because frankly, to date, the internal U.S. government thinking on this has been pretty limited. I mean, I can give a couple of specific examples where the U.S. government did think through defensive side. You know, when we were designing the Russia sanctions, for example, there was obviously some sense Russia might retaliate in different kinds of ways.

And so there was kind of ad hoc thinking about what U.S. companies would have exposure, not only to what we in the European Union are doing affirmatively, but also are there are other U.S. or allied companies the Russians could retaliate against so that we could at least think through how to defend that.

But -- and then -- and then, you know, as we've been discussing, when you -- when it gets to China and sort of dealing with the -- the range of economic threats we're facing from China, that we're sort of thinking about how do we approach it on a cyber front through prosecution, through sanctions, through presidential jawboning, you know, and other -- other kinds of tools you have at your disposal.

But there really hasn't, within the U.S. government, been any systematic evaluation of vulnerabilities either of us or of our close allies and thinking through, you know, in a more systematic way, how do we wanna be positioned to play defense for the long-term.

So you know, as I say, episodic instances of defensive thinking, but nothing systematic, and that's why I really think it is great to see FDD take this issue on, you know, as I said, for the last 18 months but really now going forward in a robust way.

SCHANZER: You know, we -- we certainly have them thinking about this and -- and I think looking for bureaucratic fixes is not necessarily an easy thing. Bureaucracy is sort of a -- I'm not even sure if it's a tamable beast.

What I can say is that we have thought a little bit about maybe some mechanisms within the U.S. government. For example, one idea that we've been kicking around at -- at FDD is this idea of within the Commerce Department, with the Bureau of Industry and Security, there's an Office of Anti-Boycott Compliance. It's called OAC. It's really not a terrible active arm of the U.S. government right now. It -- originally just designed to tackle the Arab boycott of Israel.

The thinking is perhaps that we could broaden that out and perhaps give it a little bit more of a robust mandate, that perhaps it could start to look into China's actions against some of its neighbors, looking at Russia's responses to some of our allies.

And so this is something to think about, but I -- I would actually pose to you, if you have any thoughts about other areas of the bureaucracy that we might be able to

strengthen, and I'll maybe ask each of you to go down the line, think about ways where we could actually change the way that the U.S. government approaches this element of illicit finance, to think about defense.

How would you -- how would you start, Peter, if you had an opportunity?

HARRELL: I -- I'd begin by saying -- I mean, as everyone around the room -- and I see so many of you have been in government -- knows when you're in government, you're dominated by the tyranny of the inbox. So it -- gives me a perspective of if the U.S. government is going to think defensively, somebody has to be assigned the job of thinking defensively, because otherwise, reality is it'll also be, you know, issue number nine on somebody's 10-issue to-do list.

So you know, whether it is something like you suggest over at BIS, broadening out the -- the Office Anti-Boycott Compliance or thinking of Treasury, you could picture, I think, in the TFI under secretary world, you know, get a new TFI under secretary in there. Some -- you know, it doesn't have to be huge to start, but you know, couple of people to begin to think through strategically the defensive issues I think would be another area.

And then the third area, and I've seen it kind of marshal resources in the past. You know, for the new -- once Dan Coats gets in as director of national intelligence to -- to order up a national intelligence estimate on this. I mean, those are long-term projects. They're not overnight, they're complicated, but they do actually kind of force people to think about these things over the course of the year that you develop an NIE.

And so I wouldn't -- I wouldn't undervalue that as another way to move this issue forward in the U.S. government.

COOPER: Agree with everything that Peter just said.

The -- the one point that I'd add is that I think this has to have some home in the White House. Certainly, when we thought about this with the Soviets, you had a point person in the White House who is responsible for coordinating among the departments and agencies, and so you have to get back to that.

Now, perhaps the good thing is that there is going to be more interest on these kinds of issues from the new team. They've written publicly about their concern on economic coercion. So I don't know whether that home would be some person in the National Trade Council, the National Security Council. But I think you have to have some locus in -- in the White House that is going to take this and push on it.

You know, just one example of why this is important is that there are people at the U.S. Pacific Command that have been paying a lot of attention to this issue. But they have no place to go in the current bureaucracy to help them figure out how to use economic tools to respond to this kind of coercive activity in a defensive way. They need to be able to go to someone or to a group of people that can help them come up with

responses because they're watching the threats come in and they don't know right now who to go to.

CARLIN: I'm gonna move a little bit to -- to cyber and the threats that are posed to our economic security there. But I think we're at a crisis point, and we've been there for a while, where there -- there's no excuse not to know that the system is blinking red when it comes to the potential for a major national security-driven cyber incident to hit our critical infrastructure in a way that causes major economic issues.

And we've had this dating back now nearly five years. The September 11th Commission issue another -- 9/11 Commission issue another report saying that cyber, in some respects, is like we were with terrorism prior to September 11th. And since then, each year, we say this is the year that the -- we see the canary in the coal mine, whether it's North Korean attacks on Sony or the more recent Russia systematic campaign to undermine confidence in the integrity of our election or the use of an Internet of Things botnet disruption to take the internet down for nearly a day.

So when -- in terms of waking up then, two things that are urgent to address that threat. One is -- and this is where offense and defense meet -- we have to have an effective deterrence strategy that crosses different departments and agencies, that uses Commerce's authority to designate entities as ones who do harm to the national security, that uses Treasury Department's ability to sanction, the use of Justice's ability to bring criminal indictments, that has the full employment of military response -- responses at its -- at its disposal and State Department diplomacy.

And then we need to advertise where our red lines are so that people know we're determined to use this deterrence apparatus.

The second would be we're not where we need to be in terms of having defense -- defensive investments. And by that, I don't mean a product that keeps the adversary out because the product doesn't exist, so there is no product that can keep a dedicated nation-state out of your system if they're determined to cause damage.

So that means having a fundamental re-calculus of risk both in our private sector and government as to what it is we're putting onto a medium that was not designed fundamentally with security in mind. So we make it digital and then we connect it to the internet. It's not designed for security. What should be on there? And then secondly, how resilient are we? Because we know if they want to, they could impose malware that could disrupt those systems. So how resilient are we at getting back to whatever the product is that you want to get out?

And so in order to incentivize that, that is going to take, I think, leadership from the White House driving through the National Security Council with a sense of urgency across each department and agency. And as critical as that issue is now, we're on the cusp of another evolutionary transformation. So as radical as it was to our society when for instance we went from a horse and buggy to an automated car, we're in the midst of another transformation where we're going from a car with a driver to a driver-less car.

And make no mistake, that's gonna have a huge effect. What we're -- and that's just in the automobile industry. That's the so-called move to the Internet of Things. As we do that, we can't make the same mistake of underestimating risk again and we have to build security by design in before the drones in the sky, the pacemakers in our hearts and the cars on our roads are all connected to the internet in an insecure way.

SCHANZER: Well -- but -- I'm gonna move to Q&A, but just want to flag for everyone that the FDD has a project on cyber-enabled economic warfare led by Samantha Ravich and Juan Zarate and Mark Dubowitz and we're gonna -- we're gonna be looking into that more deeply some of the issues that you just touched on, so stay tuned.

I do want to open this to Q&A now. Please wait for the microphone, you raise your hand, I'll call on you, and then we -- just please identify yourself. Try to keep your questions short. We've got about ten, maybe fifteen minutes to do this, so let's get started. I'm not sure where the mics are, but let's take right here in the front.

QUESTION: Joe Pinder with the Financial Services Committee.

John, you talked a little bit about CFIUS. One of the things that I think that we're -- we need to recognize is that however well-formed our foreign investment screening process is, it's not very well formed at all or unified in a lot of our -- even our western European countries. I think we need to figure out a way to do outreach on that to bring them up to the same sorts of levels that we're aiming at.

I wondered if you any of you have thoughts on that?

CARLIN: I think that's a great -- it's point, and a couple things.

One is, the secrecy that rightly surrounds CFIUS makes it hard to discuss it openly as a policy tool and explain how you're using it to define national security threat and how you're not. So, I wonder if there's work that the committee can do there so that there can be a more transparent discussion, and that might help in terms of incentivizing behavior as people try to avoid having transactions stopped through CFIUS.

Secondly, CFIUS right now is a pretty blunt tool, so if it triggers, for those who aren't as familiar with it, it means essentially the president can block a transaction. There are -- any transaction where there's a foreign acquirer that poses a national security risk. On the other hand, if you structure your deal differently, it may not fall within the scope of CFIUS at all.

And I know with some of our foreign partners -- so it may still pose a national security risk, but the risk isn't posed because of a foreign acquirer. I know some of our foreign partners overseas, they have had questions about when it's on and when it's off. Might be another area to address.

COOPER: Just one thing to add here, you know, a little vignette of the challenge that our allies and partners face on CFIUS-like investment groups is take the Australia Darwin Port deal , which I mentioned earlier. So when it was announced that a Chinese firm was going to buy a very large stake in the port of Darwin where the U.S. is now doing a lot of military activities, there actually happened to be a U.S.-Australia two-plus-two going on. So SECDEF, SecState along with their counterparts in the Australian government.

They were meeting, I think, in Canberra. That announcement happened while they were meeting and no one that was there knew it was happening in the Australian government. So the way the U.S. found out was by reading the newspapers afterwards, which lead to a fair amount of concern about whether the alliance was paying enough attention to this kind of issue.

And so certainly, we have problems in our government on these issues. I think a lot of our allies and partners have thought even less about some of these challenges. So we're going to have to work these into those relationships. We've done a little bit of work with the Japanese who are obviously having to force themselves to think about this a little bit more.

But it's going to have to be part of the discussions with allies and partners, you know, not just in these major -- when you have a major purchase that you're watching, but every day to get us to the point that we actually are working together to watch these kinds of strategic investments.

HARRELL: I understand -- very short two thoughts on that.

First, I mean, I very much agree with you, this is an area we could work better as the U.S. government with our allies and partners. I might actually think this is something that you could -- you could even -- I don't want to overstate their value, but you could get the G7 to think about, right? As -- as a core group of very politically like-minded and economically like-minded countries that are, you know, I think frankly facing some of these same issues.

We've -- we actually have coordinated Russia sanctions, a few other things through the G7 over the last couple of years, and that might be an area where you could think not just about sort of, you know, individual deals and how do we respond to some individual deal collectively, but more structurally how to respond.

The other thing, and I -- I -- I say this with great trepidation because I -- I very rarely find myself disagreeing with John, but one area where I disagree very slightly with John is that, although at one level CFIUS is a blunt instrument, when it gets up to the president's level, he can either approve or reject a transaction. One of the things I think we need to do a better job of explaining to our allies about CFIUS is that for most deals, it is not that blunt.

Actually, what happens, companies come into the process, they -- and because it's not transparent, it's not fully transparent, but the companies can think about ways to mitigate. You know, they can spin-off a part of the deal, they could make sure it's independently managed U.S.-born -- independent U.S. board of directors that manage .

So I actually think there's some things we can explain that would make it more appealing to our allies than it -- sometimes is misperceived currently by some of our allies.

SCHANZER: OK. We've got other questions. I'll take you sir, right there.

QUESTION: Good morning. Dan Wachtler with Root9B.

John, question for you I'd just like you to comment on. I just read an article over the weekend coming out in the latest issue of the Journal of Law and Cyber Warfare. It opened my eyes a bit on the -- one of the challenges in the private sector, about the victim, meaning the company that had the advanced persistent threat and them being -- then looking like the bad element in public.

And so when you think about really the victim being put in that position, when there's no way they can compete against a sophisticated adversary, can you comment on any policy changes that we may see or need to address along those lines?

CARLIN: That's critical. We -- we have to figure out a way to stop -- to both incentivize people to have better defensive practices, but stop blaming the victim. You know, I don't want to make a direct analogy cause it's serious and different, but I started my career prosecuting domestic violence cases. It was an area of law-enforcement where we knew, we couldn't stop this from occurring unless we got the cooperation from the victims and we had to look at our system very hard and figure out what was dissuading people from coming forward and how can we change it.

And again, I don't want to make a direct analogy, but when it comes to cyber, we have a similar phenomenon in that even companies are worried if they come forward, it's gonna cause more loss than it would if they kept it private. And so what we're seeing is on scale, almost every company in the Fortune 1,000 has been hit with a cyber intrusion. You've had multiple FBI directors and director of international intelligence say that.

They haven't all come forward and discussed what they are and we're not gonna be able to tackle it together until we reach that point. I think that means taking a look at what are the carrots and sticks and is there some free pass that you can get, if it requires high-level approval, let's say attorney general blessing that say you did what was sufficient on the defensive side and the real issue here is going after the bad guy. You're not that guy, Sony. And that was -- us going public I think helped change that dynamic. The bad guy's North Korea.

And by the way, as soon as we said publicly that it was North Korea that had attacked Sony because a movie about a bunch of pot smokers, the whole narrative inside the country and media coverage changed. Instead of saying what did Sony do wrong, it became government, why aren't you doing more to protect companies from bad actors like North Korea? And that pressure should be -- I'm still saying us something us -- on us in government -- on them in government now if we want this to work effectively

SCHANZER: I wanna call on Samantha Ravich from FDD's project on cyber-enabled economic warfare.

RAVICH: Great, thanks.

Just a comment that I'd love to hear your thoughts on. John, it was particularly taken when you referenced that the 9/11 commission is again, kind of raising this specter and saying, look, we may not again be connecting the dots as to what's happening. And that's one of the things we're trying to focus on in the -- in the work on cyber-enabled economic warfare is to understand the potential adversarial campaign, right, that is behind this.

That's it's not a series of one-offs. That's it's not that China is doing this over here and this over here and it's just one plus one, plus one, equaling one plus one, plus one. That there is a campaign behind it, potentially from China and other adversarial state and non-state actors to undermine our economy in order to undermine our ability to project power and defend ourselves.

So, the comment is, when we look at this potential weakness or failure of the government -- of our government right now, not to connect the dots. I see it in at least three capacities. One, these bits and pieces; how do we understand them as part of the campaign? The second is how do we -- how do you or -- or those in, transmit that information to all the cyber operators that are currently operating as part of the U.S. government? All right, there's a whole host of them. How are they understanding the playing field so that they can operate on it both offensively and defensively?

And then the third piece is when we take an action, either offensively or defensively, how is the adversary perceiving this? Because, I think Peter, you had mentioned and -- and Zack as well, the concept of deterrence. Well if we don't really understand how the adversary's perceiving our actions, are they being deterred by them? Are they even noticing them? Or is it actually ramping them up their escalatory ladder?

So I mean, you know, that those are three at least pieces that we're trying to help connect the dots or at least think through the analysis and collections to do so, but I know there's a lot more and you guys are right in the midst of it. So any comments you have on that will be greatly appreciated. Thanks.

HARRELL: Well, let me just start with what you brought up at the end about, sort of the complexity of signaling, you know, deterrence strategy. And I think it's

certainly true, you know, that we've thought about -- when the Obama administration thought about how to deter some of the Chinese enabled -- Chinese cyber-enabled theft, you know there was a lot of thinking about what's the message we're gonna send to China?

And there was actually a lot of private dialogue with the Chinese rule, we tried to make as clear as possible to them I think, what our redlines were -- not all of which were stated publicly obviously. But you -- you clearly need to have that for deterrence to work. We do need some method of communication in a robust way with them and so I mean, as I've said I think it is very important we have a deterrent strategy here.

I do think we can't just stumble into that. That is something we need to think very carefully and we need to think through how we would message that both, privately and publicly. And also, how, you know you do have this problem of attribution which you bring up as well.

And I mean often times these attacks are actually a little bit hard to attribute and you do have to work that through as well when you're thinking about your deterrence strategy.

COOPER: I see this, you know, especially as regards China as an extension of what you see from China in a lot of different areas. So people often talk about Chinese gray zone activity, so what they mean is, activity that is not crossing the threshold to war, but still above the threshold that we think of as fully peaceful.

And what we see from the Chinese, in those areas, is that they consistently used ambiguity, asymmetry and incrementalism to gain advantage over the United States, right? So the United States might have greater capability in one area, but there using those three elements to weaken our ability to respond. And so what deterrence requires, theoretically, is clear, credible commitments and signaling about our capabilities.

And so I think the good thing is, we do have substantial capabilities that we've talked about. The bad part is that we probably haven't been communicating our redlines as clearly as we need to. Now that's tough because when you communicate those redlines, you have to be willing to enforce them. So you need to draw them in places that you're willing to take substantial risk over. But I think that's what's required if we're going to reestablish deterrence.

SCHANZER: Can we say redlines again? You know, let me -- actually we've got about a minute or so left and I think maybe this is just a -- we can do a lightning round, have you guys respond very quickly.

But the idea of having deterrence I think, also rests -- at least to some extent, on our ability to work with allies. Are trade agreements part of the picture here, do we need some sort of a NATO against cyber attacks or other forms of economic warfare.

How -- when we think about America's role in world, how does this fit in? Maybe just give a 30 second answer before we -- before we close.

HARRELL: Great question. I mean and I think that -- that -- I'll sort of leave with it, I think it is an open questions in some ways. Particularly, as we have a new administration that is coming in, rethinking a bunch of things, but including things like trade agreements and, you know, the kinds of agreements that, for some years now we would ordinarily have turned to as a piece of the solution on this, right?

I mean, if you're were thinking about how to help allies affected by sanctions, you know, a couple years ago I'd say, well, you try and work out some trade agreements where maybe even have some preferential access something, that's probably off the table now.

So I think we do need to think through what is our toolkit? We have plenty of tools, we'll come up with, but we do need very carefully what is our toolkit.

COOPER: Just one thought on this is, one issue that doesn't get a lot of attention, especially when we talk about cyber, is Article Five commitments. And this has come up in the NATO context, but it's increasingly coming up in the context of Asia as well, where, you know, the U.S. has Article Five commitments, and whether some cyber attacks in certain circumstances might trigger an Article Five commitment, I think is a really tough question. But it's something we need to look into.

And when we talk about deterrence and allies and partners, that's got to be part of it. When do we actually cross a redline that requires a U.S. or allied response and reaction to this kind of offensive attack.

CARLIN: I'll just say, we're working with our allies as well, it's important -- a lot of times our response to a cyber enabled incident has been seen through a bilateral lens. So if it's -- if it's China stealing economic information, then it's a China problem. Or if it's Russia undermining confidence in the integrity of the election, Russia or Iran attacking our financial system through denial of service attacks as they did, then that -- we need to think about our Iranian issue.

And we've had terrorist groups, as well, steal information from private sector to try to create kill lists. If we're gonna have a multilateral response working with countries around the world who say cyber in some respects, is the wild West, we don't want it to be, so we need to agree on what the -- what the laws of the road should be going forward.

That was a successful part of China, where the solution wasn't China focused, it was President Xi saying, we're not gonna use our services to steal economic information for the benefit of private companies, then the G20 adopting that. And now of course we need to make sure people live by that -- by that commitment.

I think right now we've fallen into the bilateral trap a few too many times and we need to think about each incident, not just in terms of what the affect will be on that particular country, but for all the other countries and non-state actors who are wondering what are the rules of the road? What can I get away with? What's going to cause a response?

SCHANZER: We're going to leave it there. I want to thank John Carlin, Zack Cooper, Peter Harrell. It's been a terrific panel. Let's give a round of applause. Thank you guys.