Cyber-Enabled Economic Warfare: Welcome Remarks and The Rising Global Cyber Threat

Remarks by Dr. Samantha F. Ravich, Principal Investigator, FDD's project on Cyber-Enabled Economic Warfare; Vice Chair, President's Intelligence Advisory Board, followed by a panel discussion featuring John P. Carlin, former Assistant Attorney General for National Security at the U.S. Department of Justice, Juan C. Zarate, Chairman and Senior Counselor, FDD's Center on Sanctions and Illicit Finance; former Deputy National Security Advisor

RAVICH: Welcome. I think we're all taking our seats now, except for me, I'm standing. My name is Samantha Ravich and I am the Principal Investigator on the Cyber-Enabled Economic Warfare project here at the Foundation for Defense of Democracies, a non-partisan research institute focusing on national security and foreign policy, organized in the immediate aftermath of the 9/11 attacks.

Before we begin, I'd like to take a moment to honor our veterans, members of the armed force -- armed services, law enforcement and public servants. Our nation thanks you for your dedication and service to our country. You defend our nation and our ideals, and in the cyber realm you are increasingly joined on the battlefield by the private sector, as we'll discuss today.

I would like to welcome and acknowledge our distinguished audience of foreign policy and national security professionals. We are privileged to have with us ambassadors, cyber and defense attaches and other senior diplomatic officers from more than 20 nations, as well as officials from the White House and the Departments of Defense, Energy, Commerce, Justice, Treasury and State.

We welcome members of the Intelligence community as well as congressional staff. We'd also like to acknowledge the many members of the press, both domestic and international, here with us today. Welcome, also, to the audience joining us via live stream.

We're pleased to be joined today by members of FDD's National Security Network. I've had the privilege of traveling on a few of the NSN overseas trips and speaking at events with this cohort. This next generation of National Security practitioners gives me great confidence in the country's future. We're also delighted to welcome several members of the Cyber-Enabled Economic Warfare Advisor Group. Your insights have helped shape our work over these past few years.

I'm pleased, also, to welcome fellow members of the Board of Advisors for FDD's Center on Sanctions and Illicit Finance. It is a pleasure serving with you all.

After the conference we will be circulating a survey, via e-mail, to help us understand the perceptions of the threats from cyber-enabled economic warfare. We ran a similar survey a few years ago at the outset of our work, and it will be interesting to see if and how perceptions of the threat has changed. The results will be anonymous and I hope you all will be willing to participate.

So as we get started, I want you to keep three things in mind during today's conversations. And I know it's -- it's not an easy feat with everything that is going on in our personal lives, and our

country and the world, but important enough that for today I don't feel bad about asking you to do this.

So the first thing is the recognition of the critical role that American inventions and innovations have played in the prosperity and security of our country since the birth of our nation. George Washington so recognized the importance of encouraging the advancement and protection of inventions that he called for the passing of the Patent Act as his -- in his first State of the Union Address.

And in fact, there were 150 patents issued during his presidency, and each was signed and sealed by President Washington himself. Over the next two centuries American inventors, such as Samuel Morse, developed the telegraph -- patent number 1,647 for those of you who are counting, and the Wright brothers flew the first controlled flight of a power-driven airplane -- patent number 821,393.

Ponder for a moment on the transistor, the key active component in practically all modern electronics, developed by William Shockley at Bell Labs. Consider the personal computer, the internet, GPS.

All right, now second, think about what would have happened if those inventions had never come to be, because the inventors themselves could not profit from their hard work and so decided not even to bother, or if those inventions had been stolen by our adversaries before they could give our country their full benefit.

World War I may have come to a different conclusion if General Pershing never had the air advantage. And if Andrew Higgins' boat design, protecting the propeller from grounding -- patent number 422,146 -- had been stolen by the Axis Powers, Normandy may not have been possible and the tide of World War II may never had turned in our favor.

And now, third, think about the critical inventions and innovations today that are being killed in the cradle or stolen to be used against our prosperity and security. All right, you all may have heard about the recent Micron case and our panelists may speak about it more today, but briefly, the Boise, Idaho based Micron provides approximately 20 to 25 percent of the world's supply of dynamic random access memory integrated circuits -- alright?

The company has invested billions of dollars over the years to develop its intellectual property. And since at least the fall of 2015, a Chinese state-owned company has been stealing its trade secrets through cyber and non-cyber means, most likely looking to counterfeit the technology and flood the market with cheap substitutions, severely impacting the health and welfare of Micron going forward, and by extension, the security of our personal computers, workstations and servers.

Think about the effect on our security and prosperity, if a critical component of our wired world was powered by a Chinese state-owned entity. When the U.S. Commerce Department added Fujian Jinhua Integrated Circuit Company to the entity list at the end of last month for its theft from Micron, Commerce Secretary Wilbur Ross quite rightly stated that, "when a foreign company engages in activity contrary to our national security interest, we will take strong actions to protect our national security."

So, the actions to protect Micron and punish Fujian Jinhua were long overdue. But in some ways, that particular horse had already left that stable carrying billions of dollars in revenue and military vulnerabilities on its back.

To protect our national security industrial base going forward, the U.S. government and our population at large needs to understand that there are adversaries out there who know that our greatest strength is our ability to create and innovate, and own the fruits of our labor because the business of America is truly business. We are the number one military in the world because we are the number one economy.

So our work here on cyber-enabled economic warfare helps in this mission by shining a light on the strategy on of our adversaries to undermine our prosperity, and thus, our security.

We have entered a frightening new world. Where not only a country like China or Russia can cause massive harm to our economy, but so could Iran and North Korea. Two countries with a combined GDP of less than 1/10th per capita the GDP of North Dakota, right, but all the cyber capabilities of a super power.

So with that statistic now rattling around in your head, I want to welcome Juan Zarate and -- and John Carlin to the stage.

Juan Zarate serves as Chairman and Senior Counselor of FDD's Center on Sanctions and Illicit Finance. It is his fault that I joined CSIF's board more than four years ago and I thank him every day for that vision and his thought leadership on future threats and opportunities facing our nation. And as many of you know, John Carlin served as assistant attorney general for national security and is an adviser to our Cyber-Enabled Economic Warfare project. John has a new book out, "Dawn of the Code War: America's Battle Against Russia, China and the Rising Global Cyber Threat." I cannot recommend it more highly. If you have not already picked up a copy, we have books for sale at the registration. And with that, let me thank you all for being here and hand it over to Juan. Juan, Thank you.

ZARATE: Thank you, Sam.

(APPLAUSE)

Good morning, everybody, I hope everyone is doing well. First of all, Sam, I want to thank you and Cliff and FDD for hosting this conference. I want to thank you for your leadership on, in essence, pioneering this space, the space of exploring what cyber economic -- cyber-enabled economic warfare actually means, how it's playing out, how it dovetails with our concerns on cybersecurity, supply chain security and all the other issues that relate to our core national security interests. And so, Sam has really been at the forefront of this, and I want to thank her and FDD for your leadership in pioneering this -- this thought -- thought domain.

There's nobody better actually to kick off this conference -- this inaugural conference on CEEW, as we call it, than John Carlin. As Sam mentioned, John has just come out with his book, "Dawn of

the Code War: America's Battle Against Russia, China and Rising Global Cyber Threat." Aside from being an incredibly insightful book, very detailed -- incredibly detailed, it has probably the best title I've heard in a while. It's a blend of "Planet of the Apes" meets "Star Wars." "Dawn of the Code War." So -- but I saw it at Barnes & Noble yesterday, it looked like it was selling well, John, so congratulations.
CARLIN: Thanks, Juan.

ZARATE: As you know from John's bio, he's had a leading role in the law enforcement and policy space, both as chief of staff at the FBI as well as assistant attorney general for the national security division, where he really did pioneer and -- and focused on cybersecurity threats, in particular from a law enforcement perspective. And the book details all of the cases and investigations that John was a critical part of and the FBI has been -- and the National Security Complex, has been a part of.

John is now writer and commentator, he's also written other -- other works. I use a law review article of his in my Harvard Law School course, which talks about law enforcement and deterrence in the cyber domain. He's also now a practitioner at Morrison and Foerster. So, we're really lucky to have John with us talk about these issues. John, welcome.

CARLIN: Thank you, Juan.

ZARATE: Let's start first with kind of your view of the scope and evolution of the cybersecurity problem and our vulnerabilities. You have been a part of the national security -- sort of community -- for a long time looking at these issues, prosecuting these cases. How do you describe the evolution in terms of the actors, the vulnerabilities, the capabilities in this space?

CARLIN: Well, you really look back and there's been a significant change both in what the threat actors are doing and our response to it. And so when I was a prosecutor prosecuting computer hacking and intellectual property cases, a so-called “CHIP”, which is one of the worst -- worst ideas that Former Director Mueller had -- but the name came back when he was running the prosecutor's office in San Francisco. I worked with an FBI squad; great squad, and we worked on the criminal side of the House. There was another squad behind a locked, secure, compartmented door and they were dealing with intelligence threats.

The whole time I was working those cases, I never knew what was happening on the other side of that door. In fact, an agent would occasionally switch squads and they just disappeared never to be seen again, we didn't know what happened. When I went over, I ended up coordinating that program criminally nationwide for the Justice Department and still it was -- the focus was on criminal actors. When I went over to the FBI to be then -- now director of the FBI, Bob Mueller and relatively anonymous compared to his current role, the door opened.

And for the first time I could see what was happening on the intelligence side of House and amazing work had been done at starting to map the threat and we could watch -- there was a JumboTron screen actually, size of a movie theater -- we could watch in real time as nation-state actors, particularly China, attacked places like universities, then would hop from the university into private companies and we would see billions and billions of dollars' worth of intellectual property, trade secrets and trade negotiation strategies flow out of the United States. It's watching that that

led the former head of the National Security Agency, Keith Alexander, to call it the largest transfer of wealth in human history.

That was focused on -- on transferring wealth, making money, had an economic motive. I think what we've seen since then, in addition to that type of dollar-focused theft, is the growth of destructive attacks and the use of cyber -- the cyber domain as a tool of coercion. One of the things you track through the book is how in the beginning, there were some amazing work done at -- for incidents that looked like they might be the result of a nation-state, and there was some early nation-state activity, but often they ended up being, you know, the caricature of a teenager in the basement.

You know, they weren't the world's most sophisticated actor once we got to the end of the line and figured out who did it. I mean, that's similar to, I don't know how many of you are familiar with the so-called Mirai Botnet; this was just a year and a half ago, and what happened is, the group figured out with these new Internet of Things connected devices -- so devices and billions and billions of new ones are being added to the Internet each day using the same insecure protocol that we've been using for years with digital communications, but now it's our baby monitors, it's toasters, it's refrigerators, their default being rolled out, sold and they're not secure by design.

And so what happened is, some young Canadians, basically kids, as a prank, really had to do with gaming, decided to create what's called a botnet. So that's essentially a cyber weapon of mass distraction. They release code, compromise, sometimes millions of devices and what they do is they set up one command and control node so with a single command, you can direct this army of compromised computers.

And for their purposes, which had to do with some gaming dispute, they launched this cyber weapon of mass destruction and it took down part of the Internet. It took down the -- that we're relying on now, it's not e-commerce anymore, right, it's commerce. So when you disrupt the backbone of the Internet, you're affecting lives, you're affecting commerce, you're affecting economies. So that's what kids can do now.

And what we're increasingly seeing is nation-states deliberately using these tools and it's moved from the province of the kind of war games caricature of a kid fooling around in their house, to big business for organized criminal groups and as part of a tool of power for nation-states.

ZARATE: John, it's a little frightening the way you describe the sort of divide between the criminal and intel side, because it harkens back to the counterterrorism world and the divide, the intel wall that was so much a part of the 9/11 commission report. Talk to us about, you know, walking through that door. And you've mentioned sort of seeing the map. Talk to us about, what you saw the nation-state actors doing and not just doing on their own, but in combination with the organized criminal groups and hackers that they were able to enlist. I think -- you've talked about this before, you've written about it. The blend of actors has been really important.

And I would just commend those watching those here, if you haven't read the FDD reports on Russian, Chinese, North Korean and Iranian cyber-enabled economic warfare you need to, because

it -- all those reports -- detail what those campaigns, what those capabilities look like. But from your perspective, what have those asymmetric capabilities and the blend of actors looked like?

CARLIN: Yes, so two quick threads. One, so after the -- when we looked at that incredible intelligence feat mapping -- when I say we could watch it happening, they had a graphic user interface. The tech guys will call it GUI. So we literally were watching them steal the -- steal the information on this screen. When we looked at it, although it was an intelligent success, I think you'll agree it did not feel like strategic success to be able to watch it flow out of the country.

So what we took from that was we need to change our strategy here, we need to figure out a way to disrupt. There was a -- there was a logic to why it was staying in the intelligence lane. You know, for years there was an approach when we did espionage cases, where if we identified a foreign espionage ring inside, say, the United States, often we would let the ring continue to run while monitoring it, feeding it false intelligence. And that was because if you disrupted it, it might be harder to find what they replaced it with.

It was on a relatively small scale and so it was better to figure out what the operatives were doing here rather than disrupt and encourage them to improve the way that they were collecting information. The problem with cyber, which you touch on, Juan, is that this asymmetric threat -- we were seeing on scale actual -- what I will call -- low intensity conflict that was causing real harm to real victims now and putting companies into bankruptcy.

And we weren't learning a whole lot. It was too -- too broad, too big. The -- former Director Comey called it, like, having a drunken gorilla banging around in your house as a -- as a burglar. They weren't taking steps to hide their tradecraft. And so we needed to disrupt. When I went back to the Justice Department, we created a new initiative to do just that and it's still very new. It was only created end of 2012, 2013, and it led to the first case of its kind, the indictment of five members of the People's Liberation Army, a specialized unit, unit 61398.

And that unit, their day job, they put on a uniform, they went to work and we put an attachment that showed it around 9:00am the activity spiked. You'd see this activity. It hit places like Westinghouse right before they were going to do a joint venture where they stole the technical design specifications for a lead pipe so the next morning they wouldn't have to pay the lease the pipe or hit a solar company, stole its pricing information from its e-mail, bankrupted the solar company, and then to add insult to injury, when they filed a trade action to sue for unfair trade practices, they stole the whole legal strategy.

So that's what the second largest military in the world was doing. And that attachment showed it started at nine, it went from nine to noon, unlike today's conference. Apparently they don't do the working lunch because it decreased from noon to 1:00.

(LAUGHTER)

Increased again from 1:00 to 6:00, decreased overnight on weekends and on Chinese holidays. So the prosecutor in me would call that circumstantial evidence, but also as -- as a threat, as a national

security threat, that means what company can compete if that is literally the day job of the second largest military in the world and it's causing real damage?

That is a government problem. That is a conflict where we need to engage or we will lose. So that was the -- why we brought the case. And you asked about the blended threat.

ZARATE: Right.

CARLIN: I think what we've seen since then increasingly -- there are four major actors in the space, China, Russia, North Korea, Iran. Particularly -- so with China, we're seeing the so-called blended threat where state actors on the side, to make a buck, are using state tools to commit crimes for their own purposes. One thing that's trending not just from China but from Iran and from North Korea, are sophisticated what look like so-called advanced persistent threats.

So it has the tactics, the techniques, the procedures of a nation-state entering companies. I have clients like this all over the United States and they say oh my gosh, we've been hit by China or looks like North Korea, what are we going to do, they're getting the world's best forensic experts to help them and it turns out they've hacked in just to get the free bandwidth so they can mine digital currency. Mining digital currency, you get paid a small amount and the idea is it costs a lot of electricity, essentially, to maintain the bandwidth so that you ultimately -- you don't really make a lot of money from mining.

But if you hack and use somebody else's bandwidth, you can make a buck. That is not part of China's strategy. It may be North Korea's because they're trying to raise money due to sanctions, so like ransomware, it may actually be for a state aim. With China, Russia, Iran, who also are doing that same type of activity, they're using these increasingly available tools of statecraft, these same weapons, just to make a buck. So that's one version of the blended threat.

Another version of the blended threat, though, is -- is -- what's shown in the Yahoo! case. So here's a case where Russian -- we tried to get Russian cooperation. We had a top 10 most wanted by the FBI credit card hacker. So someone that goes around, steals numbers and then uses the dark web -- so that portion of the internet that is not indexed -- to sell what they have stolen for a buck. And it's a very sophisticated market.

If you go to the right place today on the dark web, it looks like Amazon. And when I say it looks like Amazon, I mean you go on and you say I want to buy stolen credit cards and there's a bunch of vendors who sell the stolen vendor -- credit cards and they have customer reviews, including a five star system.

ZARATE: It's a Yelp for the dark web.

CARLIN: It's a Yelp for the dark web. So they have -- literally it'll be like five stars, I've bought from this crook before, a large percentage of their stolen credit cards work. Great review. And then what I love are the ones that are one star, this crook is not trustworthy. Like, what did you expect?

But anyway -- so they go on and sell this type of information. And so we said, OK, this isn't statecraft, let's get Russian cooperation the way we have with child pornography in the past and other issues that -- where law enforcement can cooperate no matter how many different disputes you're having in other areas.

In this area, though, what they did -- and this is laid out in the indictment Justice Department later brought -- they didn't help. Not only did they not help, they signed him up as an intelligence asset. So then they said keep stealing but also we're going to task you sometimes to steal things that are for the benefit of Russia. So that -- that is another version of the blended threat. And the third version is, I think the increasing organized crime problem right now, is increasingly a Russia problem.

Russia is a rogue actor when it comes to cyberspace. And this is true in terms of unleashing indiscriminate tools of destruction, like NotPetya, a ransom worm -- so a worm that self-propagates to lockup the -- lockup computers inside -- and servers inside companies in order -- ostensibly that if you pay a certain amount you can free it. Although with NotPetya, it seemed like there was no way to pay to unlock your goods. This is something that hit all across the world, it caused a global shipping company to lose over $500 million, it caused FedEx to lose $300 million of damages, and that's just two companies.

ZARATE: And the health sector in the U.K. was affected.

CARLIN: Health sector in the U.K.

ZARATE: Yeah.

CARLIN: This is similar to WannaCry, a North Korean...

ZARATE WannaCry, yeah.

CARLIN: ... version that had happened earlier, that...

ZARATE: Right.

CARLIN: ... that escaped. So you have that type of activity. And then you have, if you look at some of the best cases the department has brought recently, you know, cases that you kind of can't believe the details but it's important to share them.

Like indicting a criminal conspiracy that stole billions of dollars of goods whose name was, In Fraud We Trust. That was the motto of the group.

And so it was like a -- a kingpin of criminal group where all the best fraudsters had a place where they could share information, work together. Which is what we need to start doing with our foreign partners.

When you do those takedowns, you see great international cooperation and then you see a no-go zone with Russia. So they are just not cooperating at all.

And as long as these actors don't hit Russian targets, cooperate with tasking, they're providing cover for them. And that's not going to change until we take concerted action.

ZARATE: Right. That's fantastic, the way you described that. It's not fantastic that it's happening, it's fantastic the way you've diagnosed it.

John, how do you -- how do you think about this concept of cyber-enabled economic warfare? I mean, you've -- you've described some elements of it already.

You know, there are dimensions of this that -- that involve a tax on the financial system. Jamie Dimon recently talked about cyber-security being the fundamental challenge to the integrity of the financial system.

You have the types of attacks that you've described, which are attempts to gather information, undermine, you know, companies, takeover markets.

There is, in the maximalist version -- and this is something Sam has pioneered, this idea of weakening an economy to actually undermine political and military power.

How do you see this domain of cyber-enabled economic warfare, and what are some examples of it that people can think about, get their hands and -- and minds around it?

CARLIN: Yeah. One of the reasons -- so we talked a little bit about how it used to be in the shadows, and we weren't applying the core lesson of September 11th, right?

Which was, we need to share information across the law enforcement and intelligence divide, and work at -- at scale and speed within and between governments so that we can disrupt attackers who want to attack the American way of life. We've started to apply that now in cyber.

But what makes the cyber threat different, right, is that that's not sufficient. So that was necessary. But then the next part, which is really a new problem for government to tackle, is that the infrastructure is in private hands. You know, over 90 -- well over 90 percent of the infrastructure is in private hands.

Which means if we're going to effectively combat this threat, we need to call it for what it is – I named it dawn of the code war -- that we're in a low-intensity conflict that includes nation-states, and we need to start figuring out ways to -- to share information at speed and scale across the government-private sector divide.

That means figuring out ways to incentivize private companies to share information with the right authorities in law enforcement and intelligence. And it means figuring out ways to change the way we were all trained, so that our default is to share information that -- that, right now, still, I think,

overwhelmingly gets marked either "sensitive" or "classified" so we don't default-share it back to -- to show what the threat is.

Now, we've made great progress. And one thing in the book is, just to make public and share what we have already done through great work by law enforcement agents, by FBI, by intelligence analysts, and made public.

Put it together, and you start seeing that this isn't a science fiction or threat of the future, which I was finding when I talked to boards or CEOs. A lot of this has already happened, we just are not sharing what has already occurred.

So in terms of the -- the threat of cyber-enabled warfare -- economic warfare -- we've had it. So Iran was using, as a tool of government power, they used two affiliates of the Iranian Revolutionary Guard Corps to attack our financial sector with distributed denial of service attacks.

So it's that same concept of botnets, hundreds of thousands of compromised computers given a single command. And what they did is, they attack the weak point on the financial sector. Not where they're spending lots of money, protecting how transfers are effectuated.

But instead, the outward-facing websites that consumers use. And they bombarded them with these requests for information. They did so at times of diplomatic churn. And while we had sanctions in effect, and before a compromise had been reached or a deal had been reached. And it affected hundreds of thousands of customers, and cost tens of millions of dollars to the financial sector.

We showed that that same group -- and I believe this is also an arm of economic-enabled warfare -- showed that they had been able to hack into the sluice control systems of the Bowman Dam in Rye, New York. So that meant they'd be able to life up the sluice gates and flood the surrounding areas.

And we had talked for years, that this was a threat. But no case had been made public before, that -- that someone had actually done it.

Now as it happened, the Bowman Dam wasn't working. It was down for physical maintenance. But I think you'll agree, like our -- our principal response should not be crumbling infrastructure as a defense against cyber -- cyber-attack.

(LAUGHTER)

ZARATE: That's one form of cyber-defense.

CARLIN: It's one form of cyber. You don't see -- just to segue slightly, but it is actually true, when you're thinking through -- I mean, partly what we did, is we, over a 25-, 30-year period, we moved almost everything we value, from papers and books...

ZARATE: Yeah.

CARLIN: -- to digital, and then we connected it through a protocol. And we go through the history of the internet, including interviewing the founders, it was never designed for security in mind. It was designed for communications.

And we did so systematically, in government and the private sector. We did that without properly calculating what the risks were.

Some of those decisions might remain the same. Many would not, if we actually thought, "Hey, what would a terrorist, what would a nation-state, what would a crook do to disrupt this activity?" And now we're all playing catch-up.

One of the answers is...

ZARATE: Yup.

CARLIN: ... use old stuff. You know, the Russian attack on the Ukrainian power grid was not as effective as they thought it would be, and as it might be, here in the United States, because they had only recently upgraded their technology so they actually knew how to operate, still, the electric grid manually.

Now, we're moving to places where that's no longer the case. Maybe we shouldn't. And the same thing happened to our electoral system, right?

ZARATE: Yeah.

CARLIN: What was the solution to this great sophisticated 21st century nation-state attack of potentially disrupting our elections? Paper ballots. You know.

So they may be lower-cost solutions...

ZARATE: Floppy disks for the nuclear program, yeah.

(LAUGHTER)

CARLIN: Only take it so far.

ZARATE: And are you -- just to take the Iran example, are you worried that Iran will dust off that playbook again, given that sanctions have been ramped up? Do you think Iran is poised to attack, perhaps in more sophisticated ways?

CARLIN: Yes. I mean, I think it's something that we need to take -- there has been an increase, it looks like, in Iranian activity over the last year, year and a half.

There was a great case that laid this out, that didn't get a lot of attention, I think, because of so many things -- other things that are going on, that showed Iranian activity across this swathe of U.S. industry that the Justice Department brought, based on FBI investigation.

I don't know why right now. And so be it, people are theorizing as to why you've seen the activity, what are they doing with the information that they've been taking.

You have this diplomatic play right now, where Iran's working effectively with Europe to try to evade sanctions. If that fails, then I can definitely see an increase in disruptive attacks, and something we need to start preparing for now.

North Korea is already quite active. And what they're doing is, in some cases, less to send a political message and more as a way to evade sanctions. They're committing ransomware on a regular basis, so they're attacking private companies and collecting ransoms just like crooks are doing. They've committed a nearly $100 million bank heist, that also has been laid out in a public indictment, taking advantage of the SWIFT system and would have been a $1 billion but for a small actual mistake that allowed it to be uncovered. So they're...

ZARATE: So it was the Bank of Bangladesh case...

CARLIN: ... Yes.

ZARATE: ... that people have heard about?

CARLIN: Yes. And then WannaCry itself looks like it -- it's unclear to me whether that could have ever raised money, or whether that was a tool that escaped from them that they were going to use to try to coerce, or whether it was a money -- a money-raising tool.

And we've already seen them use cyber as a political tool, again, with this low-intensity conflict concept when it came to not liking the First Amendment, or the right of free speech, when North Korea attacked Sony Motion Pictures because they didn't like a movie they were going to make. It's the only time in my career I've had to brief the President of the United States in the Situation Room and start with giving a plot summary of The Interview.

ZARATE: Did you play a clip?

CARLIN: We played a little clip -- I don't know how many of you have seen it but it -- it -- it's not an easy movie to summarize because it doesn't make a whole lot of sense. And we war gamed for years, what would it look like if a rogue nuclear-armed nation attacks the United States through cyber means. We got that one wrong in terms of what the first attack would look like, but that was an attack.

I mean make no mistake -- on a value, right? The same way the Russians are undermining confidence in our electoral and democratic system, and view democracy as an existential threat, which fuels their strategy in Germany, and then similar attacks in France and elsewhere.

North Korea was saying, hey, we can sit from North Korea and influence the decisions of moviemakers in the U.S. so they don't produce content...

ZARATE: Yeah.

CARLIN: ... that we don't like. That is a form of warfare. It's using coercion to change the way we behave.

ZARATE: Yeah. An asymmetric attack on our soft power, right?

CARLIN: Yes.

ZARATE: That's right. John, help us to, sort of, think about, sort of China and the threat from China. You know, China is a major economy, you know, soon to be the largest economy in the world, a major military power to -- to your point earlier, major cyber capabilities. They're doing lots of nefarious things.

They also do a lot of things under the guise of just being a part of the international community. They're trying to grow their economy at a certain rate every year to meet the needs of their people. They are trying to make technological advances, the China 2025 plan. They're now talking about greater self-sufficiency in the wake of the trade battles with the United States.

How should we think about Chinese behavior and especially in the cyber-enabled economic domain? How do you diagnose this, because I think it's hard for people to kind of get their hands around understanding Chinese behavior?

CARLIN: Yes, it's so -- it's -- and I know it can sound somewhat pessimistic when you describe where we are and the current threat. And I think that's a necessary bell to ring because we -- this is the area in which we move furthest, fastest, and we are more vulnerable than other countries and it needs to be addressed.

I'm optimistic in some ways with -- with China and Chinese behavior because, at the end of the day, it's a cost-benefit strategy for them and it's a cost-benefit strategy that can be measured in dollars and cents. And so, what it is going to require, and sooner rather than later, is a concerted effort to raise the cost, and raise the churn and raise the diplomatic tension over a targeted type of conduct, to say it is not OK to steal intellectual property or trade secrets.

Your better -- your strategy is better effectuated by investing in research and development. And it seems like, you know, ultimately they don't -- unlike some regimes, North Korea or possibly Iran, Russia -- they don't want to blow up the current international world order. They wanted -- they want to succeed within it, so there may be an incentive.

And we saw this a little bit because after the indictment of the People's Liberation Army members. And then, there's a case that I go through in the book that got less attention at the time, but I believe China was tracking carefully, and that's the case of Su Bin. So there was a lot of discussion. Is this name and shame? You've indicted these officers. Unlikely China is going to extradite members of its -- of an elite military unit, so why are you doing this?

And we said, you know, this is -- these are real charges, if we catch people there will be criminal consequences. There was an individual named Su Bin, who had stolen economic -- committed economic espionage in a conspiracy against Boeing and other companies, who was arrested pursuant to U.S. process in Canada. They knew he was under arrest, they wanted to get him out, they weren't successful, he was brought here and he did serve -- he was incarcerated.

So there was that case, and then President Obama signed a new executive order that -- for the first time, thanks to the Juan Zarate approach built in terrorism, but if we applied that same approach of allowing individuals to be sanctioned, not just those who stole information through cyber-enabled means but the companies or individuals that benefited from the stolen information, and there was a lot of reporting that the Obama Administration was about to use that new sanctions authority.

So, I think it was that combination that led President Xi in a breakthrough to say we agree with the concept. You shouldn't use the military and intelligence to target private companies for the benefit of their economic competitors. And the talking to the third-party groups, the CrowdStrikes, Mandiants -- you're going to hear from CrowdStrike later today -- and along with government analysis we saw a decrease in change in the behavior. Now, it was very narrow. It -- it fit exactly in that bucket and it only was companies when they were headquartered in the U.S.

We are now seeing that they are moving away, according to analysts, from that agreement during a period where there's a lot of trade churn. I think it shows, though, if you can -- you can change the behavior, but it takes continual raising of the costs. And you have to do it as part of a strategy that includes not just use of criminal indictments, but use of Treasury Department sanctions, the Commerce Department authority to designate certain entities as those with whom if you do business is contrary to the national security interests of the United States, so you -- they can no longer rely on our supply chain.

Diplomacy, so that it's top of the president's talking -- the Commander in Chief's talking points every time they meet with their counterpart, all the way down our system and -- and you need an off ramp. You need an exit strategy that says if you stop the activity and it's measurable, then we will stop escalating the costs so there's a -- they can change the cost-benefit analysis.

And I think that is the drive behind the recent announcement by the attorney general of the United -- the former attorney general of the United States -- two weeks ago. But that -- I just interviewed the -- the lead person in charge, who is my successor. John Demers is the assistant attorney general for national security. They said, even though there's a switch of attorney general that approach will continue, that says that the Justice Department is going to continue that all-tools approach.

ZARATE: And the Justice Department, thanks to your leadership, innovated this use of indictments to get more information out, to attribute these kinds of attacks. And so, you've seen indictments of Chinese officials, Russians, certainly the Mueller investigation, Iranians as well. So I want to -- I want to make sure to credit you John appropriately because you -- you really did innovate this idea of indictments as forms of attribution as well as a -- as part of a deterrent policy.

Let me ask you two -- two more questions quickly, because we're running out of time.

You talked about the private sector, the private sector uniquely targeted and affected, especially in this domain. What more can the private sector do or demand, especially of the U.S. government?

CARLIN: So I think the private sector should demand action in this space with the concept that there was a -- there was a time I think where people were hesitant on action because they saw more opportunities for business in place -- places like China than they saw risk.

But as we're seeing in sector after sector, if you allow the military and intelligence services to be directed against you, you're not going to win that fight, and the 2025 plan does not involve U.S. business success in China.

So you need government help to change that -- to change that calculus. And then we have to do a better job -- you know, when I talk to private sector, understandably there's a lot of confusion that they're going to be regulatorily punished or civil action if they go tell people about the threats.

So the current cost-benefit analysis inside our own C-suites is often let's not tell someone about a threat, or it's so privacy-focused, which is important, but at the end of the day, I don't know about you, but as a consumer, I've been told my information has been stolen something like 15 times.

My daughter's first, you know, mail addressed to her by name was a notice that her identity had been stolen and she was a baby because she was in my OPM -- Office Personnel Management forms. We can't do a lot with that information as consumers.

We need to encourage the conversation to be with the right parts of government that could take action.

ZARATE: Yeah, and there may be a need for more collective action within the private sector within particular sectors.

CARLIN: Absolutely.

ZARATE: You've seen this, for example, in the banking sector. Last question, I know our time's up but I -- I have to ask this question because in John's book he talks about the failure of imagination. Part of it is just not realizing where the threats are coming from, how the vulnerabilities manifest.

What's -- what's your concern about what we're failing to imagine at this point?

CARLIN: Yeah, if there could be one call -- call to action today, it's read science fiction and look at the world that they depict. You look at so many of the threats that we face, they all were -- from the word cyber itself, which comes from a -- a William Gibson book, "Neuromancer," to many of the threats we're facing, they've been articulated in our movies and in our books.

The Internet of Things -- so the -- we are moving forward at rapid speed without doing that same risk calculus that we did with the books and papers to digital form. So we have already put

pacemakers into people's hearts that were not encrypted so an 11 year old can hack and kill and then realize hey that's a problem so they've rolled out a patch.

Now I don't know how many of you have had some glitches with your Windows system -- that's one thing when it's happening with your, you know, computer at work, it's another thing when it's the pacemaker in your heart or the cars on our road where we had a similar recall of 1.4 million jeeps because we realized that you could hack from the entertainment system, hop over to the brake and steering system and take over the car, and it also happened with drones in the skies.

We're at an inflection point, because we are moving in that direction. So we need now congressional action, we need action by companies to incentivize security by design on the front end before we move into that world where everything we have is connected and still using an insecure medium.

There is time to do that, but we need to act now.

ZARATE: Fantastic. John Carlin, author of "Dawn of the Code War," great opening to the conference. Thank you John for your time and your work.

CARLIN: Thank you.

(APPLAUSE)

ZARATE: That was great.

CARLIN: Thank you.

RAVICH: Thank you John and -- and Juan, that was really fascinating.

END