Cyber-Enabled Economic Warfare: CEEW Threats from Russia and China

Remarks from 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 Daniel Hoffman, former Chief of Station, Central Intelligence Agency, B. Edwin Wilson, Deputy Assistant Secretary of Defense for Cyber Policy, Dr. Larry M. Wortzel, Commissioner, U.S.-China Economic and Security Review Commission of the U.S. Congress, Michelle Van Cleave, former National Counterintelligence Executive

RAVICH: I -- I encourage the folks that are standing in the back, you know, come up, sit -- sit, have a seat. You know, I was particularly struck by how John was talking about how to map the threat and how to deduce what the adversary's doing strategically from what we're seeing and what they're doing and how they're doing it.

And it is leading to a very robust conversation that is happening I think throughout the national security ecosphere on deterrence versus things like persistence and how it will vary depending on the adversary that we're dealing with.

And, you know, building on these themes, let me welcome our next discussion focused -- focused on cyber-enabled economic warfare threats from Russia and China. Because when you look at the top -- these top cyber powers, these nations, China and Russia, kind of lead the bad guy side of the ledger.

And to lead the conversation on the scope of the threat and what the U.S. needs to do about it, let me introduce Michelle Van Cleave, who will moderate our panel and introduce the other speakers. Michelle's full bio, as well as those of the rest of the panelists is in your program booklet.

But let me just highlight Michelle's service as National Counterintelligence Executive, which she held the position a few years back and the insight she brings about the ways that cyber technology has exponentially enhanced the espionage capability of our adversaries.

Michelle, thank you and -- and over to you.

VAN CLEAVE: Thank you Samantha. So do I -- can I do that from here? I don't have to get over to the podium, do I? Excellent, thank you. So hello everyone, and I think that the first presentation this morning made a good stage -- stage setter for the conversation this panel is going to have.

I have to begin by saying however that I am currently with the Jack Kemp Foundation, and Jack was my first boss in Washington, D.C., long ago in the early '80s, and I've been close to him and his family over the years and I know from that experience that -- if I'm not mistaken, tell me Samantha, that Jack was one of the founding forces behind the creation of the Foundation for the Defense of Democracy.

So I'm especially pleased to have the opportunity to be here to see your good work being carried forward, I know he would be so pleased. This panel is comprised of a -- a number of very interesting people that bring different perspectives to the panel.

As you know, your -- you can find their bios, but if I could very briefly, from the left, Dan Hoffman served for 30 years in United States government and served in several high-level positions in CIA, including Senior Executive Clandestine Service Officer and Station Chief I suppose more than once -- we'll need to talk about that.

Ed Wilson -- Major General Wilson is the Deputy Assistant Secretary of Defense for Cyber Policy, where he helps formulate the policies and strategies to improve the Defense Department's ability to operate in cyberspace, so we're glad you're here, Ed.

And last but not least is Dr. Larry Wortzel, who is an eight-term Commissioner of the U.S.-China Economic and Security Review Commission, so a broad reach of talent on this panel so let's get into it.

I -- I think it would be good to start by looking at a broad strategic perspective of how a cyber-enabled economic warfare plans and activities support the advance of strategic objectives, policy objectives of China, Russia, and what the U.S. strategy or policy has been needs to be in response. So if we can start as sort of that -- something of a 30,000-foot level, Larry. So how do these activities fit in with China's general strategy and policy toward the U.S.?

WORTZEL: If I could, I'd like to start with the most recent arrest and indictment of Xu Yanjun, who managed to penetrate a number of aviation companies with a whole network of people. The past panel discussed a little bit of it.

But I want to focus on turbine fan blade, and turbine jet engine technology. We lead on that. We -- we lead the world on that. And I've been watching China for far too long, but they are terrible at it, and they always have been.

I mean, they tried to crack the technology with G.E. wind turbine engines. And I visited their factory, talked to a bunch of the engineers. And they just could not manage the metallurgy and the quality control.

So here we're leading the world in the engines that power our bombers, our combat aircraft, our civil aviation. And the Chinese can't make it. That leaves them with a one-time use army.

So their intent may not have been to cripple the United States, but what they did -- well, with that sort of a penetration, was potentially leap themselves forward, and change their air force from an air force that could be used once, and then they had to go back to the Russians and beg for more engines. And that's going to take some time to, potentially, being able to put out a military, and an air force, and a naval air force that can reconstitute itself in a war.

And at the same time, my -- my greatest fear is that we -- if they are able to navigate a network that well and in so many companies, we really don't know what they injected into the network. So you're really talking about cyber-enabled economic warfare.

VAN CLEAVE: So in addition to that, there's a rather active Chinese exploitation of cyber networks for the acquisition of -- of information. And I've got say the -- the espionage piece of this obviously interests me quite a bit. I -- and -- and there's something about it that, genuinely, puzzles me that I would like to get your response to.

I -- I think, you know, certainly, the attack on OPM...

WORTZEL: Yes.

VAN CLEAVE: ... and the -- and the exfiltration of 11 million personnel files and -- and records of all of the intimate details that that -- and anybody -- of us who's had a security clearance are well aware of all the very private information that is -- that is posted in there about your family, your health, your finances, the people you know, the places where you got all of these things.

So the -- those personnel files, and the personnel files that they lifted out of contract as doing background support, those things I understand well -- and Dan could tell us -- I understand well the value of that kind of insight for potential recruitment, and human espionage that is -- is very -- very obvious, the value of that.

But I'll tell you what I don't understand. There are all of these attacks on -- on health records, on credit card records, you know, on the -- the Ashley Madison type of stuff who have nefarious people engaging in things they probably wish their family didn't know about.

It -- it kind of looks as though that they may be building files on individual Americans with -- with this kind of Social Security information, and all of the things that they're reaping, what's the endgame here?

WORTZEL: Well, I think the endgame is being able to know who to target, know who is traveling where, identify our own clandestine service officers that may travel to meet their people. And -- and a lot of these cyber penetrations initially became -- began with, either, fishing attacks, or actual recruitments, or handing somebody a flash drive. So -- so it allows them to do an awful lot of things.

And they -- they really keep great records. I mean, the Russians do too. I -- I -- I was in Singapore with five GRU and KGB fellas who ended up in China with me. And they -- they remembered my wife -- this was 1982 -- really enjoying lemon vodka.

I ran into their station chief in Japan in 2003. We had dinner. He saw me to the airport and handed me a half gallon of lemon vodka for my wife. So the records are good.

(LAUGHTER)

VAN CLEAVE: Nice. Well, that's a good segue, maybe, to Russia. Could you -- Dan, do you want to speak about that a little bit? I mean what is the perspective...

WORTZEL: Sure.

VAN CLEAVE: ... and the differences that -- that we see with the -- the main avenues of approach that the Russians have, given their strategic interests and their objectives?

HOFFMAN: So just one comment on China, just what we see from Russia and China, a very symbiotic relationship between cyber and HUMINT, cyber-enabling human operations. When you -- when you steal people's health records, you know vulnerabilities. You know if people need help with one or another medical condition.

And then there's HUMINT-enabled cyber where the Chinese and the Russians in particular but not exclusively those two nation states, might seek to recruit individuals with access to private industry or a government cyber infrastructure, and use that to their advantage.

As far as Russia is concerned, look, we're under siege from massive Russian cyber attacks while they impose cyber sovereignty on their own people to deny them the freedom of expression which would threaten Vladimir Putin's regime security, which is all that matters to him.

They're seeking to penetrate our cyberspace. And -- and they do it in a multitude of ways. They'll conduct traditional espionage operations which are the ones that none of us will see because they're run by Russia's intelligence officers, their Foreign Intelligence Service, the SVR and the GRU. Less so, they're the ones that kind of bungle things. If you read the Bellingcat report, their tradecraft isn't always up to par.

And then, they're running what I like to call discoverable influence operations. Vladimir Putin served in East Germany supporting illegals, so I like to use the Hansel and Gretel metaphor. He's leaving a lot of bread crumbs with a Kremlin return address and what he's doing to us by buying ads in Facebook with rubles, and a Kremlin return address back to the Internet Research Agency.

He does those things because he knows the best way to soil our democracy is to intertwine it in some conspiratorial fashion with the Kremlin. It doesn't mean that he's not doing things that are non-discoverable in cyberspace, for sure he is.

But he's run a series of these operations against us with that in mind. And then, lastly, what I would say is Russians are seeking to make us pay a price just like the Chinese for doing business in Russia. So they demand that if you do business in Russia you turn over your source code.

And banks and other elements in the private sector, I think, really struggle with those requirements imposed upon them by Russia's FSB. And that's with only thing in mind, which is to penetrate our -- the Russians don't draw a distinction between our private sector and the public sector. For them it's all one big, giant target. That's why you see them targeting energy infrastructure, our electrical grid and other things.

VAN CLEAVE: So could you elaborate on that a little bit. I mean the Dragonfly 2.0 attack on the energy infrastructure seems especially startling?

HOFFMAN: Yes, so...

VAN CLEAVE: Can you speak to what you think is going on there.

HOFFMAN: ... if you look back at Russian history over the past 10 years, start with the massive DDOS attack against Estonia, and then the first ever hybrid war against Georgia, which the Russian Army Chief of Staff Valery Vasilyevich Gerasimov wrote about in a military journal, 2013. This is concurrently finding on land, air, sea, maybe even space, and then in cyberspace concurrently. And so it's war fighting, and that's why the GRU were the ones responsible for hacking into our social networking and media sites. It's also why they're seeking to probe our infrastructure. And they'll do it in a way often to show that -- that -- to show us that they're capable of doing it, as a measure, I think of deterrence, so that if we target them, we've talked -- this administration has indicated that they're interested in mounting offensive cyber operations at the point of attack to damage the Russian entities that are targeting us. The Russians want to show us that they can get us as well.

We're in a -- in an arms race with Russia. It's not just intermediate range ballistic missiles with a nuclear warhead; it's all about cyberspace as well.

VAN CLEAVE: So I think that's a good setup, Ed, to turn to you. I was struck with the issuance of the national cyber strategy earlier this year with this passage in which it raised a purely technocratic approach to cyberspace as insufficient to address the nature of the new problems we confront. The United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation.

Can you elaborate on what that is all about?

WILSON: So, first, Michelle, thanks for hosting us and really, for the FDD organization in setting this up. A great opportunity to really have a good discussion here.

I think maybe backup just a second and look at the strategy, the national cyber strategy, and just to put it in context, and then maybe I'll speak -- what I'd like to speak to the national security implications of that.

So, when it comes to the economy, I mean, clearly this nation -- and it's articulated in our national cyber strategy -- it's the prosperity of citizens and our way of life, as well as our allies and partners. I mean, that's one of the key components of the national cyber strategy.

And to preserve that and to secure that, we want use all the power of the -- the tools of power for the nation, along with our like-minded nations and our allies and partners.

And so, we do reserve the right when required, to step in, whether that's cyber-effects operations, or sanctions, or all of the tools of the nation.

When you look at what the Department of Defense's perspective on this, what we've seen is two revisionist powers, in the form of China and Russia, really beginning to -- those are our pacing threats in the way that we think about the national security landscape.

And each country uses a suite of tools with, but they're operating, from our perspective, below the traditional thresholds that we would typically respond with traditional military power.

So what do we mean by that? That's theft of intellectual property. That's malign influence, potentially in elections, or just in society at large, drive divisions across different segments of society, whether that's here in the United States, as Dan highlighted, in Georgia. We've seen it in Europe, Estonia, as other countries. This isn't -- we're not the first country that's been targeted by Russia.

When you look at China, it’s more of a manipulation in terms of economic tools of power, if you will, to seek to gain strategic advantage. And so the department has leaned forward in support of the national cyber strategy, and we're really looking at all of the mechanisms that we can bring to bear, and the Department of Defense has some unique capabilities. We are typically externally focused, threat focused. That's our job in the Department of Defense. And so we align ourselves to those threats and bring to bear capabilities. That may be within cyberspace, but we also operate, as Dan highlighted, in you know, land, air, sea, space and cyberspace. And so we're beginning to normalize our operations and the actions that we would be able to take within cyberspace.

Is it the only solution, cyber-effects operation, whether defensive or offensive? By no means. We want to make sure that that's in concert with all of the other elements of power from the nation.

VAN CLEAVE: So a part of this is a defend-forward strategy?

WILSON: Exactly. And so from a Department of Defense perspective, our uniqueness is that we understand the threat externally, and that we bring to bear a unique set of capabilities and what we describe as defend-forward. So we need to be able to see and understand the threats that are forming against the nation from a national security perspective. In doing that, we are able to identify threats, no matter what threat that is, and then to be able to work as a whole of government to counter that threat.

It may be a Department of Defense solution, but in many cases, and I would point maybe to recent efforts underway with election security, where we have unique arrangements in place now with the Department of Homeland Security, where we share information, intelligence about particular threats so that we can make their defenses more robust. Does that mean that the Department of Defense is taking any aggressive action? By no means, but we think the insights that we have gained alongside the intelligence community, the defense community, and share that with our other interagency partners, departments and agencies. And that's been very effective, in terms of raising the bar associated with the homeland's defense.

VAN CLEAVE: So, I -- I was reading the Defense Science Board report from last year, and I've had the opportunity to serve with them in various capacities over the year, and this conclusion is -- is troubling with implications. I wonder if you would discuss it. They say, "The unfortunate reality is that for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed our ability to defend our key critical infrastructures." Now looking at the infrastructure defense piece of that. How do we -- how do we deal with that? What is the -- what is the -- what is the approach?

WILSON: Right. So we -- in concert with the national cyber strategy being issued, the department issued an the updated DOD cyber strategy, and we deal with that concern. It's really deterrence in cyberspace. A lot of people use the term "cyber deterrence," but I beg to differ. I think there's strategic deterrence that's underway, and we use cyber-effects operations, alongside all of the other tools of power for the nation to be able to choose some deterrent.

And so there's really two components. Traditional deterrence at play would be, one, deny the benefits to the best of our ability, and I think that's where the Defense Science Board had it right is, that's a very difficult proposition in today's society, as the threats have increased dramatically.

VAN CLEAVE: And different if you are speaking about China or Russia I assume... the deterrence approach is adversary dependent.

(CROSSTALK)

WILSON: Any nation-state that is wielding these types of capabilities, but clearly the most potent threats are emanating from, you know, the more mature threats, Russia, China being examples.

So we want to deny benefit, and so that's what you see with regards to the department assisting and partnering with other departments and agencies, to information sharing, bringing to bear unique expertise that we might be able to bolster their defenses and working with industry and partners through the ISACs, et cetera, to be able to do that. And so we're beginning to work through a series of pathfinders and pilot projects to take that -- that burden on, to be able to assist in a more effective manner.

The other is, is to be able to impose or increase cost on an adversary. So the risk, the decision calculus becomes more complex.

And so increasing costs, that is standing up and being able to have -- at-bear, you know, when directed by the President or the Secretary, to be able to deliver affects operations when required.

And so it's really hand-in-glove. It's both. And it's not only cyber effects operations, it's alongside the other tools of power, sanctions.

The attribution you see, very -- we've been very -- as Larry highlighted here just recently, attributing and indictments. You know, attributing actors, designating specific organizations, indictments, trade sanctions, et cetera. And then in tandem with that, if required cyber effects operations.

So it's not only about cyber-on-cyber.

VAN CLEAVE: Did you want to jump in and...

WORTZEL: I -- I really did. I mean, this is -- there's an old debate. Vice Admiral Arthur Cebrowski in 1999 raised the issue of offensive operations versus defensive operations in cyber.

We've been debating it. I -- there's Harvard Law School articles. But -- but let's look at some of the major exfiltrations of U.S. data that improved Chinese capabilities. Lockheed Martin, G.E., Northrop Grumman.

Now, Northrop Grumman, I don't think the government's the answer to this, frankly. Northrop Grumman, for our China Commission, published the first name-and-shame report on the cyber unit for the PLA in Shanghai.

And then -- you know, I'm glad the government followed up. Finally, the government decided, "Well, maybe that's a good idea. Let's expose it."

I'm more interested in pursuing Cebrowski's idea of defense. I mean, think of the -- the concept of a castle defense law that applies to cyber.

Lockheed Martin, G.E. and Northrop are quite capable of putting together an offensive cyber effort. They don't need the government, and the government's not going to be able to cover them.

These companies -- I mean, there's a lot of legal arguments against doing it -- could deploy their own honey networks to figure out who's trying to penetrate.

And could put out honey pots in those networks that are full of malicious data, as -- it could ruin their -- what -- they think they're getting something great, it'll ruin their engines. They'll blow up. They could put in malicious information that'll put down a computer system.

It -- it's kind of a dog-eat-dog world. And I just don't think the government's got the assets to protect these big private actors. The government and homeland security, in my opinion, can help small businesses and people. But banks and the Northrups, that really affect the U.S. economy and warfare, are quite capable of doing it themselves.

VAN CLEAVE: So that sort of leads me to ask, is this one of the things you consider to be the -- among the greatest dangers, I guess? That's really the next question to all of you. Where -- what are the areas where you think are a genuinely dangerous for the future?

HOFFMAN: I'll just add one other point. But first, I want to -- I agree with you 100 percent. it's about -- in the private sector, it's about hardening your own -- your own facilities, your own installations.

And a cyber-attack isn't a lot different from a -- a terrorist attack. There's surveillance that's conducted before the attack, and that's where you need to detect who's out there targeting you, and then seek to learn who that -- who that -- where that threat actually came from.

And we've talked a lot about state actors. What also concerns me are the cyber capabilities of non-state actors, terrorists in particular who might seek to target our critical infrastructure...

VAN CLEAVE: The only reason we haven't gone into that, because our host asked us to just talk about China and Russia.

(LAUGHTER)

(CROSSTALK)

HOFFMAN: Got it, I'll stay away from the terrorists, then. Even though it just occurred to me. But I'll tell you that the challenge on Russia is that the lines are often blurred there.

The Russians use criminal hackers and -- to accomplish their mission, often. And those hackers could also be doing the mission of others as well, and that, I would just -- I have to say, that's of great concern to me. It's a little bit off the tangent of Russia, but I have to highlight that.

VAN CLEAVE: What else?

WORTZEL: Well, for China, I mean, if you -- actually FDD's own publication on China mentions Dai Qingmin, who wrote the Chinese doctrine on integrated network electronic warfare follows old Soviet radio-electric combat. Combination of cyber strikes, electronic warfare, penetrations and precision fires.

But other Chinese authors -- military authors since then have advocated attacking through cyber, ports of embarkation in the United States. Going into our NIPRNet, our non-classified military networks that would deliver logistics.

If you did that, you could knock out the shipping of spare parts out into -- well, let's assume Asia, anywhere. You could slow down and misdirect airplanes, thinking they're going to refuel in one place and send the refuelers someplace else. You could shut down trains, you could shut down ports.

That's what scares me.

VAN CLEAVE: So, Ed, you have a good big portfolio, figuring out how to deal with all of these things. What is it from your perspective, that most concerns you? The hardest nut problems.

WILSON: So just to put it into context, I think when we step back and look from a historical perspective, we see a lot of the same behaviors from the key nation-state actors of Russia, China in particular. But I think the challenge that we have right now, fundamentally, is the pace, the sophistication, the proliferation of these threats.

This domain behaves differently. It's a man-made domain. And it's those -- these -- these threats accelerate. That's one of our key challenges.

And so as large as the Department of Defense, really the nation, these threats present unique challenges. And I don't believe we've seen in history to the degree we have over the last decade or so.

Does that mean that we throw in the towel and -- of course not. And so clearly, I think there needs to be a public-private partnership. We're actually -- have begun to look very, very keenly at our partnership with the Defense industrial base in particular.

We've done that in the past. We've actually brought to bear, a task force to begin to address some of the key findings that we've been seeing, based on behavior over the last few years.

It -- it's coming to -- it's coming, really, to a culminating point. And so we're beginning to take different types of actions, looking at contracting language, in other words, to qualify to compete, those types of activities.

Our acquisition and sustainment community's been very vocal over the last few weeks about that. We're looking at, how can we share information in a more agile sense. How can we then help with sensors, especially on the smaller companies. The larger corporations typically do fairly well. It's the second- and third-tier suppliers that are the most at risk, and where we see a lot of the exfiltration occurring.

It's because they just don't have the means to be able to go up against, really, a nation-state. It’s not a fair fight. And so, it's not one solution. There's really a variety of solutions we have to bring to bear.

VAN CLEAVE: Well, there's a variety of problems too, when you think about...

WILSON: That's right.

VAN CLEAVE: ... think about trying to prohibit exfiltration of technology we don't want out. Then there's also to protect the infiltration of technology we don't want in, which brings to mind...

WILSON: Right.

VAN CLEAVE: ... the whole question of the supply chain manipulations, which we haven't really talked about yet. But -- but the -- that frightening business with -- what was it? -- Supermicro was the company out in California where -- can you tell us a little bit about that, where the -- the motherboards that were imported -- that were manufactured and -- and -- and promulgated by -- sold by Supermicro, and it got into so many different systems across the country.

WORTZEL: Yeah -- yeah, I mean it's -- it's really an unsettled accusation. I mean it's really...

VAN CLEAVE: Is it?

WORTZEL: Yeah, it's -- it's debated, but -- but the fact of the matter is that the Department of Defense alone and State -- I'll include State -- has no idea of their supply chain. They only know their primary suppliers.

Our commission several years ago went to Army, Navy and Air Force with four ongoing weapons systems under development and said give us your supplier's supply chain to the fourth tier. They couldn't do it. They still can't do it.

So they don't know what they're getting and what's going into their systems.

WILSON: It's one of the fundamental challenges that we're -- we're facing and we're taking -- beginning to take actions to resolve that, yes.

VAN CLEAVE: Well, just so the breadth of this -- of this topic -- I'd like to go back to -- Dan, something that you -- you mentioned in your earlier comments, influence operations. I -- I wonder -- I mean we've seen the state of play with respect to influence operations directed at trying to affect elections, influence the decisions in -- of voters and viewing -- what about -- what is the future of influence operations?

I -- I -- I wonder, is there a potential here? Am I making things up? And is there a potential here for influence operations directed at other things to affect public confidence in markets or in products or -- or other things?

What do you -- what do you see coming down the pipe there?

HOFFMAN: Yeah, I mean -- I think we -- we look at cyberspace, a manmade domain completely unregulated as a force multiplier for economic growth and freedom of expression, and what Russia sees is OK, that's the critical backbone of our -- of our democracy in the United States and that's why they want to target it.

And they want to degrade our trust in cyberspace and then simultaneously use it to influence our population to the extent that it serves their interests. I'm not sure that we've seen any evidence of Russia seeking to influence our economics as much as we have our politics.

And again, what we've seen so far, these -- what I like to call discoverable influence operations, but the Russians are good enough to run misattributable political influence operations if they want to support one candidate over another and not have a Kremlin return address.

This goes back to Soviet days, when they -- you'd have journalists in their pay. Essentially what -- what we're seeing in cyberspace from Russia really isn't a whole lot different from what Soviet intelligence officers were doing to us, it's just the technology has changed.

The idea, the strategy is -- is pretty well -- pretty well the same as it -- as it always has been for them. And it's -- it's cheap and it's asymmetric warfare, and I will just highlight based on the many years I served at CIA -- I served five years in Russia as well as in South Asia and -- and the Middle East, but -- but the years I served in Russia, I can tell you the most important thing that -- that our intelligence community could do is -- is make human source penetration so that we understand where the Kremlin is headed strategically.

And we can use that intelligence to give us the threats, the indications in warning so that people like Ed and our other colleagues in the government can harden our defenses and then share that -- that -- that threat warning intelligence with the private sector to protect them, as well.

VAN CLEAVE: Well, that calls to mind a question maybe for Ed. The process by which our intelligence requirements are generated is so significant for the decision maker to be able to get their arms around difficult problems.

And -- and -- and I -- I wonder, from your -- from your perspective, and -- and Larry and Dan, chime in as well, but from your -- your perspective, what are the big unknowns? What are the areas where our insights are perhaps not as robust as you would like them to be?

What are the big -- if you had a magic wand and you could say, all right, this is what I want to know in order to be able to plan correctly -- blue sky this for me. I mean what is it you really, really want to -- to know that we don't?

WILSON: I'll -- let me address that, but I -- just would -- pile on with Dan, I think we've seen a history, especially from Russia in particular, of behavior that's targeting institutions of trust. And so one of those that we have abiding faith in in the United States is the elections process.

It's -- it's the core of really who we are in terms of a structure of freedoms and choice here in -- in the United States. And so Russia sees that as a center of gravity, if you will, using my military speak, but to go after it -- and it doesn't necessarily have to tear down the elections process, but our faith and confidence in the elections process.

So that's what we see, and it's Russian, really Soviet behavior, from generations back. That's not -- nothing new, it's just tools of the trade that are being used -- really have been brought into the 21st century in scale at a -- scope and magnitude that we haven't seen before.

And the -- the technique of using proxies associated with that gives them a sense of deniability. And so we see that behavior not just in the United States, but really around the free world. And so whether that's striking at the institution of NATO, our elections process in the free countries, that's really what you'll see over and over again and that's what we're combating.

So with regard to the question of the -- the priorities, we -- we always have, as one of our top priorities, is to understand the thinking and the motivations, the intentions of senior leaders, and you don't -- adversary nations.

And so that will never go away, that's always at the height of what we're after. In terms of being able to counter that, and to be able to put in place confidence building measures, et cetera, to be able to backstop and give us some stability, especially in this space, is going to be key every step of the way.

VAN CLEAVE: Ed, from your perspective?

WILSON: Well, I -- I think the Chinese are -- actually, if you can read a little Chinese, pretty transparent about their broad strategic objectives. I mean the literature's out there, the doctrine's out there, there's tons of meeting results.

What -- what we really don't know because of the way they've exfiltrated data -- so you talked about all of this health and personnel and travel, is who their targets are. So -- and -- and -- and Chinese intelligence services have really shifted targets.

They used to go and -- and try and recruit the diaspora, ethnic Chinese. Today, they're happy to get anybody and target anybody and either pay them or coerce them. So I -- I -- I -- if I could have my way, I would want to get into their targeting.

That's what I'd want to know, who are they targeting? What are those weaknesses? Is it -- double agent operations are very difficult, but could -- could some of these be turned into double agent operations, either with -- with malicious cyber tools or through human agents?

VAN CLEAVE: Dan, you... your perspective?

(CROSSTALK)

HOFFMAN: No, I think those are all great points, and it just highlights the value of intelligence so that we know our enemy.

And then I would just highlight too if we think about what we're going to do about it, the last thing we want to do is curtail our own free speech.

So the deal -- the way we deal with Russian and other disinformation in our cyberspace is with more free speech. And the private sector has actually done well in exposing Russian disinformation efforts, including on Twitter with the Hamilton 68 site, for example.

I think that's -- it's always important to think about the intelligence you're collecting, and then ultimately how are you going to analyze it and then what you're going to do with it. And in this case, I think exposing the Russian disinformation for what it is is the best way to educate our citizens, so that they can step out smartly and discern what's real and what's not.

VAN CLEAVE: So on -- I'm wondering a little bit about something we were talking about before the panel started, Larry, which was a concern that you mentioned, with respect to the management of crises to be able in time -- to be able to respond in times of crises and how some of the activities that we see now may be, if I can use the term, sort of an operational preparation of the battlespace to be able to execute certain operations to make things difficult, especially difficult for us.

So from your perspective, Ed, as the -- and -- and -- and I hope you'll speak to that a little bit more and elaborate on what you were talking about. But your perspective, Ed, is there a particular emphasis at looking at crisis management and the effects of -- of these cyber-enabled operations in times of crisis that are of concern and -- to your -- your office, and the things you're doing?

WILSON: So we're one department across the interagency, and so we look at this quite often. And so we do tabletops, war games, et cetera. So we look at a threat and how it may manifest and then from whole-of-government perspective and we exercise that. So that's part and parcel to how we handle any type of crisis management.

In cyber, with regards to the threats that's put a lot of emphasis behind the types of threats that we're talking about. And so from a department perspective, with all of our geographic combatant commanders, we include cyber threats as part of our traditional mechanisms that we at the very senior levels look at in terms of preparation and being able to counter and respond to crisis.

So absolutely, it's just part of who -- what we are and who we are as a department. That's our job is to prepare for those moments.

What we see now is the need to be able to handle those types of threats across the interagency. It's not just a Department of Defense job. It's not just a national security problem. But it manifest itself in critical infrastructure segments, et cetera, and so that's why you see a much heavier lift being paid and a much stronger dialogue between DHS and all of the other sector leads in the department. And so -- which is why the secretary has moved us in the direction, Secretary Mattis, in terms of a new agreement with DHS, the Department of Homeland Security and DOD in terms of how we can support DHS in particular with the other departments and agencies in information sharing, understanding threats and the right kind of support to include if there was a crisis how would we respond and bring the weight of the DOD into a crisis response.

VAN CLEAVE: So this something that factors into Chinese planning and operations, Larry? Is there...

WORTZEL: Very much. And -- and -- and that's in a way why I like the idea of cyber-enabled economic warfare. Not all of Chinese penetrations are designed necessarily to attack or weaken the U.S. but there are points in crises -- you know, we have steady-state penetrations that go on all the time. But there are points in crises where suddenly you know space is going to get involved. You know, you don't do global cyber, in a lot of cases, without space.

We know that are critical infrastructure, by their own doctrine, at times as you move into crisis is going to be attacked. So you can sort of use some of this as indications and warnings that there is a crisis or that they've decided to have a crisis. Once the Politburo's standing committee and central military commission make a decision to take some action, it's very difficult -- you probably won't turn it around.

But if you had the indications and the warnings of what it looks like in the cyber domain when they are preparing for that, you -- you -- you have a chance to react and maybe turn that around.

VAN CLEAVE: So, Dan, in Russian planning and thinking, do you see -- correct me if I'm wrong, it looks like they've been using Ukraine off and on as sort of a proving ground for some of the variety of things that they do and their concept of hybrid warfare. Does that fit into their thinking as well?

HOFFMAN: You know, I think absolutely it does. I think we saw Russia deploy the hybrid warfare in Georgia and we've seen it in Ukraine. I think it just highlights the importance of an incident response plan.

We want to deal with these threats in left of boom. And we want to -- we want to detect the surveillance before the attacks take place, and maybe even consider mounting an attack or deter somehow the attack. But you've got to have an effective incident-response plan.

And I think Estonia, which is a place where I've served many years ago, has been absolutely at the forefront of -- they -- of course they were the victims of a massive Russian attack, but they've been at the forefront of helping NATO build an effective national security cyber strategy, including a really effective incident-response plan.

Everyone in Estonia votes online. And so in order to insure the integrity of their voting, they need to have that incident-response plan worked out, and I think that's a good lesson for us in this country as well.

VAN CLEAVE: So incident response is certainly a big part of what...

WILSON: Yes, let me just echo. I think Dan hit on a key point is, it's not just the incident response, but it's seeing eminent threats, understanding the threat as early as possible, being able to message if need be that we see that threat.

But how do we make ourselves in a more resilient fashion hardened systems, whether that's critical infrastructure for the department or national security systems? And then in a worst-case scenario we need to have the mechanisms in place to be able to respond with incidents, response teams, et cetera. So the resiliency in terms of response, and then reconstitution and when required. And so that serves as a deterrent. A -- when we have a viable responses and a response mechanism, and so that's what we're working hard on across that whole full spectrum.

VAN CLEAVE: We've got a few minutes left. I think it would be a good time to open up to audience questions if we have anyone out there who has a question mark there -- a question for us -- for the panel rather. There's a microphone coming and my request to you would be that you identify yourself and ask a question.

QUESTION: Sure. Zach Biggs with the Center for Public Integrity.

I wanted to ask broadly the idea of allowing companies to attack back or to counter attack, which was raised earlier in the panel, and in particular I'm curious what General Wilson thinks of that idea.

But I'd say across the panel, what's the -- the response to the idea that companies might need to attack back, and whether that's a viable option to try to improve the security for the private sector, in particular defense firms?

VAN CLEAVE: Go for it.

WILSON: You lead us and I’ll pile on.

(CROSSTALK)

WORTZEL: I -- I can only tell you that the -- the law enforcement community hates the idea, and -- and so does Justice, but I'm a -- I'm kind of a simple person, you know?

The city in the United States that has one of the lowest home invasion rates is Kennesaw, Georgia, that requires every citizen to have a gun.

(LAUGHTER)

WILSON: Do you live there?

WORTZEL: No.

(LAUGHTER)

WILSON: So I think within bounds -- I think industry, private citizens there should have the ability to defend themselves. I think the -- there is a unique nature within cyberspace with regards to offensive activity. We -- I think you want a stable environment, we want an increase, you know -- the stability within this arena as much as possible.

And so abiding by and reinforcing the norms of behavior that we've sanctioned with the United Nations alongside a whole, you know, other nations, I think is going to be key here.

And so to have industry that is picking up in a kind of rogue environment I think is a -- is a destabilizing influence.

And so I think there's a unique aspect from a government perspective as -- not just the United States but all governments, for security purposes and that's what you see at NATO, that there's nations that have stepped up and said in a collective defense arrangement if we have attacks on nations that we would respond in kind as appropriate alongside other like-minded nations.

And so I think to have stability, to have a -- a -- a variety of industry partners out there taking unique actions offensively may not be in the best interest of -- of the -- of the domain called cyberspace.

HOFFMAN: I'd just add one point there. I'm from Massachusetts. We don't have guns in our houses up in the north like you all do in Georgia.

(LAUGHTER)

But talk -- I'll propose another idea, and I've been -- only been out of the government for a year and a half, but -- but if you want to regulate this a little bit, hypothetically you might have a set number of companies that essentially give the private sector some insurance.

And if you've been hacked, you could go to these companies, present the information you have, and then those companies might be authorized to hack back. It -- it -- this is one that's been discussed a lot. There's been a lot of testimony in the Congress about it. And I think the idea for me has some -- some value, but at the same time, it can't be unregulated. So maybe that's a middle ground between the two answers you've got.

WORTZEL: And -- and I would only add that if -- if you want to back away from my first answer, the -- it -- there's no reason that the Department of Defense and Justice can't go to selected defense industries in black, secret programs and actually deploy defensive systems and malware that -- which would both discourage attacks and would be a little more controlled.

VAN CLEAVE: So we have another question out here?

QUESTION: Thank you. Giovanna Cinelli with Morgan Lewis.

The panel's insights were extraordinary. You talked a lot about external cyber intrusions, penetrations into system.

I'd like to ask you whether you're considering what we call internal threats, which are through the foreign direct investment process moving into the second, third, fourth, even sixth and seventh tier supply chain to come in from within and basically get access that way and allow for external penetrations as well as internal.

How are you looking at that? Is that part of the overall strategic approach?

VAN CLEAVE: Ed, do you want to jump in on that?

WILSON: Yeah, I'll -- I'll touch on it. Won't get into too much detail because that's being worked by the Department of Commerce and others, but the Department of Defense is clearly part of the solution. And so understanding the relationships with mergers and acquisitions, and then how suppliers are providing in the second, third, fourth -- and I highlighted that earlier -- we don't have enough insight at this juncture in many cases. And so the task force that's up and running is one of the key areas that we want to try to really focus on so that we have visibility to the behavior of those sub-tier, the lower, smaller corporations that are providing some of the bedrock in terms of capability.

Secretary Shanahan has spoken on this at length. We see that as a -- an area that we need to improve. So we're in the process of generating some fixes. Those are under deliberation within the Department, and so we've got some work to do.

VAN CLEAVE: Do -- do you also envision a more robust role for the Committee of Foreign Investment in the United States? Might look at some of these larger acquisition issues in more detail?

WILSON: So in general, I mean I think we're blessed with the ability -- we have CFIUS in place to be able to look and be able to put in counters when required. We get approached many times by other nations that are looking to replicate that model.

I think it's a great starting place, the CFIUS -- the construct that's in place within the United States is pretty powerful when used. And so the question is how do we carry it forward in the future?

VAN CLEAVE: Do we have time for another question now – we've got one up here.

And silence.

QUESTION: Sorry.

VAN CLEAVE: That's OK. You need to wait for the microphone. You're doing it right.

QUESTION: Yeah, a cyber threat there.

Fred Roggero with Resilient Solutions.

Just a quick question on the security, or the insecurity of the cloud. If you look at around Dulles and even Manassas, the cloud lives out there evidently.

But have we just created another center of gravity for attack for cyber commerce?

WORTZEL: I mean, I have my opinion, and you know what they say about opinions, but I think the cloud -- because so many of our major software companies have had to turn source code over to both China and Russia to do business there is the most insecure thing you could possibly do, unless you know where it is and you know it doesn't leave -- and the data, the new data laws in China, the new legal restrictions mean that any data stored in China is Chinese data.

VAN CLEAVE: So that does kind of raise the big question about the -- which we haven't had a chance to talk about, and now it's too late, but the whole matter of international standards for the Internet of things, and the whole -- the -- the struggles that are going to go on in trying to define whose laws, who's in control, who's in a power position with respect to data.

Is that something that we worry about?

WILSON: Well, I was just going to add, I think clearly cloud-based technologies, machine learning, A.I. technologies offer a tremendous amount of opportunity, right, so if you're in business, to be able to generate productivity, efficiencies, savings in an operated scale are clearly -- merit the shift and we see high transition in the Department of Defense, we're moving in that direction as well.

The -- the -- the challenge is -- is are we creating additional threats? And so I think the way that you transition to cloud-based technologies has a lot to do with trying to minimize those -- those risks, if you will.

And so looking at qualifying vendors, looking at the way we shape the ability to have insights into how those services are being provided, not leaning on our traditional CSIS-P structures that we would have in a network environment.

I think we need to take a hard look at that, and that's, as you've heard our CIO, Mr. Deasy, has been highlighting with -- with clarity here over the last few months. And we're in the process of moving a large section of the department over the next few years, to cloud-based technologies. And so that's -- that's why we're very, very focused on it.

VAN CLEAVE: Do I have any more inquisitive members of the audience that have something to raise? No? We've got one up front.

QUESTION: Thank you. Jonathan Ward from Atlas Organization.

So I wanted to ask a -- a sort of broad question about what kind of consensus we need, and what kind of, you know, interactions do we need between the national security community and the business community, and also the finance community.

Because I feel like there are still narratives on China that are being spread throughout our society by those doing business in China, that are really actually very counter to long-term U.S. security.

And at what point do we sort of get this broader picture and what kind of consensus does the United States need to address these challenges?

VAN CLEAVE: So, Larry, I think you could take the lead on that one. But...

WORTZEL: Well, I think the chambers of commerce -- American Chamber of Commerce, the U.S.-China Business Council and -- and most of the businesses are more aware of the threats from China.

They've -- all their hopes that they would penetrate the Chinese market, kind of China 2025, took that apart. They're becoming more realistic. They're moving some of their operations into southeast Asia and other places.

I -- broadly speaking, I think across the government, at least -- certainly across the Congress, there's a greater recognition of the problems that exist with China. And I think that's a very good thing. I hope that -- I hope that responds.

VAN CLEAVE: So other thoughts before we wrap this up, on what is required from our private sector?

HOFFMAN: I guess what I would just add on -- on Russia is, I think we have a really effective means by which to share terrorist threat information with the private sector.

When the intelligence community detects that there's a threat out there, overseas or domestically, we share that information so that we don't get to the right of boom-incident response.

And I think we're building the connectivity right now, in the area of cybersecurity. But I just don't think we're quite there yet. And in a sense, it's a little bit of a clash of civilizations because our private sector is wide open.

When you look at some of the social media and networking companies that have been targeted so ruthlessly by the Russians, many of their employees come from those criteria countries like China and Russia.

And if you think that those people aren't under a lot of pressure to share everything they know about everything to do with those companies, it just -- it just creates a -- a real challenge for us, and a lot of work yet to be done.

But I think the connectivity is important, and maybe you could speak to that.

WILSON: So I think fundamentally, we all realize that the homeland is no longer a sanctuary with regards to the threats that we're seeing within cyberspace. And so that's -- that's had -- that's created the -- really, the catalyst for fundamental change that you're seeing across the whole of government over the last several years.

For the department, we've revamped and -- and looked at how to defend forward. It's really -- we offer some unique capabilities and assets associated with that, as well as looking to how can we defend the homeland and be more active partners alongside the Department of Homeland Security and FBI in particular, to be able to counter the types of threats we're seeing.

And so the department is much more active, much more proactive. Though I would describe the strategy as compared to what we've just recently released, it's a much more proactive strategy in terms of trying to get ahead. See the threats, mitigate the threats. And then in worst case, if we have a -- an incident, a significant incident in this country, as being able to respond and mitigate that threat to the best of our abilities.

And so it is a change. We have shifted in a big way. One of the fundamental differences within the department that's different, if you look in the rearview mirror four or five years ago, we didn't have a Cyber Mission Force. The nation made a decision in the 2012-13 time frame, to establish that.

That force has now been built, and now we're in the process of employing it, mostly in the defensive fashion. But when directed, we can flip in the other direction.

And so that's a unique set of capabilities that has come on board and allowed us to be a bit more proactive in this space, alongside the other departments and agencies in the U.S. government.

VAN CLEAVE: So I think time is up.

(CROSSTALK)

VAN CLEAVE: Thank you all so much. I really enjoyed sharing this conversation with -- with each of you.

Thank you, Samantha.

(APPLAUSE)

RAVICH: Thank you, Michelle.

I want to thank the -- the panel. Two quick points from what they were speaking about. One, something that Dan mentioned. You know, could there be a class of companies that would have the ability in the authority to, quote, "hack back?"

I urge you all to take out what I hope is your handy-dandy pocket Constitution. And look at articles -- letters of marque and reprisal which are, of course, in our Constitution, that would be able to grant private actors authority from the government to take on hostile adversaries.

The other thing is, the -- Larry was great and mentioned that we do have monographs -- Juan mentioned as well, on the strategies of -- of China and Russia, and North Korea and Iran.

The Russia piece sometimes gets underappreciated because we focus on, of course, bad actions they're doing in our electoral system and -- and now in the grid.

But there is a significant cyber-enabled economic warfare component in the Russia calculus as well, which we explore in our monograph, "Kaspersky and Beyond," which I -- I urge you to read.

END