Cyber-Enabled Economic Warfare: CEEW Threats from Iran and North Korea

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 Dmitri Alperovitch, Co-Founder and CTO, Crowdstrike, Frank Cilluffo, Director, McCrary Institute for Cyber & Critical Infrastructure Security, Auburn University, David Maxwell, Senior Fellow, FDD; 30-year veteran of the United States Army, Ellen Nakashima, National Security Reporter, The Washington Post

RAVICH: All right. So now, let me welcome our next panel to the stage to discuss the cyber-enabled economic warfare capabilities and strategies of -- of North Korea and Iran.

You know, as we know, both of these nations are subject to significant U.S. economic sanctions. Of course, to change those countries' policies and strategies and orientations.

So you have to wonder, at what point -- if you're an adviser in -- in Tehran or Pyongyang, you know, you say to your boss, "Hey, boss, you know, we -- we have to be -- how can we change this? You know, we're under sanctions and they're constraining our economic capability."

You know, "What can we do? And now potentially in cyber, we have the capability to do it -- to constrain America's economy in order to change the decision calculus in Washington?" Right? So that's the -- that's what we're going to explore now.

So I'm going to turn it over to Ellen, national security reporter with The Washington Post, to draw out what cyber-capabilities and cyber-enabled economic warfare look on the Iran and North Korea front. Thank you.

Ellen? Thanks.

NAKASHIMA: Thank you, Sam, for that introduction. And as we are the last panel before lunch, I see some -- see it starting to empty. Maybe everyone should just stand up and stretch and do a couple of jumping jacks first and then we can start.

But I'd like to quickly introduce my panelists here. We have to my immediate right David Maxwell, a senior fellow at FDD who served for 30 years in the U.S. Army, including as Director of Plans, Policy and Strategy and the Chief of Staff with Special Operations Command Korea.

Frank Cilluffo directs the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University and was recently appointed to the congressionally mandated Cyberspace Solarium Commission. And to his right is Dmitri Alperovitch, co-founder and CTO of Crowdstrike and a thought leader on cyber security strategy and tradecraft.

And as Samantha mentioned, our panel will focus on the other two of major competitors or adversaries with the U.S. in cyberspace. You heard about Russia and China earlier, we'll talk now about North Korea and Iran and the way in which they conduct their cyber operations to advance their interests, the extent to which those undermine -- those activities undermine U.S. economic and national security, and then strategies to counter that maligned influence.

I thought I would start with you, David, to give us a brief overview of -- of North Korea's cyber operations, who's conducting it, who their targets are, what their aims are and what the -- from a threat perspective, the impact is on our economic and national security.

MAXWELL: Well that's a lot to cover.

NAKASHIMA: A lot to cover in two minutes, but you can do it.

(LAUGHTER)

MAXWELL: OK, all right, well first let me acknowledge my co-author and colleague Mathew Ha. Only one of us could be up here, and I think we flipped a coin and I -- and I won, so Mathew was really the backbone of -- of our report here, so let me acknowledge -- acknowledge him.

You know, the World Economic Forum yesterday published a report that said it's like cyber attacks is the biggest concern among business leaders -- some 12,000 business leaders in 140 countries, you know, in Europe, Asia, and North America.

So I think it's pretty timely that we're -- we're talking about this. And of course General Hayden wrote this morning in an article in Cipher Briefs that the cyber cavalry is not coming to your rescue. So I think -- I think that's very, very important.

Although North Korea's cyber capabilities do not match Russia and China perhaps, we should expect that they are going to continue to develop and improve. Eli Cohen and John Gooch wrote a book about military failures, or in this case, national security failures.

And all failures are a result of failure to learn, a failure to adapt and a failure to anticipate, and our report is really about anticipating what -- what might occur. And of course John and Juan talked this morning about failure of imagination.

I think that's another way to look at -- at the failure to anticipate. And so the six case studies we look at, you know, are really characterized as -- as cyber attacks, economic attacks, cyber terrorism. Of course we talked -- we heard about Sony this morning, we can talk more about that -- cyber extortion, cyber-enabled theft.

Again, we heard about the $81 million stolen from Bangladesh and -- and the like. So North Korea is conducting cyber heists, and really it's only a matter of time before they go from really trying to make money to being able to use their capabilities to support other -- other operations.

And I'd -- you know I'd -- I would not -- I'd look at this as North Korea really mapping the cyber battlespace, mapping the terrain for future exploitation. We haven't seen significant attacks yet -- I mean Sony's significant, $81 million is significant, but really not significant direct attacks against the U.S., U.S. government, and the great majority of attacks are of course against our ally, South Korea.

And so I think it's really important that we look at -- at North Korea's use of cyber through its strategy.

NAKASHIMA: Yes.

MAXWELL: And you know despite -- you know the – maybe peace is breaking out, although after reports of the 13 missile sites this week and the criticism of -- of our -- our talks with North Korea, you know we still need to consider its strategy.

And its strategy has really long been based on, you know -- for seven decades on achieving dominance of the Peninsula. You know, ultimately unification under northern control through the use of subversion, coercion, extortion and use of force to unify the peninsula to ensure regime's survival.

And so, subversion, coercion and extortion are all elements of its strategy, and of course cyber can contribute to -- to each of those. And I think those case studies that -- that we've outlined in our report do illustrate various forms of that.

So I'll -- I'll stop there ...

NAKASHIMA: Great, so from a cyber perspective, their primary target at this point is -- is their neighbors to the south, South Korea, and what -- what they're doing right now is primarily income -- revenue -- revenue generation throughout -- throughout the world through the cyber heists and Bitcoin.

But they could possibly elevate -- move on from there to more destructive attacks.

MAXWELL: You know, I think you -- you see really from -- as they've evolved, they keep getting better and better.

NAKASHIMA: Right.

MAXWELL: And I think that -- you know again, it's only a matter of time before they expand and of course if there's conflict or anything like that, we should really expect that they're going to exploit their capabilities.

NAKASHIMA: Thank you. Frank?

CILLUFFO: Thank you Ellen, and -- and like David, I'd want to be sure to underscore and -- and -- and thank my co-author for this, Annie Fixler. She clearly was the backbone for -- for our paper, as well. A pleasure to be here.

A couple of points I want to pick up, sort of maybe do a little compare and contrast...

NAKASHIMA: Absolutely.

CILLUFFO: ... with North Korea and then go into Iranian intentions and capabilities. I think first and foremost anyone analyzing, assessing and evaluating the intentions, capabilities of our cyber adversaries, it cannot be divorced from understanding the geopolitical objectives and aims any of these adversaries have.

So cyber's a tactic, a cheap one relatively speaking and a technique and a procedure that allows them to achieve whatever military, political, or economic objectives they may have. So I think that often gets lost, and -- and that's one of the really challenging issues when the government tries to get the -- the right people around the room to tackle these issues.

You need to have a -- a -- regional expertise and you need to have cyber expertise, and -- and I think one of the things that FDD did really well was bring people with all those backgrounds together. So I think a hat off to them -- there are a lot that have geopolitical, there are a lot that have cyber, but rarely do the two come together.

NAKASHIMA: Right.

CILLUFFO: Secondly, I think that when you think cyber, technology changes, will continue to change. There are going to be those that are first adopters, whether it's in a -- in an economic sense or an adversarial sense, but human nature remains pretty consistent.

So when thinking about -- about the Iranian challenge, they have long turned to asymmetric means to achieve their objectives. They've long turned to proxies to achieve their objectives. Just think of Hezbollah, to a lesser extent Hamas.

Cyber is a new way for them to be able to achieve some of the objectives they perhaps can't militarily, economically or diplomatically. So a long-winded way of saying history may not repeat itself, but it tends to rhyme, to steal a phrase from Mark Twain, and when you look at Iran's intentions, there are -- they're escalating pretty quickly.

So they're by no means on par with Russia and China.

But they don't have to be. To have a drive-by shooting capability, you don't need to integrate it as fully as maybe Iran or China are, into their military strategies, doctrine and war-fighting capabilities.

So I think we need to appreciate that the old way of thinking about how you rack and stack adversaries doesn't fully add up in cyber. Because you need that one-time drive-by shooting capability.

The truth is, is Iran is spending a lot of money on cyber. They've spent a lot of time, and they are starting to integrate electronic warfare and cyber means in their -- in their military strategy.

So -- and -- and I think we tend to dismiss the threat when, in reality, I think we need to think about it a little differently. So cyber-enabled economic warfare in particular.

I -- I mean, if you think about their big -- their first series of -- of major attacks, it was on the U.S. banks. No surprise there. Ostensibly, in response to what was allegedly a U.S. operation with Stuxnet, they immediately went to hit the U.S. banks.

They followed that up also in 2012, with cyber-enabled attacks on, what, Saudi Aramco. Again, banks, energy. Both economic targets. Both had significant economic effect. And it fulfilled their broader objectives beyond just the -- the -- the cyber-enabled means.

And then they also went after one that also had a dual effect in terms of Sands Casino, because they were upset with Adelson, and -- and they also had the effect of turning computers into bricks.

And the Saudi Aramco case, by the way, that was over 30,000 computers that were turned to brick. So relatively significant at that time.

Let's fast-forward to this past year. So the Saudi Aramco attacks were Shamoon. Shamoon 2, more recently -- not necessarily a much more sophisticated attack. But what they've been able to do is cobble together tactics, techniques and procedures that others have engaged in, and put that into one place.

So they'll take other people's techniques, tactics. And in this case, that is relatively unique. Because normally, you can -- it's pretty easy to identify who the perpetrator is, based on modalities and tactics they've used.

This was a cobbling together of different techniques. And -- and quite honestly, I believe it was actually intended to be a dry run. I didn't think it would have as much effect as it actually had initially.

And this is David's point. And, Ellen, you put a -- a fine point on this. All of these countries -- Russia initially looked to Estonia, now they're looking to Ukraine as their practice field.

The North Koreans look to South Korea and Japan as their practice fields. Iran has looked extensively to Saudi Arabia, UAE, increasingly other North African and Middle Eastern countries as -- as their practice field. China's looked to everyone as their practice field.

But the bottom line is -- is, these are all movies that are coming to a theater near you. They're using it to refine their tactics. They're using it to refine their techniques. And I think Shamoon 2 did show an escalation in terms of capability, that we shouldn't dismiss.

NAKASHIMA: Who -- where -- where was Shamoon 2 targeted, at who?

CILLUFFO: Saudi Arabia. Sorry...

NAKASHIMA: Saudi? OK.

CILLUFFO: ... so this was phase two. And -- and it was a combination of different TTPs they've used, and other...

NAKASHIMA: OK.

CILLUFFO: ... tactics, techniques and procedures in other environments.

NAKASHIMA: Thank you.

CILLUFFO: I've gone on way too long.

NAKASHIMA: No, no, no. It was great.

So -- So, Dmitri, you get the hard part. Integrating the two very excellent overviews, can you compare and contrast these two near-peer adversaries in cyber, in terms of their -- their tactics, their capabilities, their aims and their impact on...

ALPEROVITCH: Yeah.

NAKASHIMA: ... our national and economic security?

ALPEROVITCH: Thank you for having me. I would say -- I would not necessarily call them near peers. The North Koreans have actually been interested in cyber for almost 30 years.

So it goes all the way back to 1990 when Kim Jong Nam, the now-deceased half-brother of Kim Jong Un, who was assassinated in the airport in Malaysia, started the Korean Computer Center in Pyongyang and started to gather elites to study computer science.

And later on, many of those people went on into various institutions within the Korean government, and were forming their initial cyber forces. So they've been interested in this for a very long time.

And I would actually call -- despite the fact that they may not have the technical sophistication of Russia, China or, certainly, the U.S., I would call the North Koreans the most innovative threat actors in cyberspace.

If you look at what they've been able to do over the last two decades, they've really, in many ways, pioneered the tradecraft that others have adopted since then. They were one of the first ones to use destructive cyber-attacks, going all the way back to the mid-2000s, against South Koreans. They've targeted -- government networks have, targeted critical infrastructure networks -- media, banking and energy. They've leveraged botnets -- excuse me -- they've leveraged botnets very extensively for their attacks. Yeah.

And of course, with Wannacry, they were one of the first nation-states that were (ph) to actually use a global worm capability as a disruptive attack. And they're using cyber-crime as a way to actually fill in the coffers of many of these agencies.

Just as an aside, it's really interesting to know why exactly they're -- they're executing these financially motivated attacks. Of course, it is to -- to support the regime. But more specifically, it's actually to fill in the gaps in budgets at these agencies.

They're executing these attacks, because in North Korea, unlike in other countries, if you're in a military intelligence agency or civilian intelligence agency, you're given certain missions and priorities, but you're not necessarily given the full money to support those missions. But yet you're still expected to execute on them. So you have to fill in the gap somehow.

And as a result, we've seen over the course of many decades, the North Koreans use counterfeiting and drug trafficking, weapons trafficking, and now cyber as a way to compensate for those gaps and -- and make up for the -- for those shortfalls.

In terms of the primary threat actors, they're actually a number of them in North Korea, one of the main ones is RGB, their military intelligence agency. So roughly equivalent to the GRU in Russia.

You also have MSS, Ministry of State Security, the largest SIGINT, signals intelligence agency. And then you have the general staff department that is part of their military leadership, that would really focus on cyber in times of war.

Most of the attacks that we have seen on Sony and the like are believed to have come from RGB and -- and units -- Bureau 121, famously -- within -- within RGB.

But this innovation that we've seen from the North Koreans has really been adapted by many other nation-states. So when you look at -- as Frank mentioned -- Shamoon, it came a number of years after the North Koreans first tried destructive attacks.

And in some ways, borrowed some of the trade craft, whether there was overt communication or not. They certainly paid attention and -- and adopted some of those techniques.

So in many ways, North Korea is a trailblazer in cyberspace, for other nation-states including those, frankly, with -- with more sophisticated capabilities.

So for now, of course, they're in a charm offensive this year. I -- I expect that it'll come to an end, probably next year, as they have shown zero interest in dismantling their nuclear program, and I expect that -- that to come to a head with -- with the -- with the United States sometime next year, and we'll start to see a resumption of offensive attacks from the North Koreans.

They've never really stopped the financial theft they've been engaged in, but the more overt destructive attacks...

(CROSSTALK)

NAKASHIMA: Has -- has that financial theft really affected the U.S.?

ALPEROVITCH: You know, for the most part they targeted sort of easy pickings. So they've targeted large financial institutions in other parts of the world -- Bangladesh, Chile just got -- recently in June was a -- an attack where they infiltrated the banking system Bank of Chile, stole $10 million, and then destroyed the network of the bank to make forensics really, really difficult.

NAKASHIMA: So why have they targeted or been able to get to U.S. financial institutions? Because our banks have good defenses or ...

ALPEROVITCH: I -- I actually think that the North Koreans -- you know, we -- we always talk about them as -- as this reckless actor in the -- in international affairs.

I actually think that they have probably the -- the most brilliant foreign policy of any nation, because for the last 70 years they've been able to achieve literally everything they ever wanted without giving an inch by knowing how to use blackmail to maximum effect and walks up right to the line without crossing it and endanger the regime.

So when you look at what they've been doing with the U.S., they've actually been extremely cautious, right? So they -- they've never really launched destructive attacks against the U.S., Sony aside, where you could argue that was a personal affront to the leader, and, frankly, Sony is a Japanese company after all.

But you know, in terms of even kinetic actions, we've seen them shell islands, we've seen them try and sink ships, never really the United States -- against the United States. So they've been very, very cautious I think for many, many years in terms of provoking the U.S. before they were fully ready with their nuclear delivery capability to deter us.

So -- realizing that a war with the United States is not in their best interests. So I do think that they will remain cautious for the -- for the foreseeable future in terms of attacking the homeland, unless they believe war is imminent.

NAKASHIMA: So in terms of our economic security, North Korea's not as great a threat as, say, Iran, in your view -- your -- either one?

CILLUFFO: No, it -- absolutely, and -- and one thing -- cause this came up in everyone's remarks and it came up earlier, but I think it's worth sort of highlighting.

The truth is if you can exploit, if you're involved in intellectual property theft, if you're involved in economic and or military or industrial espionage, if the intent is there you can also exploit, cause what makes this a little -- I mean attack -- what makes this a little different is the -- the exploitation medium can easily be utilized for an -- an -- an attack medium.

So I think again -- and it's not to overstate this point, but you can't look at cyber as a black magic away from everything else that these countries are intending to do.

NAKASHIMA: So what Dmitri seems to be saying is the intent from -- on -- on the part of North Korea is not there yet -- yet.

CILLUFFO: I'm not sure I fully -- I -- I love Dmitri and we agree on almost everything, but -- but I think that -- I think Sony was a pretty -- and it was Sony USA that was actually hit. It was a pretty destructive and disruptive attack and I -- I actually think the SWIFT hacks did affect the global market.

And the big concern I have with banks is not the attack -- not the 9/11 equivalent, I'm more worried about erosion of trust and confidence in the system, and -- and SWIFT really is that single point failure that all financial institutions and central banks depend upon -- are 100 percent dependent upon.

So I -- I -- it's not that I disagree with Dmitri, I think that we have a little different accentuation. But the one point I do want to say is Iran has been comfortable engaging in disruptive and destructive attacks, just as they have been very comfortable in engaging in terrorism.

ALPEROVITCH: And I -- and I would add that on Iran specifically, now that JCPOA has been torn apart and the sanctions are back in place, we certainly expect that the disruptive attacks and other types of destructive attacks, primarily probably against our financial sector, would resume once again as -- as they had launched them back in 2012, 2013 time frame.

They stopped when we engaged in negotiations. I think now that's a naturally way for them to head back ...

CILLUFFO: Stopped against the U.S., not globally.

(CROSSTALK)

NAKASHIMA: David?

MAXWELL: Yeah, I -- I -- Dmitri makes a great case, but I -- I would be hesitant to accept that and you know, Sun Tzu said, you know, never assume the enemy's not going to attack, you know, make yourself invincible.

And I think as we continue our maximum pressure -- and it's going to be maximum pressure from the United States -- at some point, I think we should expect more aggressive attacks by North Korea against -- against the United States.

And you know -- and one of the reasons I think is that, you know, we rarely responded to North Korea with any kind -- I mean the last time we responded, the last really kinetic action against the United States was 1976, and we responded with a pretty strong show of force.

And so, you know, since then -- I mean now -- Sony attack now, we've just indicted Mr. Pak there four years later, which I think illustrates -- and I'd defer to you on how -- how difficult it is for attribution, you know, and why it took that long to -- to do that, so ...

NAKASHIMA: Remind the audience who he was, this ...

MAXWELL: Well he is a computer programmer from North Korea who was indicted in September by the U.S. government for the Sony hack.

NAKASHIMA: I think the first time the U.S. government has obtained such an indictment against a North Korean ...

MAXWELL: Against a North Korean as -- as far as -- as far as I know, yeah.

(UNKNOWN): But they -- they did sanction people ...

(CROSSTALK)

... Sony, so -- cause the -- cause the indictment comes much later, it does not necessarily mean that they didn't know ...

MAXWELL: Sure, sure, but I think -- I think it would be -- we would be remiss in -- in -- you know, in ruling out the possibility and I think in North Korea -- and again, Dmitri has pointed out they are very adaptive and innovative.

And I think that -- that we need to expect that and prepare for it.

NAKASHIMA: Is it possible their restraint is a result of these sanctions or ...

ALPEROVITCH: I -- I think -- I think they're concerned with one thing and one thing only, which is regime preservation and until they're confident that they have the capability to actually land a missile in the United States with a nuclear weapon on it -- which they're not yet there, but close, I think they will continue taking a cautious approach.

Now, once they do that -- and I think that the greatest problem with nuclear non-proliferation in North Korea is not that they're going to actually launch a nuke at us, but that will give them a complete free hand at launching all types of attacks, including cyber, without fearing that we would launch a kinetic -- kinetic action response.

CILLUFFO: Just to -- I -- I agree. So I probably know the least about North Korea, and every time I try to think about them, my head hurts.

(LAUGHTER)

But -- but the reality is -- is that is the only prevailing set of issues -- its regime -- is to maintain the regime and ensure its survival over the long-term. And right now, cyber crime is -- I mean they're being cut out of the global market.

So I mean what they were doing in terms of their super bills, those were the most sophisticated counterfeited bills that the U.S. had seen ever, and that's North Korea that came up with it. They were smuggling it through diplomatic pouch, so you can't separate the state from the criminal activity.

And they are a state sponsor of crime, so there might be a -- a -- a decision made where the -- maybe we're really ramping up some of our -- our security efforts, where they -- they could turn to destructive attacks. But -- but I think by and large, they'd be biting the hand that feeds them because it's been a very successful corporate operation.

MAXWELL: But I think it fits into a -- you know, a -- its other asymmetric capabilities. You mentioned counterfeiting. Counterfeiting cigarettes, counterfeiting medication.

(CROSSTALK)

MAXWELL: You know, the slave labor trade around -- you know, that it's conducting all of these. You know. And then you said, cyber is a tool, you know, a tactic...

NAKASHIMA: Right.

MAXWELL: ... and so I think that you know, going against American financial institutions, I don't think it's out of the question because I don't think that they expect a decisive response from us.

I think that's one of the things -- you know, we talk about...

NAKASHIMA: Yeah.

MAXWELL: ... a decisive response, but are we really -- you know, and have we demonstrated that we're willing to do that. And so I think that without that, that will embolden them over time.

NAKASHIMA: Yeah. That's always a big question in cyber, right, is the decisive response. But what does that look like? What -- what do you all, as experts, think a decisive response would look like, that wouldn't invite undue escalation that we cannot dominate in the U.S.?

CILLUFFO: Start with Dmitri. This is my...

ALPEROVITCH: Go ahead.

CILLUFFO: No, you start, you start. I'll try to be quick.

ALPEROVITCH: Well, I think any time we look at cyber-attacks and we're thinking about response, we should not be limiting ourselves with -- with cyber-response. Nor should we even, perhaps, start with a cyber-response...

NAKASHIMA: Yeah. We've had indictments and...

ALPEROVITCH: ... we should be looking at...

NAKASHIMA: ... and sanctions, right.

ALPEROVITCH: ... what -- what objectives we want to achieve. And you know, that can include anything from military to sanctions, indictments and everything else in the toolkit.

Of course, the challenge with North Korea is that our primary problem with them is not cyber, not even close...

NAKASHIMA: Exactly.

ALPEROVITCH: ... it is the nuclear weapon program. And we have not been able to, so far, make a whole lot of progress on that front. So our levers of power against them are extremely limited, short of going to war.

The Chinese are not willing -- and I would argue also not able, really, to do a whole lot to put pressure on them. And as a result, you have a regime that really can continue doing what it wants without much repercussion, knowing that only if they trigger that red line, whatever it may be -- though (ph) it provoke a kinetic response, would they actually be in danger.

CILLUFFO: Yeah. I -- you know, the reality is is, what cyber-deterrent strategy do we have. And -- and there have -- and the -- everyone's been recognizing the fact that we need to ensure that there are consequences on bad behavior.

But it's not just the perpetrator of that particular incident. Everyone else watches how you respond. So right now, whether it's Russia, whether it's China, whether it's North Korea, the U.S. doesn't have a very effective narrative. And there have to be consequences on bad behavior.

NAKASHIMA: Right.

CILLUFFO: And to me, it's a dissuade, deter, compel. Obviously, you don't want to limit it to cyber. But cyber needs to be visible. I mean, what is the nuclear test equivalent for cyber? I don't know. But we need to start thinking about some of these things a little differently.

And -- and right now, we're blaming the victim. I mean, the reality is, we're blaming Sony. We're blaming JPMC.

NAKASHIMA: Yeah.

CILLUFFO: We're blaming -- and -- and I'm not suggesting companies shouldn't do more. They must. But the reality is, is we have to start articulating or going beyond the nouns into the verbs, and ensuring that there are some consequences for bad cyber behavior.

And that's across the board. Whether any of the countries we're discussing here, and every other country that has a modern military, has a cyber capability.

NAKASHIMA: Yeah. I think you all may have a raised a good point, here, though, which is that the main problem with North Korea is not cyber. It's -- it's the nuclear -- the regime issue.

Until that gets solved, I mean, you know, you're always going to have a cyber problem. And you -- one might argue that the cyber, the nuclear test equivalent in cyber is Stuxnet (ph).

But what -- what that, you know, generated was then a -- sort of a new arms race, and a lot countries then started building up their own cyber-offensive capabilities.

But anyway, let's move to Iran for a minute here.

The last disruptive attack against the U.S. was I think -- Frank, as you mentioned, 2012, with the DDoS's against the banks, right?

CILLUFFO: It continued through 2013 and all the way ...

NAKASHIMA: OK, and then there was the stands (ph), yeah. But tell me, what -- what was the intent of -- of that operation? It didn't really -- it didn't -- it didn't destroy anything, it was public facing systems, it didn't -- they didn't -- well they -- they lost some hundreds of millions of dollars I guess too, but what was the intent?

Was it saber rattling? Was it to say this is what we can do, beware, we have more capabilities ...

ALPEROVITCH: I -- I think that this was their thinking about an asymmetric -- a symmetric response, a proportional response to what they felt was economic war -- warfare launched against them by the United States in terms of sanctions, really choking off their economy and they're saying well, you know what, you're going to do that to us we'll do -- we'll try to do something against your economy and target a financial system.

Of course it wasn't very effective, the DDoS attacks were mitigated very well by most of the banking institutions. I think that the Iranians probably thought that -- that the attacks were a lot more effective than they -- they were in -- in response.

And you know how it is in -- in big bureaucracies, you may have people that are launching those attacks that are reporting up and telling the leadership how great this is, but not necessarily that being the reality of the situation.

But Iran -- Iran is quite different from other countries in the sense that a lot of their activity is being launched by contractors. So not necessarily military and intelligence officials like you would have mostly in Russia, China and North Korea, but companies that are working on behalf of the two primary actors in Iran, IRGC -- Iran Revolutionary Guard and MOIS -- Ministry of -- of Intelligence.

And those people have some level of concern because they tend to travel, they -- they tend to get educations in lesser (inaudible) countries, as well as UAE and other places. You regularly find them in Dubai attending conferences, and then they go back and start companies.

And they do a variety of things, some -- some of -- some of their efforts are focused on cybersecurity efforts, and they're also moonlighting for the government in offensive tradecraft, as well.

And as a result, you have a little bit of a separation between sort of the orders going out from the regime saying go do this and what actually happens with these contractors and -- and the level of control probably is not as tight as -- as it would be in other countries.

CILLUFFO: You know -- now I wouldn't dismiss the impact those DDoS -- they were the most sophisticated at that time, Distributed Denial of Service attacks, and -- and when people thought cyber disruptive weapons, that's what they were thinking at that time.

There's also some indication that maybe that was even a diversion, that there were other activities going on at that time as other actors have done when they have engaged in DDoS sorts of attacks. But it was -- the -- the thing is is I wouldn't compare-contrast Stuxnet to -- Stuxnet was -- if the U.S. had any involvement, I -- I don't know, but if -- it was very discriminate.

It was going after a nuclear set of capabilities. Iran's response was quite indiscriminate, it's going after our economy. So when we start thinking of proportionality, there are certain things that don't add up and aren't equal, and I think we just need to think about it.

I don't think actors like Iran would have any concern about targeting some of the more socially unacceptable targets.

NAKASHIMA: In terms of the response though to those DDoS', I know the banks were divided. Some of them felt that the U.S. Government should have done more, taken a harder stand and others felt that ...

CILLUFFO: If it happened today we would. So, in a weird way, that was, at that time, it was an effective attack from Tehran's perspective. Did it have long term implications? No. It actually -- but it still signaled what they wanted to signal and that was that, hey, we're here, we've got a capability and everyone's potentially a target.

The other thing that I would say, and Dmitri's very right in that, so the IRGC does over -- have a -- play a major in Iran's offensive cyber capabilities and we lay out some of the actors and who they are in our paper, but there was a big -- so they initially focused all their efforts on their own population.

So, think back to the Green Revolution, how aggressive Iran was going after their own -- trying to disconnect the people of Iran from the rest of the world and the activities that were occurring at that time.

So, at that time Iran -- the IRGC had a hard time pulling in all of these hacking communities that existed for many years. Ashiana network, there many that were -- that exist and they were quite good, but then they've recently started focusing their efforts a little more externally as well and IRGC, in essence, took control of all these, what were at one time, autonomous and independent hacking communities. There was a question whether or not they'd be able to pull that off, and sadly, I think it's fair to say they pulled it off.

So, moonlighting maybe, but when they need them they're there.

NAKASHIMA: Yes, and so does the fact that these hackers who moonlight, like to travel? Does that suggest another way to get at the deterrents or response in punishment by say, sanctioning or indicting these people who may, in fact, want to travel out of Iran? So, give us a bit of leverage.

ALPEROVITCH: Well, we were at an event last week with John Demers, who is the Assistant Attorney General for National Security.

He was talking about this very issue, that indictments probably would have a very hard time deterring people that are actually working for Foreign Intelligence Services and militaries, just like if our intelligence professionals were indicted in China, that would not stop their work and would not have any impact on their ability to execute the mission.

But contractors probably would think twice because they're not in uniform, they're not getting the orders, they do have a right to not take contracts and for them it's much more of a financial gain, cost reward analysis, and that might deter some of those players from participating in the secret (ph) system.

CILLUFFO: Absolutely. It's been very -- I, so -- I think it does have a significant effect on those that may engage in such activity, because we have become quite creative in terms of finding countries where we have extradition treaties and being able to get people over there, about three cases ongoing right now.

Russia got so concerned that they put out a travel warning to their hacker community, an official travel warning, saying don't go to country -- don't visit countries that have extradition treaties with the United States. So, it does have some effect, but not only in Iran, but in North Korea.

So, most of their operations are being driven not out of Pyongyang alone, but China, Southeast Asia, so there are opportunities to pluck these individuals and use law enforcement as an instrument.

MAXWELL: And I think another way to respond to that is, those countries that host networks, we really need to pressure them to dismantle those networks, not familiar with Iran as much, but certainly North Korea operating outside in China and in Southeast Asia, really need to pressure those countries to dismantle those networks.

NAKASHIMA: Have we begun to do so with China, with respect to North Korea ...

MAXWELL: I am not aware of -- of any -- any attempt to -- at that.

ALPEROVITCH: I -- I don't think China has a lot of incentives to help us right now.

NAKASHIMA: OK. What -- what kind of leverage the -- does the U.S. have against Iran right now, do you think, to prevent destructive cyber attacks, now that the most crippling sanctions have been re-imposed?

ALPEROVITCH: Well, ironically, I think the threat of sanctions probably was a deterrent effect that is now gone now that they're back in place. You know, what else can we do to them?

Perhaps escalation of sanctions, although they're -- they're already pretty tough and the administration is talking about making them even tougher. And at that point, once you reach the limit on that, your only option is war. And I don't think a lot of people have an appetite for that.

NAKASHIMA: Do you think...

CILLUFFO: There are discriminate techniques, tactics and capabilities that can be brought to bear. And -- and when you think about -- just think about the sanctions discussion. It used to be you sanctioned a country, now you can continue to do that, but you can also sanction individuals ...

NAKASHIMA: Right, with ...

CILLUFFO: ... personalize it, and there are ways where you can tighten some of those screws. I know that Mark at FDD has been doing some very good work on some of the SWIFT activity in terms of way you can be discriminate and calibrate some of your responses there.

So I wouldn't say that we're out of options, I -- and -- and short of actual military conflict, but we do have to be creative ourselves in terms of how we make an impact.

NAKASHIMA: Can we really -- can anyone think of anything creative that would work with Iran, or even in the cyber realm, that -- something that would be discriminate, proportionate and not be unduly escalatory?

CILLUFFO: Well the -- we do it all the time with ...

NAKASHIMA: With demarches ...

CILLUFFO: ... different sorts of activities. So part of it is -- and ...

NAKASHIMA: But that would be effective, I mean ...

CILLUFFO: Yeah, that's -- that's -- that's a longer conversation.

ALPEROVITCH: Well look, I mean we -- we have a bigger problem with Iran being a sponsor of terrorism and we haven't been able to do a whole lot in deterring that activity in -- in certain areas like activities in Syria and Yemen and other places. So ...

NAKASHIMA: Exactly.

ALPEROVITCH: ... those would be much higher on the priority list than -- than probably most things that would be in cyber.

CILLUFFO: I actually agree.

NAKASHIMA: With -- I wanted to get in a quick question here about influence operations. We know Facebook recently took down a number of Iranian-linked or Iran-linked accounts before the midterms.

How concerned are you about Iran beginning to move into this world of cyber-enabled influence operations and what would they be taking a page from Russia -- what do you think?

CILLUFFO: I think every country's thinking about this right now, and -- and -- and Iran's been doing it in one form or another for a number of years, long before Facebook. So the reality is -- is I don't think -- just like you can't separate cyber from overall geopolitical ...

NAKASHIMA: Right.

CILLUFFO: I don't think you can separate the perception, management, psychological operations and information operations element from the cyber equation. We play by queen's rules, but no one else really does.

And if you actually look at what Russia -- I think cyber is a piece of their broader information warfare campaign rather than the other way around. So should we be concerned? Absolutely. Is it only Iran? Heck no.

NAKASHIMA: Yeah.

MAXWELL: And I think we don't see North Korea conducting influence operations so much against us -- social media, but certainly against South Korea. We don't see that in the Korean language (ph) since we -- and so that's ongoing.

Now, I -- I would say that North Korea is becoming more sophisticated. I know at the Committee for Human Rights in North Korea, a subject of -- of a lot of phishing attacks -- suspected North Korea and North Korea is suspected of defacing the -- the -- the website, but the staff notices their improved English and improved sophistication and it may be only a matter of time before we see North Korea trying to conduct influence operations beyond South Korea and so I think we have to be - to be on the lookout for that as well.

NAKASHIMA: Dmitri, any thoughts on that?

ALPEROVITCH: No, I would agree with that by the way that one interesting point about the North Koreans is that they've been having a dedicated effort of actually attracting foreigners to come into Pyongyang and teach courses at universities. I actually know some Americans who have gone over there to teach computer science of all things.

In fact, training perhaps the future generation of cyber warriors that will be used in action against us.

NAKASHIMA: OK, so I think we may have a few minutes now to get into questions from the audience and we have I think microphones coming around and if you could first introduce yourself and then ask a question. OK great.

QUESTION: Is this on?

(UNKNOWN): Yes.

QUESTION: OK. From the Wilson Center.

What -- question was also relevant for the last -- the previous panel, what does this panel in Iran or North Korea sound like when it considers the American threat -- the American cyber threat and how should that influence our policy? This is not a one-sided game. I mean more than one.

MAXWELL: Well certainly North Korea would view this as part of our hostile policy. You know that we recognized their cyber capabilities and the fact that we might consider offensive cyber operations against the North. You know they would view this as very hostile.

I think it's interesting to look at the Panmunjom Declaration (ph) in April and the North and South agreed to cease hostile activities in all domains and then it said including air, land and sea. It did not include cyber and you know whether that was on a mission deliberate or you know just based on an oversight error or I think that the North looks at cyber operations that we've conducted in Iran and you know and any capability that we have would be part of our hostile policy against North Korea. So they would view this I think very negatively.

NAKASHIMA: Anyone else?

CILLUFFO: I'm not in the business of advising Tehran or Pyongyang or Moscow or Beijing, so -- and never will be but, you know, we obviously have a ton of capability in the cyber domain but I would argue we have actually quite restrained in terms of how we utilize it.

ALPEROVITCH: Perhaps overly restrained.

CILLUFFO: What's that?

ALPEROVITCH: Perhaps overly restrained.

CILLUFFO: And I would say clearly overly restrained. So where you will see cyber come into play in a U.S. context is more in combination with other means, so cyber as a component of other sorts of operations. I actually think we need to be comfortable discussing our offensive capabilities, acknowledge that we're never going to firewall our way out of this problem alone. We're never going to defend our way out of this problem alone. Use restraint but when you use it you fight and you fight to win.

And I actually want them worried about U.S. cyber capability. I just wouldn't be all that worried based on the track record so far so I feel like now is the time where we can. So your question I actually think that when they do start really worrying about that I'm feeling pretty good.

NAKASHIMA: Well in fact the Department of Defense just issued a new cyber strategy that talks about persistent engagement with adversaries defending forward and preempting attacks at their source including protecting critical infrastructure -- U.S. critical infrastructure in that way I think that might be signaling to our adversaries that we're willing to be a little more aggressive. I don't know whether we're starting to see the results of that change in strategy yet but you know, time will tell. Yes, in the front row.

QUESTION: Zack Biggs with the Center for Public Integrity.

So I wanted to ask, obviously the parallel between these two countries is their nuclear programs. When you look at Stuxnet which was used against Iran's nuclear program, that occurred a very different time period. Setting aside the technical constraints that might impact the ability to use cyber weapons against the North Korean nuclear program. From a policy perspective, are we in a different environment now? Would something like Stuxnet be a viable technique or tactic now against a nuclear program or has the world changed sufficiently in terms of the view of cyber that that's no longer a viable option?

NAKASHIMA: That's a great question.

CILLUFFO: Really good question.

ALPEROVITCH: Yes, the important thing about Stuxnet, it was never designed nor could it ever have been a way to stop the program. It was a delaying tactic; you know at best the estimates are that it may have delayed them by about eight to nine months. So it's a way to give you space to hopefully solve the issue through other means but it is not a solution in and of itself so that's the best way to think about a lot of cyber capabilities actually.

CILLUFFO: You know I'm going to disagree with a point I brought up earlier, so with myself.

(LAUGHTER)

But not in the way that I really mean. But the reality is I do feel we need to be more forward leaning but we also have to be willing to inoculate others that are not part of the govern -- because the private sector pays for the real or perceived sins of government in any of these cases. So we've got to get to the point where we -- if we launch we better be ready and prepared and do the due diligence and have the responsibility to enhance the security of the front lines in the cyber domain and that's the energy companies, the lifeline sectors in particular -- the most critical of our critical infrastructures.

So I think that the -- your question is a really good one. I don't know whether the U.S. was thinking about some of this activity in Pyongyang of late and either it didn't work or decided it wouldn't work or didn't even think about it but the reality is is I think all conflicts going forward of any kind is going to have a cyber element or dimension to it. I just don't think we should think of it as a silver bullet.

I don't think of cyber as a weapon. I think of cyber as an enabler to do everything we do to doing it better more efficiently sometimes anonymously and we want to play to where we're strong not necessarily where others are.

NAKASHIMA: Yes, I mean the thing about Stuxnet was it wasn't intended to become public -- it kind of broke out and broke loose and then cyber security researchers around the world noticed it and tracked it back to Natanz and figured out it was very likely Israel and the U.S. But you know, I think the main purpose there was to sow confusion and doubt in the minds of the engineers.

ALPEROVITCH: It was an information operations.

NAKASHIMA: It was in information operations -- cyber-enabled information operation, which was working beautifully at least initially, right? And then...

ALPEROVITCH: But there's a limit to that, right? So you know, the goal of Stuxnet clearly, based on technical analysis, was to was to convince the Iranians that their centrifuges were effective and the Iranians actually destroyed more of those centrifuges than the worm ever did, because it actually wasn't designed to cause destruction. But at some point you learn -- right -- so there's a natural limit to how long you get out of operations like this.

So it's not a permanent solution by any means.

CILLUFFO: And by the way, there are World War II analogies where people would jam radar to the point that you think it's just not working. So -- so there is -- whether it was meant to be an information operation or not, it seems to have had that in that effect.

NAKASHIMA: Maybe that's another tool in the toolkit we need to start discussing more publicly in terms of response options.

CILLUFFO: I do think -- I think transparency's a good thing in this case. And don't be afraid to discuss our offensive capabilities. But that's me.

MAXWELL: I think from a North Korean perspective, we think its' too insular, it's hard to penetrate. But I have to believe that we -- you know, there are people that are working on the capabilities to do that. And from policy perspective, if we have the capability, we need to be ready to use it, whether to employ it directly to achieve an effect or from an information influence perspective as well. We really need to keep all our options open from influence to actual conduct of attacks if it's in our interest.

NAKASHIMA: OK. Any other questions from the audience? There's one right there on this -- that.

QUESTION: Thank you. Abe Shulsky from Hudson Institute.

I was wondering in terms of the deterrence aspect of this question whether we have a deterrent, especially with respect to Iran, of actual information operations -- cyber-enabled information operations that would address the public itself. I mean Iran is I think considered one of the most wired -- connected nations in the world in terms of its citizenry. Obviously different from North Korea in that regard. But at least with respect to Iran, would there be possible cyber ways of conducting, you know, old-fashioned sort of information operations, propaganda that the regime might see as sufficiently threatening to it that they would be willing to pull back on other stuff in order to get us to stop?

ALPEROVITCH: Maybe or it may lead to escalation, right? So you never know. I mean, the final problem (ph) with deterrence, it is a game of chicken, right? You're trying to convince the other party not to do something because of repercussions. And really the only way you can do that is by making very clear to them that this is a serious priority for you, perhaps your top priority. And the problem with most cyber actions is they'll -- they never get to that level, right? You know, our main problem with Iran and North Korea are nuclear programs, it's not cyber. It won't be cyber for any foreseeable future, if ever.

So unless you make it your top priority, you really have little chance of deterrence and, you know, probably one of the few, if not the only, examples where we've actually had, at least for a time, successful deterrence was against China in 2015 when we got them for a period of time to back off and not to conduct economic espionage. The only way we got there is the president of the United States came out and said, this is my number one issue with China. I'm not sure I even agreed with him that that's the number one issue with China when we had South China Sea...

CILLUFFO: As a cyber guy, I did, but...

ALPEROVITCH: ... and North Korea and everything else that was involved, but he said at the time, this is my number one issue and he made it very clear to the Chinese. And they started to realize that there would be serious repercussions. Until you make that your number one problem, you're not going to get any deterrence out of it.

CILLUFFO: You know, I -- I -- I agree with --with Dmitri 100 percent. But, Abe, you've done some really good work on deterrence theory historically and -- and -- and information operations over the years. And I think we sometimes get caught up in the technology when it's really what are the intentions and capabilities and how do we figure out the best way to get the outcome we want.

And there's mixed spotty record in terms of where perception management fits into all of this. But here's my one issue, whether it's perception management or whether it's computer network attack or whether -- we've got to get to the point where we don't allow our adversaries and episodes that define strategy.

We're letting the Russians define our strategy. We're letting the Chinese define our strategy. We've got to be proactive and by that I mean it doesn't necessarily mean we're going to find the dupe that does something stupid and we come with the hammer -- cyber hammer immediately.

But we are so -- we're letting episodes define rather than what are our strategic outcomes, objectives and goals. So I feel like we're constantly whip sawing every time there's a cyber incident.

Very thoughtful reporters will call me and it feels like we're having that same conversation over and over. We should be defining that.

ALPEROVITCH: I said this a long time ago...

CILLUFFO: We should be defining...

ALPEROVITCH: We do not have a cyber problem. We have a China, Russia, Iran and North Korea problem, but we (inaudible).

(CROSSTALK)

CILLUFFO: Cyber flavor (ph).

NAKASHIMA: So in other words, we don't need a global cyber strategy, we need a China strategy, a North Korea strategy, Iran strategy of which cyber is...

CILLUFFO: Well cyber deterrence. You need -- you need separate deterring mechanisms around all that and -- and you need a deterrent strategy that cyber factors in and you need a cyber specific...

NAKASHIMA: (Inaudible) cyber is fundamentally a tactic and not a strategy, then...

ALPEROVITCH: We don't have a strategy to deter tank warfare, right, we -- or enable warfare. We think about it as deterring warfare, and cyber is just a tool in a toolbox.

NAKASHIMA: We have time for maybe one more question, if there's anyone out there. Don't be shy. No? Yes.

QUESTION: Michael Martel (ph) from the National Security Archive.

I was wondering if we saw or if you had seen any instances where cyber capabilities were exported out to proxy forces or proxy partners, either by Iran or North Korea?

And in what way you see that potential -- potential shaping power balances in the regions?

CILLUFFO: That's a great question. I don't...

MAXWELL: I -- I have not seen any North Korean use of proxy. I don't know...

ALPEROVITCH: There is a lot less sharing of capabilities in cyber space than you might think amongst nation states. Most hold it closely to their chest. Just like, you know, in other parts of the intelligence apparatus, you don't share your best tradecraft even with your best of friends, right.

For the longest time the British would not tell the Americans all the details about the Enigma project that they had in World War 2. It took a lot of effort to convince them to actually open that up, so this is something that you hold very close to your chest.

Because frankly the more you share it, the more likely it's going to leak and compromise your abilities to execute operations in the future.

CILLUFFO: You know, and I agree with everything that was said by both my colleagues here on that question. But I'm not sure you always know, because I mean countries are utilizing proxies themselves.

And the reality is -- is when you think of the deep web, dark net, obviously they're not going to be selling the most sophisticated TTPs or zero days (ph).

But it's sort of like that Star Wars bar scene, the old Star Wars bar scene. I mean you've got Han Solo, you've got Chewbacca and you've got someone with 11 eyes and you've got someone with 13 feet. And the reality is is they are sharing and they don't necessarily know who those cutouts are.

And it was sort of even in the espionage world, there were days where you had fellow travelers who were dupes. I'm sure you have the cyber equivalent. That's not to suggest that for direct operations I -- I don't know but I'm not sure we would know necessarily if that's existing.

NAKASHIMA: How active is Hezbollah in cyber?

CILLUFFO: So there is a cyber Hezbollah and then there's Hezbollah, the Lebanese Hezbollah organization that is engaging in cyber so they've used it largely for perception management issues right now. Lebanese Hezbollah. Cyber Hezbollah...

ALPEROVITCH: And espionage.

CILLUFFO: And for espionage. They do -- and very targeted discriminate espionage. So but the cyber Hezbollah which is a little more amorphous is quite active, so.

NAKASHIMA: All right, well I wanted to thank the panel for a wonderful, great discussion and the audience for some really wonderful questions. Thanks, everyone.

(APPLAUSE)

MAY: Thank you very much to the panel. I'm going to take just a couple more seconds of your time before you go out to refresh yourself and converse. By the way, I'm Cliff May, and for those who don't know me, I'm the founder and president of FDD. You heard about various reports and we have hard copies of those; we can guarantee the cyber security of all the hard copies so feel free to take some and just to sum up a little bit, you know after World War II American power, American leadership and rapidly advancing technology brought us really an extraordinary period of peace and prosperity.

Now, however our adversaries are attempting to turn our political and economic openness and our high technology against us. In particular they're using cyber means to undercut American industry and innovation as well as to increase their military capabilities and to degrade our military capabilities. So the challenge as great as we have heard today but so is or can be our response, our creativity, our ingenuity.

As just one small example let me highlight a new FDD project, the transformative cyber innovation lab where we are identifying the technologies and policies that can begin to solve the hardest cyber problems. We partnered with industry and government to shorten the lag between idea and piloting and between piloting and widespread adoption of solutions to defend our national and economic security.

The task before us, here at FDD and here in America is enormous and daunting. But each problem we solve is one less avenue for the bad guys to use against us. Before we conclude I want to take a moment to thank the entire FDD staff. Every member of this absolutely extraordinary team, they make this look so effortless but we know how much hard work goes into making events like this a success, so thank you.

And to FDD's investors in the room and who may be watching on our streaming, a reminder that this conference, like all our work is possible thanks to you, only thanks to you. Thanks to your generous and enlightened support and we thank you for that. Let me also take a moment to recognize again Samantha Ravich (ph) and her clear-eyed thought leadership.

She has zeroed in on how America’s authoritarian and undemocratic and un-free adversaries are using cyber-enabled economic warfare and she thought of this long before many others in the policy community understood the scale of the threats that we face. We should all be pleased that she's been recruited to the president's intelligence advisory board and the newly-created Cyber Space Solarium Commission. These tasks will be synergistic with her work here at FDD.

And finally to those joining us here today via our live stream, thank you for coming and for tuning in. All of us at FDD look forward to continuing to work with you on these important issues.

Again, thank you all for your patience and for your attention today. Glad to see you. Thanks.

(APPLAUSE)

END