THE BROOKINGS INSTITUTION

FALK AUDITORIUM

ASIA TRANSNATIONAL THREATS FORUM:
CYBERSECURITY IN ASIA

Washington, D.C.

Thursday, June 14, 2018

PARTICIPANTS:

Welcome Remarks:

JUNG H. PAK
SK-Korea Foundation Chair in Korea Studies
Senior Fellow, Center for East Asia Policy Studies
The Brookings Institution

Keynote Address:

CHRIS PAINTER
Former Coordinator for Cyber Issues
U.S. Department of State

Capabilities and Intentions of Regional Actors:

Moderator:

JUNG H. PAK
SK-Korea Foundation Chair in Korea Studies
Senior Fellow, Center for East Asia Policy Studies
The Brookings Institution

Panelists:

WILLIAM A. CARTER
Deputy Director and Fellow, Technology Policy Program
Center for Strategic and International Studies

SANGMYUNG CHOI
Director and Senior Security Researcher
Hauri Inc. Security Intelligence Research Team

PRISCILLA MORIUCHI
Director of Strategic Threat Development
RecordedFuture

PARTICIPANTS (CONT'D):

Cybersecurity Policy: Best Practice and Shared Challenges:

Moderator:

JAMES BAKER
Visiting Fellow, Governance Studies
The Brookings Institution

Panelists:

KATHERINE CHARLET
Director, Technology and International Affairs Program
Carnegie Endowment for International Peace

JONG-IN LIN
Professor, Graduate School of Information Security
Korea University

MICHAEL SULMEYER
Director, Cybersecurity Project,
Belfer Center for Science and International Affairs
Harvard Kennedy School

* * * * *

P R O C E E D I N G S

MS. PAK: Thank you for coming today. It's a great crowd and I am so pleased to see you. I am so thankful to the panelists, our esteemed group of panelists for this morning, especially those who had to travel very far from South Korea. So, thank you very much. And I would like to thank especially Paul Park without whom, nothing including this event, would be possible. I would also like to thank the Korea Foundation for your generous support which help make this event possible. Thank you especially to Sihyung Lee and Kiho Jang of the Korea Foundation for their support. I would also like to re-iterate Brookings' commitment to independence and to underscore that views expressed today are solely of the speakers. My name is Jung Pak and I am the senior fellow here at the Brookings institution and the chair of the Korea program.

Recently there has been a lot of conversations and discussions and media hits on the summit that happened in Singapore. And I think that this event comes at a great time in that the threat from North Korea and other actors have not decreased as a result of the summit. But that it is important to highlight some of the threats that we can't see. And that's the thinking behind this Asia Transnational Threats Forum in which cyber is our key focus for today.

Cyber is a threat we can't see, that cross borders and is one of the tools, of course, of diplomacy. Cyber is an attractive form of -- and low-cost form of statecraft and countries are risking more and more aggressive action. And in this forum, we are going to be talking about North Korea and China specifically.

As the director of national intelligence and its annual threat assessment mentioned, Russia, China, Iran, and North Korea are the greatest -- or pose the greatest cyber threats to the United States and globally. Two of those countries are in Asia. And I

think it's important that we have a discussion about how to tease out the capabilities and intentions of those countries as well as to think about the government policy responses and what kinds of cooperation that we need from -- with our private and public partners.

And to help us tease through all of that, I am so pleased to welcome Chris Painter, who is a globally recognized leader and expert in cybersecurity and cyber policy, cyber diplomacy and combating cybercrimes. He has been on the vanguard of US and international cyber issues for over 25 years, first as a prosecutor of some of the most high-profile cybercrime cases in the country and then as a senior official in the Department of Justice, FBI, the National Security Council, and finally, the State Department.

In his most recent role as the nation's top cyber diplomat, Mr. Painter coordinated and led the U.S. diplomatic efforts to advance and open intra-operable, secure, and reliable internet and information infrastructure and advise the Secretary and Deputy Secretary of State on these emerging issues. Please welcome Chris Painter.

MR. PAINTER: Thanks. I am very happy to be with you this morning and this is a very important topic. As introduction said, I am a recovering lawyer, as Jim is too, who you will hear later. And normally, since it is the morning, you would open a presentation like this with a lawyer joke. But I found from long experience, the problem with lawyer jokes is that lawyers don't think they are funny and non-lawyers don't think they are jokes. So, I'll dispense to that and move in to the topic.

Look, I think clearly, cyber and cyber security and cyber threats we face are global, and everyone knows that. It is an inter-connected world. But there are regional aspects too. And it's hard to really imagine an area where this is more important that the Asia area where both from a threat perspective because some of the major threat actors are there but also in terms of opportunities as more and more countries are

depending on technology coming out of development, generally, and investing a lot more in this area, and trying to think about cyber security and protecting themselves. So it is again, both, I think a threat and an opportunity.

Now, you know, for that reason, we ended up spending a lot of time when I was in the State Department and also at the White House, concentrating on Asia, in terms of both the threat actors, particularly North Korea and China. But also in terms of working with other countries in the region to get a better response to really up our game in cyber security. One of the very first dialogues, we had this whole government dialogues. So, we would bring all of our government which would force the other side to bring all of their government and that was actually important because it broke down the silos which we have here too between different agencies, between people who do defense policy, people who do commercial policy, people who do law enforcement, diplomatic policy, really bring them together.

And the very first one we launched, after I moved to the State Department in 2011, was with Japan. And in fact, the very last one I did before I left was with Japan. The second one we launched was with South Korea. And so, it was really understanding that this area of the world was really a key linchpin for a strategic policy and also because this is really growing area. And both of those dialogues, I think, it really prospered over the years. I think they have been very productive. You know, there is no shortage of stol pipes in all of our countries but I think that really helped break things down and that was very useful.

But we also had a lot of conversations in the ASEAN region. So not just country-to-country dialogues but more global. And I'll get to that in a second. So I want to talk about the threats and then, I want to talk about some of the opportunities, maybe some of the things we can do about that to set up today's discussion. I also want to leave

some time for questioning because I want to have a little bit of interactive session here as well.

So, you know, I mentioned the DNI report said that, not surprisingly, in terms of nation states, China, Russia, North Korea, and Iran are all the major state actors. Also, trans-national organized crime is a major threat as well. And just like the U.S., who I think is the subject of all of those actors, I think Asia has challenges with all those countries too. I think a little less from Iran and much more from North Korea and China and Russia as well. And certainly, they have an organized crime issue too. So they have, you know, these challenges. When you look at those nation state actors though, there is a really difference between both what their rationale is, what their modus operandi is, what their intentions are, and also how you can work to deter those tensions which I'll get to at the end.

North Korea, you know, even in the light of the summit, I don't think anyone should conclude that North Korea's malicious cyber activity is going to end. There may be some strategic pause to the extent that it can be controlled to not screw up those summit discussions but I think this is something that's going to continue. It's an asymmetric threat that -- cyber is generally an asymmetric threat, it is asymmetric tool. It is a tool that the North Korean government has been able to employ in the past even when they can employ other tools. It is hard, though not impossible to attribute. And one of the things I want to make clear is attribution is not impossible to cyberspace. We have done very good examples recently where we have done attribution.

There is this thought that you have a free shot because of the attribution challenges. That's just not true especially with nation states because you look at all of the different tools in your tool caddy, not just following the cyber footprints to figure out who is responsible.

But North Korea, I think, has been assessed over the years. It has been listed in the last four DNI reports as one of the major actors as having growing capabilities, and its motivations are both disruptive, which I don't think we can dismiss. And there has been a lot of particularly regionally disruptive against South Korea and there has been a lot of different instances of that. But also, in terms of making money for the regime. And that's been another thing we have seen recently.

So we have seen both, both the money-making, you know, the resource committing cybercrime, et cetera. But also disruptive capabilities both in terms of potential conflicts outside of North Korea, ways to make North Korea's influence more felt, and to attack South Korean institutions. So, you know, there has been a number of -- and also, I think it's been interesting that North Korean activity comes not just from North Korea, but it also comes from other countries where there are North Korean diaspora around the world that act together to create some of these problems.

You know, one of the cases I was deeply involved in in the State Department and working with the White House was the Sony attack by North Korea, the Sony Pictures attack. And that was very interesting because it was the first time we really -- one of the major times we did public attribution when President Obama came out and said North Korea was responsible. And it wasn't just us that said that. We went to countries around the world and asked for them to condemn that conduct. And a lot did. But one of the problems with doing that kind of shared attribution, that kind of shared response is being able to share information swiftly with other countries. And that is something we are still working on. But that I think was a real watermark of showing North Korea's malicious intent there.

But there have been several examples since then. Obviously, the WannaCry ransomware that was attributed not too long ago by the US government and

the Australian government and the UK government and others to North Korea and that was significant again. This public attribution was significant. The Bangladesh Bank, the recent FBI DHS releases on something called HIDDEN COBRA where they talk about other malicious North Korean cyber activity. So, North Korea has been incredibly active and, you know, although, all this public attribution is a good thing, it doesn't really deter North Korea's conduct. You are not going name and shame North Korea. You are not going to name and shame Russia either frankly. I mean, I think if you look at the toolkit you have against these various actors, you have to tailor that toolkit to the adversary. And in the case of North Korea, naming and shaming alone, they don't really care about their soft power.

Now there may be an opportunity with the summit to make some effects because they will care in the context of a larger nuclear deal they are trying to reach. Although I would have loved to see cyber brought up as one of the summit issues, I think James Clapper said that the former DNI said that the second after nuclear in terms of actual destructive capability of North Korea was cyber. North Korea itself has listed cyber as one of its chief capabilities. You know, I certainly understand it not being brought up there, but it doesn't mean that it can't be or shouldn't be brought up in follow-up discussions because I think it is too much of a risk going forward for them to continue that destructive conduct.

We did, you know, impose sanctions on North Korea, what we call status sanctions after the Sony event which was, you know, disassociating with the North Korean regime would lead to sanctions. So different than the cyber sanctions we have. But North Korea is so highly sanctioned anyway that I am not sure if sanctions really make a difference. So we had to figure out the right tools to deter them.

China, I think has a very different intent and modus operandi. China's main threats have been espionage and also intellectual property theft. I think they clearly are also

developing, like every country around the world is, offensive capabilities but I don't think they have a rationale or reason to use those offensive capabilities. They don't need to be disruptive right now. They are too inter-dependent with other countries in the world economy in the way North Korea is not. And so, you know, I don't think they have ruled those out. I don't think they share Russia's information warfare view because they are worried about stability themselves. However they do want to project power and I think even regionally, we are talking about Taiwan and other places that could be used.

So China really has, I think, a different narrative and there is a chance to really affect China's conduct through -- because they do care about some of their influence and their soft power. And a good example of that was a couple of years ago, when we spent a number of years -- in where I led a China-U.S. working group on cyber before it was terminated when we identified PLA players, not by us, they drove it. So I thought it was kind of an odd move because it cut off a method of communication. But a couple of years after that, after sustained pressure from the U.S. at the very highest level, from the President himself and Susan Rice and like every cabinet official constantly raising the Chinese and not letting them forget this issue of intellectual property theft to benefit your commercial sector is something we don't do and we don't think any country should do.

In the lead up to the summit, we negotiated, really around the clock in the last evening they were here, and we reached an agreement, which I think is an important agreement that agreed that that kind of conduct -- intelligence gathering every country will do and we understand that. And the Chinese used to say, you know, there is no difference between intelligence gathering and theft of information for commercial purposes and we don't do either, which was not really very credible but after this sustained campaign, and not just by the U.S. but privately by a lot of other countries as well, we were able to reach an agreement that neither countries should do that. That then became a G-20 agreement. It

became really a norm and there was, I think, a shift in Chinese behavior after that which is significant. There have been some reports recently in the press that they are shifting back now. So that's interesting and I think everything depends on the climate between China and the U.S. more generally.

But I would also say that whether they comply with it or not, we didn't take any of the tools off the table. We said that, you know, we will continue to have all the tools, sanctions, other tools we could use if we find the violation. And indeed, you know, that continues to be true. So it's a level of accountability, you know. If they don't comply, there is still a level of accountability and that's important.

Now whether we can reach something like that with North Korea, I have my doubts. I think that's far in the future. I don't think we are anywhere near that yet. We certainly don't have a dialogue mechanism with North Korea on cyber. I don't really expect one anytime soon. I know there are some people who are hopeful we can do that. And we will just have to see how that plays out.

Russia and China also poses other risks in the supply chain risks and the issues of equipment and telecommunications equipment. These are all challenges in China, both -- cares about its own integrity, its own stability and wants to control information. But they also are trying to project power around the world and really become cyber leaders in a way that frankly, I haven't seen before. They are planning, they are stepping up. They have an international strategy for cyberspace just like we do. They have a real strategic approach and you know, they are really pushing hard on this.

Russia, and I will spend almost no time on Russia because everyone knows everything that Russia is doing. I would say, I have -- and I think many of us were surprised about the sophistication of their activity, the targeting, if you read Mueller indictment, if you read some of the articles that are out, it's really incredible in how they took

advantage of existing divisions in our country. They have done that not just in U.S. but around the world. I expect, given their success, you'll see other countries trying to follow this model, when trying to sow that kind of division in other countries as well. It's a real challenge.

Russia has always been one of the most capable cyber actors and so, you know, I think they have a different -- a different take than China or North Korea so far. And I think we need to figure out ways to deter them as well.

On the positive side, I think there is a number of, you know, really positive things that have happened in the region especially since I started following it back many years ago. You know, one of the things in the region is that you have economies like China who is investing a lot in this. You have Singapore and I'll talk more about them in a second who is investing a lot in this. But a lot of the economies, a lot of the countries in the Asia region are still really on a precipice of looking at this. Are not really investing enough in this. There is not really the awareness that you need. It's a real challenge. That is changing and there has been a lot of good activities recently.

I mentioned Singapore. Singapore has gone from basically from zero to 60 in this area. Just a couple of years ago, there was a study that said Singapore is one of the most vulnerable countries in the world because of its reliance on technology in the banking sector, et cetera. In the last two and half years, Singapore through -- created this new cyber security agency led by David Koh there. They have this Singapore cyber week where they showcase a lot of different efforts they have. They have this new strategy they came out with. They have a new law they came out with. They have gone really from not seeming to care about this issue to really caring quite a bit about this issue and doing quite a bit about it, which I think is very significant.

And not only have they done that within Singapore -- and Singapore -- if

you talk to the Singaporeans, they will say, you know, we were able to do this because we are a smaller country and we can martial our different capabilities. But they have also looked outward and said, what can we do for the larger region? And can we be a leader in the larger region? They have been the leaders especially with the ASEAN countries. And you know, ASEAN has very varied capabilities among the countries. Couple of years ago, if you remember, there was a hack into the Vietnam airport which kind of raised the issue for Vietnam but most of the countries do not invest. In fact, if you look across ASEAN, they invest about half of the level of the average amount of the world in terms of their GDP in cyber security. Now, Singapore actually invests more than their average in fact. I think they are third in the world in terms of investment right now per GDP which is significant.

But Singapore has played this leading role in trying to work with these ASEAN countries to raise the profile of this issue. And the U.S. and the others has been involved in this too. They have gotten a significant -- they were the leaders of ASEAN this last year, the Presidents of ASEAN. In the Leaders Declaration this last year, they got a very significant statement about the need for norms in cyberspace and the need for capacity building in cyberspace indeed to really up the ante of this and, I think, that's significant. And so, I think that's really been helpful to have that regional center and to work with them.

Japan, I think, as I said, we have been dealing with Japan for quite some time. Japan has also been working with Singapore and Australia and others to do more capacity building in the region. And Japan is really laser-focused on cyber in a way they haven't been before because of the Olympics. Because they are worried about a potential cyber-attacks on the Olympics and what that means. So that's a real opportunity.

South Korea has been active in this a long time because they are worried, you know, about the threat from North Korea. In fact, I think they almost code every attack from North Korea, you know, wherever it's from. I think they are laser-focused on North

Korea which is not surprising. They hosted a global conference on cyberspace. It started in London just a couple of years ago and that I think was very successful. It showed more leadership there. You know, they are challenged, I think, as many countries are and not having enough coordination among their different cyber players. I mean this is not unique to South Korea.

But, you know, there is lots of different players, lots of different agencies. We saw this when we were having our dialogue. The Blue House has a role which is the equivalent of the White House but it doesn't really have the kind of controlling role because of legislations and other things. That would be useful to have. So I think they are still trying to figure this out. But they certainly take the threat very seriously. They have a cyber-command. They are looking at how we deal with this. And so they have been very good partners too.

But many of the other countries, as I said, are still trying to build these capabilities. Indonesia has a new cyber security agency, they just created very recently. They are still trying to figure out how to structure that and go forward. Many countries now have the kind of institutions you need -- the CERTs but not all of them yet, the computer emergency response teams.

So this idea of capacity building in region, and engagement in region I think is really important. And that's not just the U.S. I think Australia and others, like I said, Australia and Japan play very important role there. And Australia is, you know, in the Asia-Pacific and again, people forget that sometimes. And Australia is really playing a big leading role in terms of its own development around this issue, it is all priority and playing more on the world stage.

So as I look at -- those are the kind of threats and some of the opportunities out there. Some of the things I think we need to do and do better when we are looking at

these threats. I do think we need to definitely engage with the region even more than we have. That includes engaging with, you know, continual engagement with China. We have some dialogues that we started with China. But dialogues -- words are not enough. I mean the fact that we have a dialogue is great but it doesn't really make a difference if you are not making progress on some of the key issues we needed to do. So we need to do that.

And we need to figure out how we can both build the capacities in these countries and convince them that what we are trying to do with them is actually preferable to what other countries are trying to do. Lot of countries are worried about stability in the region but they are also worried about economic growth. So how can we work with them to be more effective?

And one of the things I think overall -- and this was mentioned recently in the report, the State Department reports on the deterrence strategy but also something I have written about in the past too is having more a collective, a better collective response to some of these shared threats and working with these countries so that we can share information which is always a hard issue because sharing information, especially when it's, you know, sensitive information, it's hard.

We don't really have the channels to do that very well. But sharing information to have the kind of joint attribution, but more importantly, the joint consequences on bad actors. And those consequences I think really need to be tailored to the actor we are talking about. What will deter or even effect -- and some argue deterrence is hard or impossible. But I think we haven't really tried it yet in a lot of cases.

You know, what is going to affect Russia is different from what's going to affect China, is different from what's going to affect North Korea. So, we are going to have to be -- work on what those tools are. Refine those tools domestically for us but really work with our partners in the region to -- and build new partners to be able to do this more

effectively.

So, with that let me stop and that leaves about five minutes for questions, I think. So, any questions? Comments? Don't be shy.

AUDIENCE: Where are Russia and North Korea and China aligned?

MR. PAINTER: So, I mean, China and Russia are particularly aligned. North Korea hasn't been that much of a player in the policy process, as you find maybe not surprising. Russia and China are aligned in a couple ways. I mean, first they have been trying to push a global code of conduct for cyberspace. They want a UN treaty for cyberspace which is more to kind of constrict others capabilities and not their own. And really, it's around content issues, controlling content on the internet. I think North Korea would have a lot of sympathy for that. They just haven't been big players in that. But, so I think they are aligned there.

You know, I think all of them are certainly willing and able to use capabilities if it serves their interest and their developing capabilities. And so, there is an alignment there. But I don't think there -- you know, I think Russia and China there is much closer policy cooperation but they are not the same. Russia and China -- there are differences between them. And we have seen that in number of forms over time. So, they are not the same. They don't have all the same interests.

They said Russia has been far more willing and this is where it shares with North Korea to be far more disruptive on the world stage and really do things that we didn't think they would do before. I mean, North Korea always had that incentive. Iran had it to some extent too. But Russia has done that. Where China, I think, certainly has an interest in espionage and theft but right now doesn't have an interest in causing that kind of disruption.

AUDIENCE: You did speak of the tailored deterrence more at a macro

level. But on a micro level what would those be if you were tailoring those for each of the countries. What type of more micro aspects for that?

MR. PAINTER: So, you have to look at what's actually, you know, effective behavior. And there was a Defense Science Board report that Chris Inglis and others were involved in about two years ago, I think, year and half ago, which talked about having tailored strategies. And I think this is something that also the U.S. government has said is a good idea. But what you really have to do is sit down with people who -- and not just the cyber people. One of the problems we have here is the cyber people, great as they are, are not the people who actually know the full set of things you can do, right. Especially when you are talking about a country-specific thing. So, I think it's very good in this conference we have not just the cyber people but also regional people and others who are talking. I think that is really critical.

And one of the problems, I think, we have with Russian interference is whilst it's just a cyber-thing, it was an influence operation and the cyber-people, this wasn't really on our radar. So, you really need, I think, a group of people to think about this. You know, and think what's going to actually change behavior. So, for Russia is it really going after finances, is it going after, you know, a high level of officials who are close to Putin? What's going to change behavior in a way that's going to make a difference. Whether you talking of sanctions or anything else.

And North Korea, I think, it's been very hard but again, I think, maybe the summit opens up some opportunity because they will be more sensitive to things that you would do or they will be more sensitive if you have increased sanctions. I think there are some opportunities there. We will see if that gets followed through.

I think there is one over here.

AUDIENCE: So, U.S. policy makers have been focusing a lot recently

on Huawei and ZTE and President has gone, sort of, back and forth. I was wondering if you had any thoughts on the competing equities there.

MR. PAINTER: Yeah. Look, I think, this is a real challenge. And not just the U.S., Australia and other countries around the world are doing it. And some countries are just accepting the infrastructure by these companies without really even doing what I think you need to do which is this risk management issue, right. So, when you talk about 5G the exposure is much greater than 4G. We are not just talking communications, we are talking internet of things, we are talking infrastructure, we are talking everything riding on the back. So, exposure is greater.

Then you are asked, okay, so what is the threat? If you have companies that are largely controlled or at the behold -- are beholden to another government who could have a malicious intent, that's a problem. Now, if it's espionage that's one thing and you can think about how you mitigate that. But if you worried about more destructive conduct, as I said, I don't think China has a current interest in being destructive. Let's say something changes in the South China Sea. Let's say something changes with Taiwan. You know, who knows what can happen in the future. And so, then the question is how do we mitigate that.

And that's the last part of it. How can you mitigate that? So, I think, you have to really go through that analysis and decide if it's even mitigate-able and what the risk is. And I am not sure that every country is really doing that and they to. Because I think that's a real challenge. Anything else?

AUDIENCE: To what extent do each of the nations that you have described rely on their own internal capability and staff, if you will, to perform these functions? And which ones require either overt or covert participation of multinational firms, private sector or non-profit agencies?

MR. PAINTER: You mean to do what? For what purpose?

AUDIENCE: For conduct the purposes that you have described for the nations?

MR. PAINTER: So, I mean -- so there are two aspects of that. I mean, I think, every country has to work with their private sector and others to do defensive measures, right. I think that's absolutely key. I don't think governments including the United States can do that alone. If we are talking about some of their more offensive capabilities then I think it varies. But I think, you know, I think it's hard to find -- I think, these are mostly government-based, is my view. Not exclusively in U.S.

Okay. All right. I think it's the last one and then, I think, is that right?

AUDIENCE: Good morning. One country which is becoming more and more adept in this sector as well, which I didn't hear you discuss is Taiwan. So, I was wondering what type of relationship do we have working with Taiwan in cyber securities, cyber defense, whatever. Because considering that could be an interesting wedge to use against Beijing for its nefarious activities.

MR. PAINTER: Yeah. Look, I mean, just like in any other area, we have been cooperating with Taiwan in a whole range of areas. Defense generally and certainly on cyber. This is not new. This has been going on for some time. So, I don't expect that will cease. I don't think we do that to create a wedge. I think we do that because we think it's important to do that. And Taiwan has vulnerabilities. So, you know, we have -- Taiwan has a special status. We don't recognize it as a country but at the same time we work with them on these issues and I think we will continue to.

All right. Well, I wanted to thank you all. I think it's going to be a fascinating day. There are lots of great speakers who are coming up. There is a lot of interesting ideas. It will be interesting to see what conclusions we agree to at the end

and thank you all for being here.

MS. PAK: Chris, I wish I had half the energy and passion that you do. Thank you for that, that was wonderful. I'm so pleased to invite William, Carter, SangMyung Choi and Priscilla Moriuchi to the stage. I would like to introduce our distinguished speakers. First, SangMyung Choi who came to us last night from South Korea is Chief of the Computer Emergency Response Team and Director of the Security Intelligence Research at Hauri, Inc. Regarded as one of the most skilled malware analysts in South Korea, he was selected in 2016 by the South Korean government as one of seven experts to participate in the cyber guardians program. He has had extensive experience in working together with the South Korean National Intelligence Service, the National Police Agency, the South Korean Cybercommand and many private companies in preventing acts of cyberterrorism. He was awarded the Security Merit Ministerial Commendation from the Ministry of Public Administration and Security in 2012 for his active contribution to and participation in national cybersecurity. I'd like to welcome SangMyung Choi to the podium.

MR. CHOI: Hello everyone. I am from Korea. I work for Hauri which is a vaccine company. My customers are mostly related to military installations and my clients, including myself and my company, we have been hacked before many times. For ten years, I have been working on hacking technologies of North Korea and I will use many of the examples of the attacks carried on by North Korea.

North Korea has carried out many, many attacks to South Korea. These have been varied in their patterns. In the early 2000's, this was under Kim Jong-un and for the most part during these times periods, they attacked military servers in South Korea. But these were not known to the media all the much because of the sensitive nature of these attacks.

And then there was the attack on the South Korea government administration and then that's when South Korean's got to know the depth of the abilities that North Korea had. Because of that, the UN also made this an issue in one of their forums. Since then, there has been hacking of the nuclear plant at which point they had stolen the nuclear reactor designs and they have also attempted many times to hack the Korean Department of Defense. They have stolen some operational plans, otherwise known as OP Plan, for USFK operations plans. This was targeted at South Korea. The information they had stolen from us was related to USFK and also United Nations forces in Korea. We came to realize that many of the attacks were carried out by North Korea but through third countries they have also attempted to have want to cry hidden cobra attack. They carried that our recent and they have also carried out attacks in Bitcoins and also encryption coins.

Currently, Kim Jong-un is in power in North Korea and Kim Jong-un had referred to cyber capabilities that they have as being as important as their nuclear capabilities. In South Korea, just about every well-known organization has been hacked or at least has been attempted to be hacked. Many institutions have been hacked including the government, the Blue House Unification Ministry, the Ministry of Foreign Affairs and also the media including the press and also many of the energy and transportation companies and institutions have been hacked. They have been attacked including subways, bus ways and also telecommunications, internet service providers and also the shopping malls, some of the bigger known shopping malls have been hacked. Also, many of the large corporations have been hacked. Also, many of the security vendors themselves have been hacked. And through these vendors they spread ransomwares and other malware.

The same goes true for our congress assembly had been attacked and

also the information used by North Korean escapees in South Korea. We know many of the professors had their servers hacked. A lot of these had not been known or made known to the general public but today, I confess to you that it has been very prevalent everywhere in every industry and institutions. This is very symbolic of the hacking activity carried on by North Korea.

This is the home page of Blue House. Blue House is equivalent to the White House here in the U.S. and they had been hacked. So when outsiders tried to have access to Blue House pages, this is what showed up. Blue House, of course, has a very good program when it comes to preventing attacks from outside. But nevertheless, they were able to infiltrate the Blue House webpage. Here it states that it is exhorting determine Kim Jong-un and his leadership and that he would be the unified president of the Koreas. That's what it says.

The same goes with 2009, to DEDOS actually this was again when the Blue House was attacked previously by North Korea. This created a lot of confusion in South Korea. At that time, about 400,000 computers became zombies for DDOS attack. 400,000 back in 2009, that's a tremendous number. So 400,000 attacks at once coming through and it would have taken over 2000 servers that North Korea had to use. Apparently what they did was they hacked into about 2000 servers throughout the world and then using those 2000 servers they controlled 400,000 computers in South Korea.

And U.S. Assert has recently gave a warning about a hidden cobra which we believe is coming from North Korea. North Korea sends a worm which is spreadable in malware and those malware are used for their cyberattacks. The Ministry of Defense in Korea was hacked, internet and intranet were supposed to be separated. One of the many servers that the Ministry had had both internet and intranet connected together. At that point, it was attacked by North Korea. They were able to enter the intranet through

the internet and they have stolen 235 GB of military documents. We're not even sure what documents were hacked and of the more important documents were old plan 5015 and this was stolen and this was a contingency plan about preemptive strikes on North Korea by the U.S. and South Korean forces. As you can see, this was a very important document which was hacked. It is true, that North Korea has been steeling many of the military information and data from South Korea including ESIS and Carrier and Cruise missiles and submarines.

Now why was it that we were so vulnerable to their cyberattacks. That's because we have certain vulnerabilities that North Korea latched on to. In the U.S. you have MS Word and in Korea we have HWP. It is widely used throughout the government as well as throughout the general population. North Korea had about 23 vulnerabilities they have found in the program and utilized the same. And then there is something called Active Acts. This is something that Korea had adopted full-hearted. During 2007-2018, about 26 vulnerabilities were identified apparently by North Korea and thus utilized and infiltrated. This was used for banking services and other financial services.

Of late, they are attacking South Korea as follows. You start with a mid-point and what happens is that they don't constraint to the target that they have, they go through the partners at the main targets that they have. So the partners or the subsidiaries or the assisting companies would be hacked into first and then through their connection to the main target, they hack more information. One of those were a nuclear plant in South Korea. A nuclear plant had mostly intranet connections but through a partner company of the nuclear plant, they were able to infiltrate the intranet of the nuclear plant and thereby stealing some of the designs of reactors.

This is another example, Korea Rail and also the subways and also the Korean Airlines were hacked. Not only that, the companies such as the partner

companies who are producing parts and components for them have also been hacked. We had media, KBS, WTN and NBC which have all been infiltrated. We had many financial institutions and companies which have been hacked into. This is from 2017, ATM and POS machines were hacked. In South Korea we have SK, KT and Korean Air which are really big companies in South Korea. They have all been hacked. They have attacked the vulnerability of ML Soft that were being used by these companies and by infiltrating the vulnerability of ML Soft that they were able to hack into these major companies. And then now we have internet part shopping malls which would be vulnerable to financial information. Bitcoin is being used, those were being hacked and also Bitcoin and other encryption coins by pretending to be a government institution. North Korea actually stole $22.8 million of Korean won from these exchanges.

After the South North Korean summit, I thought that perhaps the cyberattacks would come to a stop but it never did actually. They continue to attack South Korea and also apparently other countries. North Korea and South Korea, whether North Korean's are authentic and sincere in wanting a peace regime, I think it is important for us to keep an eye on their internet and cyber activities. If they are authentic, I think they would also stop and cease and desist their internet cyberattacks. This concludes my presentation as my time is limited. Thank you for your time.

MS. PAK: Thank you, SangMyung, that was fantastic. I'd like to invite Will Carter to the podium. He's the Deputy Director of the Technology Policy Program at CSIS. His research focused on international cyber and technology policy issues including artificial intelligence, surveillance and privacy, data localization, cyber conflict and deterrents, financial sector cyber security and law enforcement and technology, including inscription. Before joining CSIS, he worked at Goldman Sachs investment strategy group where he performed research and analysis on geopolitics and the

macroeconomy. I'd like to invite Wil to the podium.

MR. CARTER: Thank you very much for having me. It's great to be a part of this event. I'm here to talk a little bit about some of the trends that we've seen in China's capabilities and the way that they're using them. Building on some of the very illuminating comments that Chris made earlier. But I think that Chris really touched on the key theme that I want to highlight today which is that in the U.S. dialogue, we often lump China and Russia together as malicious actors in cyberspace, but I think that's a bit misguided. Particularly as we try to understand the way China will use its cyber capabilities for power projection, including in the region.

I think China actually views itself and wants to me more like the U.S. in the way that it develops and employs cyber capabilities as opposed to being like China. As Chris mentioned, that falls a little bit more under the North Korea model of being willing to be disruptive, change the status quo, be overt, be disruptive and destructive. China wants to be the good guy. They want to be seen as the good guy, more importantly. And that means that they have moved in a direction of greater subtlety, greater centralization and control of their capabilities and what I would call the professionalization of offensive cyber capabilities in China.

Whereas I do worry a lot about what Russia might do attacking say industrial control systems in our critical infrastructure. I don't worry about that was much in the immediate term with China. I think they don't want to do something that is overtly provocative. They don't want to do something that is overtly disruptive to the status quo or that makes them look like a malicious actor. What I do think they want to do is establish, we talk about China wanting information dominance. I think they now see the potential to go a step beyond that. I think they're looking to develop as close as they can to universal visibility of everything that happens in cyberspace and being able to use

cyberspace to track physical activity.

They're attacking networks in order to collect everything from financial data, health data, information on our behavior and preferences, biometrics and identity documents, family and friends and the contents of our communication. I don't necessarily expect them to use traditional Russian techniques like massive doxing and social media manipulation campaigns that are relatively overt. I do think that they want to be able to track us all. They want to see what we're doing, where we're going.

The key is really that all of this happens below the threshold of open provocation and conflict and war. I think Russia is redefining where that threshold is. China is redefining how you can exercise power and use cyber to project power without approaching that threshold and without necessarily going into the grey area quite as much as the Russians are. They do this in three main ways. Propaganda, IP theft and economic advantage and then intelligence gathering. They also do things like targeting dissidence and separatists groups in other countries. For example, there was a high profile series of attacks on dissident communities that support Taiwan, Hong Kong, Tibet and Australia about a year ago.

They also tend to launch attacks in the region following major incidents and particularly around anything politically sensitive. It's a way of voicing their displeasure about certain events and also pressuring the world to conform to their view of how things are and how things should be. For example, the attacks on the lot group around the sale of the Thad Missile sight in South Korea, the attacks on the Philippines and Vietnam around the Scarborough Scholl arbitration ruling. There, we even saw them attacking the International Court of Arbitration and The Hague itself.

There have also been a lot of attacks on Taiwan and Hong Kong particularly around their elections and votes. But what is interesting about one of the

ways that they've approached the Taiwan and Hong Kong issues in cyberspace is their efforts to use both diplomatic, economic and cyber leverage against companies to assert their view of the world. For example, the recent pressure on airlines that have listed Taiwan as a nation of destination for flights or that do the same with Hong Kong. They've also used cyberattacks on companies that engage in that behavior and against companies that do business with some of these subsidiaries of China or semiautonomous regions of China. And we saw that particularly recently with the reports highlighting the attacks that have been undertaken against major U.S. contracting firms that have been doing business in the South China Sea.

Part of this is an effort to disrupt those companies, gain commercial advantage and help to spread their own power in the region through physical infrastructure and economic influence. But part of it is also to understand what these countries are doing, gain that comprehensive universal visibility that I talked about.

But the biggest thing as I mentioned earlier is this overall trend towards professionalization. It is about greater subtlety, it's about a focus on strategic goals, it's about finding ways to project power while still appearing to be the good guy. It's about delegitimizing the U.S. So as to not only gain influence in the region but also raise its standing and influence in global government's mechanisms that control the internet.

Part of that, as Chris mentioned, is their efforts to use companies like Hawweh and VTE and their position in the 5G network to gain a footprint globally for espionage purposes but also to expand their influence in third markets. You might argue that the U.S. wrote the book on using a commercial presence in the internet backbone and other countries for espionage but China will write the 5G chapter. And I think that's a trend that we really need to worry about particularly as Chris mentioned. The implications of having a footprint in the 5G network could be significantly greater as censorization,

machine to machine communications, mass volumes of internet traffic begin to give them so much more data to work with. That ability to see everything that is happening.

Finally, they are moving to gain greater control over the governance mechanisms of the internet. The core institutions, whether that is ICAN or the ITU. That's not just about using offensive cyber capabilities, that's about defining what is okay and not okay in cyber space. It's about asserting their view of the world and their laws and their norms and their culture on the internet and particularly on content hosted in other countries. It reflects a broader shift, away from short term gains, things like defacing websites and launching noisy but not necessarily particularly impactful attacks on countries that upset you. For example, the cyberattacks on Japan around the Senkaku Diaoyutai Islands dispute and also away from traditional economic espionage. Which for a while, was one of the main under takings of the PLA, and towards long term strategic goals.

That doesn't mean that economic espionage isn't continuing to happen. For example, one of the biggest areas of Chinese cyber activity recently has been attacks on cleared U.S. contractors, not just to gather intelligence but also to get technical specs on our platforms and capabilities and figure out how to replicate them for China. It also reflects the fact that the line between economic and security espionage has always been blurred. But I think that China's understanding of national security technology is a little bit more evolved than ours, honestly, or at least how it intersects with power projection.

The main way that I think that's illustrated is in the Chinese concept of strategic industries and strategic technologies. China sees AI as a military capability, an intelligence capability, a way to influence other countries, a way to shape dialogue, shape knowledge from data. They are willing to engage in every form of espionage, every form of influence operation, every capability in IP theft in order to advance that agenda. It's

interesting, I had a conversation just a few weeks ago with a group of U.S. AI companies. These are smaller companies that have been approached by DIUX or other groups within the U.S. Department of Defense because they have interesting capabilities, say machine intelligence, national language processing. I asked them why they had rejected these overtures from the U.S. government and they said China. I assumed that that meant that they wanted access to the markets in China but it turned out that their feeling is that the second it becomes public knowledge that they have partnered with the U.S. government on a military or intelligence capability, every Chinese APT will be all over their network in five minutes. All of their IP will be stolen and while China will be doing it in large part for the national security benefit, they're going to pass all their IP to Chinese companies that are then going to start competing directly with these guys in both commercial markets and also in developing capabilities for the Chinese government.

The other interesting thing that China is doing and the other way that they're leveraging their capabilities regionally is integrating cyber and information very effectively in their physical operations in the full spectrum of warfare. Some of the biggest attacks that we've seen in cyberspace recently in the region have targeted defense ministries and intelligence ministries so the Chinese can figure out, we talk about salami slicing in international relations. How close can I get to the red line before someone decides that they have to react? So they're stealing things like the operational plans that were just mentioned. They're stealing crisis plans. They're finding out what exactly are the thresholds and events that these countries have planned responses for and what would those responses be and then they're calibrating their behavior to that.

One of the most interesting and bizarre ones that I have had some discussions about is trying to figure out the exact distances from the specific islands in the South China Sea that they can sail before countries will react or take umbrage and

then sailing one or five miles outside of that boundary. So they're showing the flag but it's not an escalation. That's where this is going. That's where China is going with their capabilities. It's all about professionalizing, centralizing, better utilizing their capabilities for strategic goals.

The last area that I want to highlight with that is what we've now termed civil military fusion. This idea of better coordinating and consolidating the capabilities of the private sector and the civil community with those of the military intelligence services in China. It's not a new thing, patriotic hackers have always been part of China's repertoire. But they are increasingly controlled, they are increasingly centralized in the same way that the Chinese government centralized control of their intelligence apparatus so that they could better task collection. They are also centralizing control of their patriotic hackers, pushing them away from these disruptive attention grabbing attacks and towards these long term strategic goals. They created things like the cyber security volunteer alliance which is bringing white hat hackers from China into organizations that directly support their efforts.

The other piece is with the development of the strategic support force, which I'm sure most of you are familiar with, it's basically the consolidation of the PLA's capabilities and electronic warfare, intelligence, space, cyber. They've also given them a whole bunch of R and D facilities. They've given them a mandate to innovate. They've given them a mandate to develop new capabilities along new lines that they had not done before. As a result, in the last few years I just looked at this earlier today. There have been six reports from major U.S. cyber security companies just year to date in 2018, highlighting how entire new suites of capabilities including new malware families and entirely new attack vectors have been identified from known Chinese APT's affiliated with the strategic support force. It is a reflection of the move towards long term thinking,

towards capability development subtlety, not making waves, moving a little bit beneath the radar and as I said at the beginning, being able to look like the good guys.

The last piece of that is the recognition of China's own vulnerability. The fact that they increasingly are using their position as a champion supposedly of defense in cyber space and of good behavior in cyber space and of norms of the code of conduct that Chris mentioned as a way to legitimize their own activities, make themselves a leader and to define the agenda for global cyberspace governance. But it's not just about that. It's about recognizing that they are genuinely vulnerable. They cybersecurity law has elements that are meant to help them project their power and project their legal norms internationally to impose their controls and their requirements on foreign companies. They genuinely are worried about threats to Chinese companies and Chinese infrastructures. I think that's something that gets lost in the U.S. debate a lot of times. One of the biggest pieces they're concerned about and one of the biggest ways we see that is the crackdown on pirated software in China. Pirated software is a huge problem in China, it is very widespread. It also tends not to be maintained and patched correctly. So when major campaigns that target known vulnerabilities get out into the wild China is often hit disproportionately. This is, thankfully, something that we do relatively well with in the U.S. because generally U.S. companies use more licensed software and are better with their patching practices, not that they couldn't be improved.

But finally, the crackdown on cybercrime. One of the reasons that I think China is different in the way that it approaches cyber criminals than Russia is because Russian cyber criminals act outward, Chinese cyber criminals have always had a more domestic focus. I read a lot of interesting things about why that is and I've talked to some people. Some people say it is a language think, some people say when you have such an enormous domestic target environment there is no reason to focus externally. But is

has meant that you have seen a very different approach to cybercrime and controlling cybercrime in China than say in Russia. Patriotic hackers in China tend to be white hats. They run legitimate Chinese cybersecurity companies. They're not guys out using ATM skimmers or stealing massive numbers of credit card numbers from websites. If they are they pass it on to Chinese intelligence, they don't tend to spend as much of the money.

All of that put together, I think there are a few key things I want you to come away with. One, China wants to be the good guys, they want to take the U.S. position in the world. They don't want to be Russia, they don't want to break the status quo, they don't want to disrupt our ICS systems and start an escalating conflict with the United States. What they want is to be the good guys, set the norms, define the governance model of the internet, define the way that other countries do cybersecurity and they want to do that the way that the U.S. has done it for decades. Which is maximize your intelligence capability, maximize your visibility of everything that's happening around the world, use subtle techniques, get into the internet backbone, get into the supply chain and make sure that you have a presence everywhere and an understanding of what's happening everywhere. That's the model that they want to replicate, it's ours. So we should look to lessons from our own history to think about how we deal with that. Thank you.

MS. PAK: Thank you very much. Last but not least, we have Priscilla Moriuchi who is the head of the nation state threat research and Director of Strategic Threat Development at Recorded Future. Her cutting edge research on North Korea and China has been featured in the *New York Times, Washington Post, Wall Street Journal, Wired* and many other media outlets. Prior to Recorded Future, Ms. Moriuchi spent 12 years at the National Security Agency, most recently as the enduring threat manager and top subject matter expert on East Asia and Pacific cyber threats.

MS. MORIUCHI: Good morning everyone, thank you for having me here. I'm going to talk today about the breadth and value of North Korea's elicit crime online and the breadth of their use of the internet. I see North Korea's online crime as just an extension of the states administered criminality. For decades, the North Korean state has engaged in drug smuggling, counterfeiting, illegal liquor sales, cigarettes, gold and precious stones, cars. If there is a commodity that will generate money, especially through the diplomatic establishments throughout the last four decades particularly, North Korea has engaged in exploiting that commodity for revenue generation purposes.

If we look at the internet, I see it very much as just another domain for North Korea's criminality. Today I'm going to go over four types of operations. North Korea has conducted over the last three years, since the beginning of 2015, that broadly our belief to be designed to generate revenue for the Kim regime. The first are the banking operations. These are intrusions into banks networks where the operators gain access to the Swift typically or other interbank transfer systems and execute fraudulent transactions in an attempt to steal money from those institutions or from some of their supporting institutions.

WannaCry has been mentioned a couple of times but it was the global ransomware attack which swept through the world in May 2017. I'm going to focus not on the attack itself but on how the attackers used and moved the revenue or the coins, the cryptocurrency coins that were generated from that attack because I think it is really implimatic and thus far really the only case that we have of confirmed North Korean attackers obtaining and utilizing cryptocurrencies. Second, I'm going to get broadly into the cryptocurrency thefts from exchanges. Mr. Choi talked about that a little bit earlier. And then this fourth level that I call low level financial or internet crime and wrap that up.

So there are a couple of slides here I have of known or suspected North

Korean banking operations over the past three years. Depending on who you talk to there are anywhere from 10 to 30 North Korean conducted banking operations since January 2015. The ones that I've listed here on this slide and the next slide are ones that I have been able to confirm either through public information, have high confidence links to North Korean actors because they've either been publicly linked by the government or by the financial institution itself.

I included the amounts of money there because there are a number of unknowns in these banking operations that make it difficult to assess the value that North Korea derives from the operations. One is that the banks are not always open, frequently are not, about how much was attempted to be stolen, how much was successfully stolen and the techniques via which their networks were exploited. So in the cyber world we would call that initial attack vectors.

Second, we know a good deal about the malware and some of the tools that North Korean operators use to gain access to some of these networks which is good. That information is based on studies of a relatively few number of attacks. Third, academic studies by think tanks and others have shown us and given us great insight into North Korean elicit networks around the world globally. So we believe that these operations and the money, whatever amount is stolen can be very easily moved via these elicit networks that have been developed over the past 40 years.

So if we go through attacks, the first one being the January 2015 attack against Banco del Austro in Ecuador where typically, based on the attacks that we know about there is an attempt at a much larger amount of money than is actually successfully stolen. Again, over time we have also seen that the attacks have exploited not just access and knowledge by the hackers of the Swift system but other domestic intrabank transfer systems as well such as the SPEI in Mexico. What is concerning about this is

that many nations around the world have their own domestic intrabank transfer systems that are, I will politely say, variously secured. In that we talk a lot about Swift because it is the most widely used system but it is by no means the only system that North Korea has attempted to exploit. And again, when we talk about these attacks, we don't know how many have been attempted, how many have been successful, how many have been completely unsuccessful and exactly how much money.

If you look at that November 2017 attack against the Mexican National Banking and Securities Commission, that was large, $110 million is a huge amount of money to be stolen. We still don't know if they were successful or not. There are a number of other suspected attacks that have already taken place this year. Again, in terms of banking operations, attribution tends to be slow because the banks are not typically transparent and have no reason to be with the public. Just to touch base and knowledge basis on the WannaCry global ransomware attack that occurred in May 2017. Again, the U.S., UK, many private sector companies have attributed the attack to North Korea. The general consensus was that the attack was designed to cause chaos. However, what I'm going to look at is how the North Korean actors moved the Bitcoin generated from that attack.

In May 2017, when the WannaCry tool piece of malware swept through the world, victims were asked to pay the ransom into one of three wallets. At the time, there was a lot of criticism of the attackers, we now know are North Korea, by the information security community because a lot of people thought it was irresponsible and it was indicative of how naïve North Koreans were about cryptocurrency system because they only used three wallets for this global attack. We could easily track the money that comes from these three wallets and it was just naïve. So that narrative perpetuated through last summer.

So when the attack began in May, by the end of the attack it ended up lasting less than a week, realistically. There were 52 Bitcoin in the wallet. The Bitcoin sat there for a number of months untouched until August 2, 2017 in which all three wallets were emptied in two transactions each within minutes of each other. So we have three wallets and two transactions each so at this point we've got six transactions. This is where it becomes incredibly complicated and why that narrative about how naïve the North Koreans were to use this methodology breaks down.

So all of these six transactions and all of these 52 Bitcoins were moved to a company into a technology called a mixer. So a mixer is essentially a legal launderer. So what a mixer does is it breaks up all of these Bitcoin into tens of thousands of tiny, tiny pieces and engages in tens of thousands more transactions to essentially oviscapte the original coins. It is like throwing dollar bills in a bag and shaking them up and then pulling out one dollar bill and assuming that was the same one you put in in the beginning. So essentially a laundering system. I personally at the time tried to tract the transactions through this mixer. I got to 40,000 transactions and just failed. So that's one.

The second really interesting technique that the North Koreans used in this case was after the coins were already run through a mixer which had essentially anonymized the entire transaction stream, they then transferred the coins into another currency called Monero. Monero is different from Bitcoin in the sense that the sender, the IP address of the sender, the receiver and the amount of coin transferred is encrypted in each block. So only the sender and receiver know who each other are and how many coins was part of that transaction. Looking at that Blockchain from the outside, all you can see is that a transaction took place. So the goal of Manero is to be a truly anonymous currency.

So if we kind of go back through this use and this one really interesting use case of how North Korea has utilized cryptocurrency, they took what many had thought was a naïve scheme for, in this case, whether it was designed to generate revenue or not is not really known. There were these three wallets that many people said we could all track and was really irresponsible of them, ran them through a mixer and then transferred them to Monero. There was no possible way, at least from the public, to track them beyond that.

Moving next into the larger North Korean cryptocurrency operations. I won't spend too much time on this because Mr. Choi touched on them a little bit. South Korean exchanges have been absolutely hammered since at least February 2017 by North Korean operators stealing large, large amounts of coins and likely money, value, from South Korean exchanges. There are also at least another two large thefts this year, so the end of last year and early this year, that remain publicly unattributed but that follow a similar attack signature to those that are known to be North Korea.

So you've the thefts on the left side and on the right side, we see mining. Cryptocurrency mining is a form of generating cryptocurrencies. Essentially, in most cases, the coins are generated using either large blocks or single user machines. The computers are tasked with solving really complicated mathematical equations. Once those equations are solved then block is created. Once a block is created, the currency typically rewards the creator with a certain number of coins. At this point, for example in Bitcoin, if you generate one block the reward for you is 12.5 Bitcoin.

Another interesting way that North Korea has been utilizing cryptocurrencies is in mining. We have seen at my company, North Korea engaging in Bitcoin mining since at least May of last year, Monero mining since at least November of last year. This is not on a large scale from the data that I've seen. Large scale mining

operations for Bitcoin for example, can generate anywhere from $5 to 8 million worth of currency per month. What we're looking at, at least from the information that I've seen is a very, very low level, a few users or a few machines on North Korea territorial networks mining cryptocurrencies. That's just because we have a relatively small optic and there are very few users of the global internet in North Korea. It's likely that there's more in other places, especially because we know how heavily North Korea relies on third party countries for its own cyber operations.

Lastly, I call this the low level financial crime section. This aspect of North Korean operations, information on this is primarily derived from defector or other visitor interviews. If you read defector interviews who have, especially defectors or other visitors who have knowledge of North Korean cyber operations, they talk a lot about a few very specific characteristics. One that North Korea likes to send its cyber operators to countries overseas outside territorial North Korea, to conduct the operations. They're sort of like warehouses or dorm style environments where they'll be somewhere from a few dozen operators, typically men, who will live together in a facility in one of these countries. They'll work together. And third is that they're required to earn a certain amount of money to maintain their status overseas and within the regime. Testimony from defectors says anywhere from about $80 to 100 thousand a year.

If we take the numbers. So there are debates about how many North Korean hackers there are and where they're living and where their numbers are. I think I heard this morning from Dr. Lin that 10,000 is kind of a safe number. I took the numbers off of this slide very explicitly because I didn't want to focus on them. I will say them out loud but they are most likely wrong. Mainly because we don't know how much money has been stolen from the Swift operations. It depends on the swings in cryptocurrency value are so broad that within the span of a few months, a single coin can be worth

$5000 or could have been worth $20,000 last year so that increases the uncertainty. And second, we don't know how many operators are overseas. So all of those in my estimations based on known banking operations has been around $105 million known to be stolen from banks globally since January 2015.

In terms of the cryptocurrency thefts in mining, this number is going to be widely off because there are so many of the large exchange thefts that are unattributed and depending on when North Korea cashed out. My sense based on other research is that North Korea really needs the cash so they're not holding on to these vast reserves of crypto coins anywhere in some sort of wallet structure. My sense if that they have the elicit networks already set up. They need the cash and they can easily move the funds. So just based on the known thefts and the numbers of coins that we know were stolen last year which is somewhere around 11,000 coins, that value could be anywhere from $30 to 220 million depending on when they cashed out.

On the gaming and low level financial crime level, if you take 10,000 operators and assume that they are even half overseas and that even half these people have that sort of $80 to 100 thousand to demand to generate revenue for the regime each year, you're looking at around $400 million. So a total could be anywhere from a half a billion to $700 million. This is a substantial amount of money for North Korea. Even though the number is most likely wrong, I think the assessment that North Korea derives a lot of value from their internet operations is indisputable.

I'll leave you with this last slide as sort of discussion points and a way forward from the policy level. So what do we do? Should we care because in this specific elicit online activity vein, companies and not governments are typically the victims. According to (inaudible) control data only about 15 percent of all sanctioned entities on North Korea to date are not North Korean. To me, that's not representative of

the amount of activity that is conducted by North Koreans overseas. It is really implimatic of what has been our effective so far but focus on territorial North Korea. I think we have to be willing to engage non-traditional partners in Asia and Africa where we know that there are North Koreans living abroad and operating. And that is part of a maximum pressure continuity that we have to keep identifying and pursuing these front companies, these enablers overseas in these third party countries. Thank you very much.

MS. PAK: Thank you. So we're going to start the question and answer session so I would ask Priscilla and SangMyung and Will to come up to the stage and join me. That was a fascinating and terrifying set of presentations so thank you for that.

I'm going to start off as the moderator, I just wanted to ask a couple of questions for some clarification and then I'll open it up to the audience. I know there are going to be lots of questions on these issues. All of the panelists talked about the capabilities and there was some talk about what the motivations might be. I wonder if you could talk about, each of the panelists, could talk about what the constraints are that China and North Korea see they have. Like what is holding China and North Korea back from going full on or shaping their approach to cyber activities? Maybe I'll ask Priscilla first if that's okay.

MS. MORIUCHI: Sure. For North Korea, the limiting factors are likely resources and personnel. Cyber operations are a relatively low investment for North Korea. Low threshold for investment and for entry and they are a good value. Not actually spending a lot of money on any of these operations while any money that they really are funds that they generate are usually a net positive, I would say. I think that for North Korea at least, cyber operations are part of the kind of national strategy. They're not as broadly effectively enabled because of the revenue generating function.

So from a nation state perspective, most nations aren't engaging in this type of

activity. As a result, they have a much broader footprint and broader capability to conduct things like espionage but they also have a lot of other targets, China and Russia. For North Korea, the target space is smaller but also their ability to develop and leverage those capabilities is also hindered because this sort of demand for revenue generation.

MS. PAK: SangMyung Choi, can you comment on that as well.

MR. CHOI: Well, in my case, when we look at North Korea, we think there are about 7000 operators who can carry out hacking. When you say 7000, we do not think at all 7000 are involved in actual hacking. We believe about 1500 programmers are there and the 5000 are support personnel. So 1500 actual programming. When I think of North Korea I think they are doing enough already. They are creating havoc everywhere and so what we know is really a very small portions of the various attacks that they have been carrying out.

There is a lot more that they have been doing that they are not aware of. For example, India, they actually have North Korean operators sent to India. Within India, they have been carrying out attacks against financial institutions and they have gotten quite a bit of income from it. Now because these operators are in India, it's been hard for people to point to them and say these are North Korean's. So that's how they are operating. There are many operations and operatives who are working overseas and we need do not know the full scale of the damages that they have been causing. I honestly think that they have been doing quite a bit already. Limitations, I don't know. They are doing all that they can.

MR. CARTER: I'm sorry to have missed my co-panelists comments but my earphone is down there. But with China, I really think it's the reputational piece. I think there are two main pieces to that. One is China runs into a lot of road blocks because they have a reputation for being a bad actor in cyberspace. So people when

ZTE want to come into their country, they think about it twice. They are actively working to delegitimize U.S. companies in order to overcome that advantage of ours and the Snowden leaks certainly helped with that.

The other piece is they don't do things that they think will enhance their bad reputation in cyberspace, in some cases. So the fact that they have actively reigned in some of these patriotic hackers from things like website defacement with pro-Chinese messages and similar activities. That's driven by the fact that they want to put out a positive image. I think that also reigning in their own intelligence community, part of that was just the Chinese government wanting to have a more professionalized intelligence community that they could task to key national priorities. Another piece is again, they want to be good guys. They want to define norms of good behavior. They want people to welcome them in and I think that that is the biggest constraint on their tendency to be offensive in cyberspace.

MS. PAK: Thank you. I was also wondering about training. SangMyung, you talked about how there is some North Korean hackers in India. So where are the North Koreans and the Chinese getting this training and the knowledge to conduct these activities?

MR. CHOI: Well, when it comes to India, they have a relationship with North Korea. They have diplomatic relationships. In North Korea there is Kim Il-sung University and also Kim Chaek Science and Technology University. That would be the equivalent of MIT in the U.S. They have some very superior talents that are coming out of that university. They have programming Olympics. In these Olympics, there are some very smart people coming out. These are programming Olympics and then there is something known as Chosen Computer Center which would send people dispatched to India.

On that side, it looks like these are people who are working on IT legitimately but at night they would be working as their operatives in India. There is ICIC in India. The one example would be that this operative would be sending phishing mail to people who are using the financial institutions accounts. And then they have malware that would be neutralizing the vaccines that financial institutions in India had. It's called Quick Kill, that's the India vaccine that was neutralized by the North Korean operative.

So North Koreans have had a lot of practice with South Korean institutions and they do very well in India especially against financial institutions. So these are a reputation of what they have learned from their practice with South Korean institutions. So my organization also is trying to work on these vaccines but India is right now very vulnerable to this type of neutralization.

MS. MORIUCHI: I think Mr. Choi is right. North Korea has a very robust development pipeline, I think we would call it and state run development pipeline. For China, I think theirs are two development pipelines for information operations capabilities. One is one that people study and talk a lot about which is sort of the state run, the POA. The POA institutes that universities throughout the country that cooperate with the POA and the government. Then you have the civilian side. There is uncertainty as to how the administration security, the other side of the Chinese, the civilian intelligence organization, how they recruit if they have, for example. Actually information operators within their ranks whether they utilize primarily a contractor or a more dispersed system.

I think also in China over the last seven to ten years, we've really seen the rise of the information security industry. There are a number of very, very capable and comprehensive companies who have very, very capable information security professionals, hackers of their own who are engaged in a very vibrant penetration testing scene in China for companies domestically. There is also the overlap between the

government and the private sector especially when it comes to information security.

MR. CARTER: I would add to that, one thing that China has really stepped up their efforts to leverage is foreign talent. So if you look at the information security scene or the broader tech scene in China, such a huge proportion of the people in that community were either educated in the U.S. trained at U.S. companies. Many have lived for more than a decade in Silicon Valley. We think of the underground hacker scene like the movie Hackers, hack the planet in the U.S. It was also in China so there was a very vibrant social community of hackers in China in the late nineties, early 2000's as well. That's another talent pool for them.

And then you see things like the thousand talents program now where the Chinese government is going out and actively pulling people with particularly technical backgrounds and expertise into the country and saying you know, teach at universities, set up research labs, set up startups, join Chinese multinationals. All of that brings tech talent and cyber talent into the country and it is a really effective pipeline for them.

MS. PAK: Thank you. We're going to open it up to questions. I'm going to take three questions at a time and the panelists can answer, you can pick and choose which questions you'd like to address.

MR. OROWITZ: My name is Elliott Orowitz. I just want to thank the panel for a very good presentation. Would anyone in the room like to speak about the PDRK counterfeiting or illegal shipments of good and people and services.

QUESTIONER: My question specifically is for Mr. Choi and it is around the issues of attribution. Specifically, around the most recent watering hole attack that you reported on. I was wondering if you had an idea on attribution, whether it's Lunaroff or another group that might be described in the open community. Same question around

attribution for a group operating out of India.

MS. PARK: Hi, my name is Rosa Park. I work at the Community for Human Rights in North Korea. This is a very serious issue in terms of the theft of cryptocurrencies by North Korea. I was wondering, as far as I know, I know that South Korea has regulations on cryptocurrency companies within the country. Are there regulations that the government can put forth that will help to mitigate this issue?

MS. PAK: So I have a question on counterfeiting, non-cyber related activities and then we have the cryptocurrency laws and then on the question that was directed to you, SangMyung. Let's just go down the line and you can address whatever questions you'd like.

MR. CHOI: Let's go to the attribution question first. I've been working on malware from North Korea for about ten years now. We have a database. We have a DNA of the codes from North Korea. An interesting fact when it comes to North Korea, the North Korean hackers they have been using the old method. Actually, they have not abdicated. They have continued to hold on to the old practices because for some reason they feel these have worked before and why do we need to change it. So they just keep on using the same codes. These are codes, we know from 2009, are similar and the same codes are continually being used. By detecting the signatures of these codes using virus (inaudible) which is a sample of viruses worlds wide.

Once you have registered there if you find the same signatures from India or other countries, then you know that these codes are coming from North Koreans. And these are the signatures that will be traced. North Koreans attributions are not hard these days. Once we have these signatures, we turn those over to the intelligence agencies or the crime investigating governments. We know our attributions are usually very correct.

As to the cryptocurrency, we have regulations, of course, in South Korea

but these are regulations to not really address the cryptocurrencies only. So when it comes to cyber restrictions, I don't think we can say we have a clear law on that. Yesterday, we had a general election and we have these elections which will result in new regulations being introduced. But for now, I don't think we have any clear direction as to the law passed. It was more of a voluntary regulation imposed on the industry themselves but now the government is stepping up its efforts to regulate more closely.

MS. MORIUCHI: I'll address the cryptocurrency question as well. I think one of the reasons why cryptocurrencies are so appealing for North Korea is because of this broader ecosystem that's around the cryptocurrency. So it is not the Blockchain technology itself necessarily that's insecure or that's attractive to North Korea but it is this ecosystem of exchanges. And wallet providers and all of these services that have sprung up that are largely outside of a few countries, South Korea, Japan and a few others largely lightly regulated to not regulated at all.

So, for example, you don't need to have any identification whatsoever to set up a wallet in most places at most exchanges you just need an email address. To cash out, to exchange your coins for dollars or euros or whatever, others with hard currency, all you need to do is go through an exchange. Many of those exchanges are taking it upon themselves to implement stricter identification requirements for their own customers to track some of these elicit uses. But broadly we're talking about a largely unregulated and anonymized ecosystem around coins, many of which are designed to be anonymous themselves. So for this sort of rogue regimes and criminal cyber actors they are quite a useful tool.

MR. CARTER: So on the question of regulation, I think that I completely agree on that point. I do think it's become clear that that's not going to remain true. So whether it is multiple countries looking at how to apply anti money laundering and know

your customer rules to cryptocurrency exchanges, trying to have better visibility into transaction flows. Private companies developing tools to try to track transaction behavior and patters of users of cryptocurrencies. The visibility of that field is going to grow over the coming years and regulation is also going to grow within constraints.

MS. MORIUCHI: I would say it depends on the coin realistically. So in the cryptocurrency market, the use of any coin is driven by the users and what those users want from that service. The general public go along with coins that are either surging in value or that are more usable. So we take Bitcoin as a given that it is going to be the cryptocurrency baseline in the future and that the information we have and we require on users of Bitcoin will be what users in the future will utilize. I don't think that's necessarily the case. If you look at currencies like Monera or Litecoin, Monera is not going to open up its Blockchain ledger to financial companies and regulators so that they can see the IP address. It's the antithesis.

MS. PAK: Because that's their business model to remain anonymous.

MS. MORIUCHI: Right. I think there are upwards of 1800 coins in the marketplace now so yes, certainly regulation is definitely in the future but this is very much a consumer driven market. If you as a coin adopt regulations that go too far for your users preferences then people will just move and use a different coin.

MR. CARTER: I agree. I think the question is going to become to what extent are these coins available to users in countries that are willing to impose penalties on some of these exchanges that are willing to exchange these types of coins. I also think it touches on another thing which is you mentioned there are always new coins that are coming out and I completely agree. I think another area that I would expect North Korea to start looking at is how they can exploit FinTech companies and new financial technologies, particularly payment systems.

As we discussed, North Korea is essentially a mafia state. It is a crime family with a really large territory. They'll see an opportunity to make money and they'll use it. I think that for countries like Singapore and Hong Kong and Tokyo which are major financial centers in Asia, they're very cognizant of this and there is always this push and pull in the regulatory space of knowing that a lot of these services, particularly from smaller firms are vulnerable, but also wanting to be a FinTech innovation hub. I would say these are the top two -- if you talk to the people in Singapore and Hong Kong, these are two of the top priorities of those countries. There is a little bit of tension there so I do expect North Korea to start looking at how it can exploit other financial technologies beyond just the cryptocurrencies.

MS. PAK: I'll just quickly address your question about counterfeiting and ship to ship transfers. So that's part of maximum pressure. My understanding about counterfeiting is that I think we've passed the heyday of counterfeiting of super nodes by North Korea may ten or fifteen years ago but that doesn't mean that it has gone away. North Koreans have various ways of making money. We've talked about the cyber, the virtual ways that they can do it but they also to the old fashioned way which is the diplomatic pouches which they use to smuggle cigarettes and makeup and other goodies. Those are some of the traditional ways that the North Koreans have been trying to make money.

I hesitate to eat into our lunch half hour. Please join me in thanking our very learned guests today.

(Recess)

MR. BAKER: We have a great panel this afternoon also. We'll start out, we're going to have one speaker do -- we're going to do sort of a hybrid. We'll have Professor Lim, who I'll introduce in a second, do a presentation from the podium, and

then the rest of us are all going to join on stage and then we'll have some discussion. And then definitely leave time after that to have questions from you all, which can be about the things that we're talking about which we'll hopefully build on what was discussed this morning as well.

So with that we've got three panelists here. Professor Jon-in Lim is here from Korea University. He is a professor of information security in the department of Cyber Defense, and he plays a very large role in South Korea with respect to cybersecurity. He's the president of the Institute for Cybersecurity and Privacy. He's also the president of the Korean Association of Chief Information Security Officers, and he was previously a special advisor to the president of South Korea for National Security.

Kate Charlet will also join us. Kate is the director of the Technology and International Affairs program at our neighbor, the Carnegie Endowment for International Peace. Kate previously played a very significant role in cyber at the Department of Defense where she was the acting deputy assistant secretary of defense for defense policy where she managed the development of DOD's cyber policy and strategy, their cyber capabilities, and expanding their cyber relationships with key partners around the world. Kate was also at the NSA before that.

And then Michael Sulmeyer is here. Michael is the director of the Cybersecurity Project at the Belfer Center at Harvard University, part of the Kennedy School, and Michael also was at DOD working with Kate, and Chris Painter as I understand it, where he was the director of Plans and Operations in the Office of the Secretary of Defense working on cyber policy.

So with that, we're going to invite Professor Lim to come to the podium and speak, and then the rest of us will join him on the stage after that.

MR. LIM (WITH INTERPRETER): Good afternoon. I'm Professor Lim.

During the early morning session, we talked about North Korea quite a bit. When it comes to cyber, it's a military option for them, as well as economic means and political tools. They have been utilizing it. It's actually a rogue nation in that regard. But we have had the historic summit meeting between Mr. Trump and Kim Jung-un, and also on April 27th there was a summit meeting of the Korean president and Kim Jung-un. And in these summit meetings, the joint communique was that there would be no aggressive actions toward one another. And in particular, when the Panmunjom communique was made, that no provocative actions would be taking place in the seas, land, and air, and in all spaces. So when it says all spaces, I must believe that cyber is also included in that space, but most of the discussions in the public arena are about nuclear attacks and missile capabilities of North Korea, but I need to emphasize that we have to have a clear understanding that cyberspace is included in all the spaces where the provocative actions would cease and desist between the two nations.

As was presented to you earlier, introduced to you, I am in these institutions and also what I am interested in is Jus Post Bellum cyberspace peace treaty which I will be speaking to. In Korea, we have been facing quite a bit of threats from North Korea. This was not limited to physical threats but quite a bit of threats in cyberspace, and much of that has been spoken of today in the morning already. When it comes to East Asia, we have quite a few actors who are quite capable when it comes to cyberattacks and also cyber capabilities. We have Russia, North Korea, China, and also we have the omnipresent presence of the U.S. So we have quite a bit of technology that's focused in East Asia. And with all these capabilities amongst the many powerful nations, I think it's important for us to have a better understanding of what it means to have a cyber-conflict.

One of the issues when it comes to cyber conflicts is the attribution. We

also are able to point to any single country or single actor and say that they are -- when there was an attack on Ukraine by Russia, the attribution was to Russia but Russia never admitted to having done anything. And as such, it's important for us to have an international forum where the parties can come together and discuss these cyber activities. And as to South Korea and the U.S., we have had a continuous dialogue, and these dialogues have been very important in the allies having a common understanding as to the threats posed by North Korea. And North Korean attacks have been occurring for a long time. And as you can see, in all those different occasions when the attacks occurred, South Korean government did come up with new policies and additional strength and postures. But they have not been all that effective in deterring North Korea.

Let's take a look at some of the structures in the U.S. and South Korea. I don't see how the U.S. would be the best practice at this point when it comes to cyber threats. Nevertheless, it comes as close to best practice as possible amongst many nations in the world, and South Korea has a similar structure to the U.S.

In the U.S., you can see that the White House is right next to NSSC and cybersecurity directorate, and the president's office also has the DNI to help him make decisions. And also, the U.S. has quite a few legislations that have been enacted and have gone into effect. However, as to South Korea, we do not have a structure that is clearly delineated when it comes to the role to be played by cybersecurity center. We do not have as many laws either enacted, and as spoke of earlier, in 2013, we have had a Seoul conference on cyberspace. It represented Korea at the time. We have come to realize, and we have a deep understanding that cybersecurity is important for the prosperity of all people in the world. And that there has to be a capacity building and trust building. And those were spoken of through the Seoul framework 2013, and also, we have had continuous dialogue with the U.S. And in 2015, we had a joint statement of

ROC-U.S. alliance. When Mr. Obama was visiting South Korea, we had spoken of and made a statement which focused on the need for capacity building in South Korea, and also exchange of technologies and people.

When it comes to cyber deterrence, we have to find ways to nurture and also train the manpower, and in this regard, there would be more exchange of people and information with the U.S. That as the joint communique back in 2015. Nevertheless, after that we have had change of guards both in the U.S. and Korea, and thus, the joint statement has not been all that effective as of now.

Now, part of the problem that South Korea is facing is there is governance issue. We have various institutions which are vying for influence and that cyber center has not been all that effective. There was WannaCry and NotPetya which had occurred, and we had Cisco and Megapi and other private institutions in Korea which were able to trace these attacks. We have some very smart people and very able people in the private sector, and we have relied heavily on these private sectors. But in Korea we do not have laws that enable the government to tape into the private industry as effectively as the U.S. might be able to do so, especially true because Korea has a large concern when it comes to surveillance of the cyber command or the intrusion into the private lives of people.

We have something called NIS, which is very similar to CIA of the U.S. Because NIS is an intelligence community, they have had difficulty sharing information with other agencies or institutions and that actually became a limitation to Korea. And for the past several conventions, it's something that we have wanted to join for a long time. We haven't been able to do so because of these limitations that we had.

We also have capabilities that we have been trying to achieve but we're not quite there, especially true when it comes to attribution. We spoke of how the NIS

was not able to share information with other institutions. The same goes with the Ministry of Defense. They have been reluctant to share information with other agencies within Korea, and as such, we are very limited and hampered by our own internal problems. And also, when it comes to cybersecurity, although we have been having many dialogues with the U.S., we are not doing as well when it comes to sharing of information. I certainly hope and look forward to the day where we have a more seamless exchange of information when it comes to cyber information exchanges.

In 2017, which is last year, we had a new administration taking place and it's more of a progressive administration. And the government does not want to become a big government, and they are reluctant to become more actively involved in the cyberspace. So this is actually a limiting factor as well. As such, we have not been able to come up with a new national strategy for cyberspace. We had Mr. Choi speak on the topic today earlier.

Yesterday was the general election that took place in South Korea. Now that we have had the election, we have newly elected members of the assembly, and hopefully, we will be able to focus on the cyber activities, but that's my hope only at this moment. We do not know how it's going to go going forward. When it comes to cybersecurity, the capabilities of a nation is very important, having the technologies and the personnel, and also policy. All these things are well known. And also, international cooperation, especially cooperation between the U.S. and Korea, the two allies.

When we realized that North Korea has many hackers, anywhere between 1,000 to 3,000 operatives are working in China as software programmers, and also, many of the operatives are working in Malaysia and other Southeast Asia countries. So during the day they have their regular jobs, but at night, when they have operative directives, they act in that capacity at night. And also, they track their targets for a long

time. They look at the target five years, seven years. They have a better understanding of our system in Korea. We joke they know us better than we know ourselves. And when that is the reality on the Korean peninsula, I think it's important for us to keep our eyes on North Korea. Especially true, now that we have had the summit, we were thinking perhaps if they are really sincere about their intentions, that in cyberspace that they would cease and desist all these illegal activities but that hasn't happened yet. Let's see how it goes. And if they continue their illegal activities, we know where they are.

As you can see here, we have had many things taking place. The North Koreans have many cyber-trained operatives. North Korea is a very controlled state. And beginning from elementary school, they would learn high levels of mathematics, and those who are excelling in mathematics, they would be selected from early on and get trained and educated. They get sent to China. They get sent to Russia. They become the cream of the crop for cyberattacks to be carried out. For now we assess that there are anywhere between 7,000 to 10,000 cyber operatives in North Korea. If they were to utilize them for greater good and positive direction, that's good. That's going to be wonderful for that nation, but we don't know which direction they will be taking.

If there is going to be any peace treaty on the Korean peninsula, I believe it should also include a cyberspace peace treaty that all the very capable and smart cyber operatives in North Korea should now become, or into the future become, people who would be working for the prosperity of North Korea using peaceful means. And if they were to engage in any illicit activities, I feel we need to have a new mechanism that would enable punishment of those who carry out these illicit activities. And this would be something that could be developed in conjunction with China, Russia, and the U.S. as well. So this way this would be more of an international action that could be taking place when it comes to cyberspace.

When you talk about CVID, V stands for verification, of course. So in order for us to be able to provide the verification that we should be able to engage China, the U.S., and many of the commercially available talents. And as Mr. Choi had spoken of, that these many talents can actually come together and assess any issues and also be able to attribute properly and prevent further flaring of cyber conflict.

Ever since 1998, I have been working on these cyber treaties. I've been to many international conferences. They have, for the most part, have fell on deaf ears. We talk about cybersecurity, cyber activities are known as very important but whenever these criminal activities take place people get mad. People get upset. But what could they do? We haven't been able to do much about these actors, the rogue actors. And we certainly hope going forward that there would be more of an international mechanism that addresses these international cross-border cybercrimes. And North Korea is certainly one of those actors that must be addressed. Thank you.

(Applause)

MR. BAKER: Great, thank you.

Thank you very much, professor. Thank you for those very interesting remarks. Thank you so much for those.

So what I'll do for the next few minutes is do some going back and forth, some questions for everybody. I'll focus on Kate and Michael first since they haven't had a chance to speak yet, and then as I said, I'll turn it over to you guys for questions as well.

So almost every time that I hear a briefing, get a briefing, or have a discussion about cyber and the situation that we're facing in the United States and in the world, I come away just very depressed by the diagnosis of what the situation is.

So, but to start out I wanted to see if Kate and Michael had thoughts first

about the description of the threat that we've heard so far today in general. Do you agree? Is it such a grim picture that we've seen so far or that exists today rather? And is it different in the United States as we're experiencing it here? And you can break that down any way you want to -- government versus private sector, does the threat look different? And then both of you have worked on cyber issues in connection with Asia, and so does it look different there? Are they experiencing different threats from the main threat actors that we've talked about today -- China, North Korea, Iran, Russia? Does it look different from their perspective? First of all, just start out with how do you see the threat and what do you think about that? And then we'll talk a little bit more as we go here about sort of why we have the situation and what to do about it. But let's just start with your perspectives on the threat.

MS. CHARLET: Sure. Can everybody hear me on the mic?

MR. BAKER: Can you hear back there? Okay, good.

MS. CHARLET: So first of all, thanks to Jim and Brookings and the team, and fellow panelists. I know it's going to be a really good discussion. So I don't think anything I'm going to say is going to make you feel too much better, although I will try to end on a positive note.

But in the trajectory of the time that I've been working on cyber policy issues and cyber incident response, I feel pretty pessimistic about the trajectory of the threat. So, I mean, if you just look in the 2012 time period, we saw denial service attacks. We saw destructive cyberattacks, most of which were targeted against specific companies -- Saudi Aramco, financial sector. We moved to critical infrastructure disruption in Ukraine with their electrical grid. To globally destructive malware that we saw with North Korea and WannaCry and NotPetya, to societal disruption that we've seen in the Russian activities to influence the election. So, you know, it's evolving and

you see new ways and larger scale ways that cyber capabilities are disrupting societies.

MR. BAKER: How do you think it's evolving? Like, what do you see behind that evolution? In which direction is it going or is that too hard to see?

MS. CHARLET: I mean, I think there's an increasing boldness. So for one, there was a smaller set of actors several years ago that I think we're kind of acting more loudly, right, that you could see that were engaged in cyberattacks and cyber operations, and now there seems to be, you know, you saw this a little with the Russians, there seems to be less of a concern that they're getting caught. And so I think it's a little bit in the nature of the boldness of it. And then in the scope of it, right, that WannaCry, NotPetya were like global in nature.

But I guess the good things I see, so one, we haven't seen, you know, massively, globally destabilizing threats, although the societal disruption that you see from the election influence kind of borders up on that. But something at a level of, you know, disrupting how the financial system operates. You know, we haven't see that yet.

MR. BAKER: Why do you think so? Do you have any thoughts about that? The self-restraint, I mean, I guess?

MS. CHARLET: I'm sure Michael and others have thoughts. But what it seems to me we've seen is a lot of kind of testing the boundaries, kind of increasing testing the boundaries to get, you know, the pushback and find where the pushback and where the boundaries are. And many of that testing has not resulted in really significant costs imposed. So I think part of it is testing the boundaries, and I think part of it is the recognition. I mean, those globally destabilizing things affect globally. I mean, everybody relies on the financial system, so I should hope that there's a reservation and certainly a restraint in thinking about those capabilities.

And then I'm encouraged also by just the international and the regional

banding together really and like what we've started to see in terms of cooperation internationally in naming and shaming, pointing the finger and attributing publicly. That doesn't do that much in and of itself but at least it does create this norm and this like sense internationally that when somebody has done something they shouldn't that they're not just going to get away with it without having a finger pointed at them at a minimum. And it sets the capabilities to then impose consequences in a way that has broader international legitimacy.

MR. BAKER: Okay, good.

Michael?

MR. SULMEYER: Thank you. And greetings. Wonderful to be here back in the promised land of Washington, D.C.

Jim, I share your depression, and I wish to emphasize your depression. I would say that at this point everyone has what they need to have to be able to disrupt an adversary's, a competitor's activities. You can call that economically. You can call that militarily. Whatever you want. But gone are the days where we could dismiss some of the rogue or revisionist states and say, well, you don't really have a sufficiently mature program. It's not true anymore. You can download for free the bulk of what you need to test your own systems and to attack. What's the difference between penetration testing and hacking? Permission. It's usually the same techniques, often, just you have permission by the owner of the system when you're trying to do it for money and help test, and when you don't, that's called hacking. Generally, people don't appreciate that. All right? But the capability has now been democratized. What we're now seeing is how different regimes use these capabilities to pursue different goals, so what we need to be looking at more of is the motive. Are things getting worse? Yes. Everyone likes to stress about the Internet of things. Fine. However, the Internet of bodies as someone

has called it, and this is not just wearables like everybody's Fitbits, but I'm talking about implants, does create new risk that we cross a new threshold. That threshold is that to date no one has yet been killed from a cyberattack. We may cross that at some point soon as a result of that new technology. So that's something I think to keep a marker on, and that is, again, a subset of where things are headed in terms of the attack surface.

Maybe the good news is that this is actually not a situation of brilliance on offence. This is more a situation of negligence and slowness on defense. Let me try that one more time. Okay? Taking notes at home and Pyeongyang. This is not a situation where the offense is always so intelligent. We are not fighting Houdini. All right? A lot of times we figure out after the fact that some very reasonable defensive procedures or steps would have blunted or at least contained the effects of an attack or an intrusion. This is not to say that offense is not a real thing. Of course it is. Of course there are some very skilled folks on the offense but that is a minority position. So perhaps the good news is that with the right kind of national strategies, the right kind of actions by private sector companies, and I think generally expecting more accountability by both private companies and governments, we actually can redress the defense posture and make a dent in this problem.

I'll stop there and we can keep going.

MR. BAKER: We'll dig into that in a minute or so.

Does the -- I have a question though. Does the parity for the equal distribution of the toolset that are used -- that is used to conduct these cyber -- malicious cyber activities, does the parity lead to some kind of deterrence or is deterrence just not sort of when you think about strategic deterrence, military deterrence, that kind of thing, is that just -- do you see that at play in the cyber arena? A lot of people have talked about this. Or is deterrence just not happening? It strikes me when you say that everybody is

sort of equally equipped. Does that cause deterrence to exist?

Michael, I'll start with you and then go to Kate.

Is there cyber deterrence?

MR. SULMEYER: There is not.

MR. BAKER: Why do you think that?

MR. SULMEYER: The core reason I think right now is that for most regimes they still believe that hacking pays. That's because hacking continues to pay. The reason is because regimes have been unwilling to impose cost in the ways that will actually get the offending regime to stop.

MR. BAKER: Why is that?

MR. SULMEYER: Because they value other priorities in a bilateral relationship or in a bilateral competition higher than they do the effects from the malicious hacking. That's why. So that's why I am much more a fan of degrading an adversary's capabilities to hack, reducing their opportunities to do that, rather than trying to find the right Jedi master combination to convince them it's not a good idea.

MR. BAKER: Kate, what do you think about this? Cyber deterrence, is that a thing in your mind?

MS. CHARLET: Yeah, I mean, I think right now I agree with Michael that we have not been willing or have found the right tools to impose the kind of consequences on this activity that would deter somebody. I think that, you know, you were talking a little bit about is there deterrence that flows from everybody having these offensive capabilities? I think there's more deterrence that flows from everybody being highly vulnerable more so maybe than fear of the reaction and part of that fear of any reaction has to do with just how much of a glass house everybody has. And I think that's essentially universal.

MR. BAKER: Okay. Let me ask this question.

Why is it so bad? Why is this picture that we've just described and I'll agree is grim and depressing, how did we get there? How did we get there? What are the drivers? Is it technology? Is it economics? Is it law? Is it policy? Is it we don't have enough of the right workers? Is it that Congress is not well educated on this? What do you think are sort of the drivers of this grim sort of picture that we've painted for everybody both on this panel and then earlier today?

MS. CHARLET: I don't think you can point to one thing because I think it's all the things that you just mentioned. So its massive complexity is one. Right? I worked on Afghanistan, right, for a long time and, you know, the key players who are making decisions on that policy are pretty well, you know, pretty contained. Right? But in cyber policy, everybody cares deeply. Right? The Department of Energy, the Department of Treasury, Trade, NIST. I mean, it's a huge set of stakeholders.

MR. BAKER: Just within the USG.

MS. CHARLET: And this is just within the USG. And then you get -- and then, of course, the deep linkages with the private sector, for whom and for all of us for whom cyberspace is a place of commerce and social engagements. And it's not just a space for the military; it's a space for everyone. So I think one piece of it is just sheer complexity, the need to clarify roles and responsibilities and who does what and it has taken a lot of time. And then I think just the lack of incentive structures and time and money.

MR. BAKER: Incentive structures, what do you mean by that?

MS. CHARLET: So incentive structures for companies or for critical infrastructure, to fill those gaps in cyber hygiene. The knowledge gap, you know, both at the high level policy making level or the CEO level where it's still less so certainly but still

kind of a realm of sort of nerds and, you know, kind of leave it to the cyber people. And that really needs to change. Whenever I've seen something good move forward, a policy move forward effectively, it was not because it was just happening within the people who do cyber; it was because the regional experts, you know, China or the experts saw this issue as a core issues that it was involved in, the bilateral relationships and with their agenda. And so I think getting a much broader contingent engaged on these issues is really critical.

MR. BAKER: Michael?

MR. SULMEYER: Well, having gone to law school, it can't be the law's fault. So we take that off the list in terms of what got us to this point. I do think that we have to think about why we're at this point based on the tradeoff with economic vitality. If you're having a conversation with cybersecurity, this is pretty depressing. If you're having a conversation about the engine of economic vitality that Silicon Valley brought us, that's a pretty optimistic record that you look back on. There's a tradeoff there. When we go first, when the Internet is born here and we start connecting everything first, what do we prioritize? Speed, performance, convenience. Right? And the market takes off. And everyone does very well financially and communications are revolutionized. That's a good story. Who wants to be the one from the government to roll in and say, "I don't like this. I'm worried about the security and the safety issues involved here." We've had reports warning that the light has been blinking for decades about the safety and security issues. It's been that bad for a long time. What has been missing is the ability to talk about how you're going to help the market correct a little bit to account for those vulnerabilities. So the fact that then our adversaries figure out how to exploit them and use them, well, that's on them. We've got to hold them accountable pretty aggressively for doing that.

MR. BAKER: So let's, in the few minutes we have left, let's -- I'll ask this of all of you. So all of you have advised high ranking government officials on cyber policy. Okay, and so given what we talked about, you know, what the situation is and perhaps why that is, and we've sort of touched on a few solutions, what are two or three things that you think we should do? What would you advise high ranking government officials today to do? What are the two or three things that you think need to be done to change the situation or maybe it can't be changed.

What do you think about it? And Professor Lim, let's start with you. What do you think government officials need to do to change the situation? You touched on some of those in your presentation.

MR. LIM: Well, when it comes to advice -- actually, before I get to that I want to talk about deterrence a bit. When we look at China, we have Mao Tse-tung. He said that Chinese, there are one billion Chinese. If three-tenths of them die, there is still a lot of us left. That's in reference to a nuclear conflict with the U.S.

Now, that's the attitude that the Chinese take. That for Chinese leaders, they are willing to sacrifice certain things to achieve whatever they are aiming at. And it's really different, the framework or the mindset. The Chinese bring different ideas when it comes to what they want to achieve. So what is the U.S. willing to sacrifice? What are the Koreans willing to sacrifice in order to achieve their priorities and whatever they are aiming at? So when you think about deterrence, you have to think about the pain threshold that each nation is willing to accept. If that country believes that they have more to gain, then there is no deterrence.

Now, as to your question, for the U.S. government, when North Korea came out to talk to the Americans, it was the international sanction that was applied to North Korea that was working. We know that North Koreans felt much pressure from the

international alliance, pressure that was put on to North Korea. They had to act, and the same could be applied to cybersecurity if the U.S. would be willing and able to put more pressure on North Korea and all these cybercriminals, I believe we would have better results. So without that real deterrence, real threat, then we would not be able to realize the real policy success.

MR. SULMEYER: Four ideas for when you are elected to Congress, audience, or when you are drafted into federal service here soon. First, as I intimated, I would try to do more to hack the hacker. Right? Degrade our adversary's ability to do what they've been doing that we don't like.

MR. BAKER: So not just defensive but offensive as well?

MR. SULMEYER: Correct. Well, I start with offense but you just stole my thunder.

For defense at scale is point two. For too long we've been talking about needing to teach you to defend this. No. No. No. That's a losing proposing ultimately at scale. At scale, there's a handful of companies that provide critical services that we all rely on. Right? We don't need to name but we know how the big -- from telecommunications to various search, cloud, content, and platforms, you've got to work with them both collaboratively but also in terms of holding accountable to provide defense at scale for all of us downstream.

Third, we've got to invest a lot more in national resilience to be able to fight through and operate through a worst case scenario. The military does this habitually. In civilian life we have not.

And finally, we best get our heads screwed on straight about artificial intelligence and what it means to have a national approach both for our security services and as a country for making sure we're working with private companies, academic

researchers, and yes, synchronized with government to make sure we don't fall behind in that space.

Go forth and give 'em hell.

MR. BAKER: Just to flush that out a little bit, what's the particular thing you see about AI?

MR. SULMEYER: So the particular thing I see about AI is that some of our competitors will have access to vast troves of data that we do not have access to. In part, the reason is we have a Fourth Amendment to our Constitution. That is a good thing that we have a Fourth Amendment to our Constitution. I'm not mocking that. I am merely saying that some of our deepest competitors in this space are allowed to search, seize, and do whatever they want with everyone else's data. They will have access to a lot more to then be able to train off of for an algorithm. We are going to have to overcome that in some creative ways.

MS. CHARLET: So I have three. One is about international cooperation. Specifically, on pressuring and constraining bad behavior. So you're starting to see a little bit more of this with NotPetya and other activities recently. And I just think no one country is going to be able to kind of push and set the rules of the road, and I don't necessarily mean norms, big end norms, but little end norms. And you know, setting a greater understanding of what is appropriate, responsible behavior in cyberspace, and I think you really have to dig down in the pressure and constraining that you do at an international level to occlude with Asian partners.

MR. BAKER: Would you agree with Professor Lim with respect to sanctions? Does that make economic sanctions on malicious cyber actors, how does that strike you?

MS. CHARLET: Whenever you can do that collectively as opposed to

only one country that is always better. I mean, sanctions matter more or less or not at all, you know, to certain countries, so you have to be eyes open about the impact, whether it really has an impact on changing behavior, but the more comprehensive you can get the better.

My second piece of advice is don't always follow the shiny object. Right? We get so tempted, but cybersecurity is place where there aren't going to be a lot of silver bullets. You just have to keep working, whether it's on federal cybersecurity and making sure that U.S. networks are -- or, you know, government networks are secure. I think a recent report card came out with lots of Ds and Fs in that regard, but not only do federal network governments contain tons of information on all of us personally, but they also manage major important missions and support major missions that serve the U.S. public. So just continual prioritization and focus on those not shiny objects.

Same thing with protecting information like what we saw in cleared defense contractors. Recently, the Washington Post reported on Chinese supposedly taking a lot of information from the Navy on military capabilities. I mean, shame on us. Right? That's not acceptable. You need to go back and make sure you're focusing on even just basic measures so that stops happening so often and at such scale.

And then my third piece of advice is very similar to Mike's but a little bit more broad. I mean, getting ahead of the threats that are coming. Artificial intelligence is a big one and there are capabilities in machine learning that you can apply both to network defense and that are going to make those automated hacking tools much -- potentially much more powerful and more available to more people. So --

MR. BAKER: Because the AI will help those tools get better.

MS. CHARLET: Yes. It's not clear whether that will change the advantage between the attacker and the defender or whether that's even the right way to

think about things, but it's certainly a capability that is already impacting how we defend networks and how hackers can automate their attempts to get into systems.

But my other kind of pet issue is, you know, that we don't have, I think, a genetic infosec mindset. I lived through the Office of Personnel Management and, you know, millions of very, very personal records getting stolen and I sometimes wonder what's going to be the private sectors like genetic information OPM. You know, and so when we're all kind of on our mobile applications exploring our personal genetic data, are we thinking about that from and learning the lessons from cybersecurity as we go down that path?

MR. BAKER: Most likely not I would say.

Okay. So let's turn it over to the audience. And we have, I think, two microphones that are available. So let's see if you have questions.

There's a question way in the back. I can't really see who it is, but way in the back corner there.

If you could just identify yourself and what organization you're with, that would be great, also.

MR. WU: Sure. Jesse Wu, Aleda Consulting.

This is a question about cross-border information sharing that's come up for a few of you. I'm curious what formal mechanisms are in place, particularly in Asia, to aid cross-border information sharing? And since my kind of pet interest is mutual legal assistance, how do you see the Cloud Act playing into that, if at all?

MR. BAKER: Perhaps, Professor Lim, you talked a little bit in your presentation about information sharing. Perhaps we can start with you.

MR. LIM: When it comes to information sharing, when it comes to cybersecurity, many countries, including the U.S., are handled by intelligence agency and

these intelligence agencies, they do not want to share information. And so if you have the information and if you are able to analyze the information, many of the intelligence analyzing companies in the U.S., they use the AI. And when the U.S. has this information, if the U.S. is willing to share this information and send it to other nations so that a partnership could be more effective, I think there's a need for confidence building amongst different nations. Once you are willing to share your information, the other party would also be willing to share their information with you.

MR. BAKER: Do you see that the sharing is not happening? I mean, this was an issue before 9/11 in the United States and with our foreign partners. When 9/11 happened there was a breakthrough with respect to information sharing and people adopted a different mentality. Do you see not enough sharing in the international arena right now as well? And why do you think -- if so, why is that different from what's happening in the CT area?

Kate?

MS. CHARLET: So I can start. First of all, you always want more information sharing, although caveated with quality information sharing, with caveats in having to be timely. I think it's notable that DHS first heard of WannaCry from Asia-Pacific partners. Jeanette Manfra talked about that when they announced the attribution in 2017. So I think that alone shows you the value to include specifically between -- with countries in Asia-Pacific. And a large part of my role at DOD was try to expand the relevance and to kind of elevate the role of cyber-related partnerships, whether that was in the Gulf or in Asia or Europe. And one of the major needs and major focuses of those kinds of partnerships has to be information sharing. And it's not just militaries. It's law enforcement. It's the CIRTS. Most countries have CIRTS that do information sharing on cyber threats. In our case, through the NKIC. So yeah, I mean, I think that only needs to

continue and expand.

MR. BAKER: Michael?

MR. SULMEYER: Briefly, I would just say find a focus on the sharing as the verb, but for baseball fans in the room, what good is recruiting the best pitcher if you haven't got a catcher? Someone has got to be able to receive the information and actually employ it and use it wisely. And that is often lacking. We spend so much time saying we need to share more, but when you look at what you're actually able to do with that which you shared, that's a pretty depressing answer.

MR. BAKER: Okay. Other questions?

Sir, right here in the front. I guess it's the middle.

MR. SHEA: Dennis Shea with the Center for Naval Analyses.

Can the panel respond about the appropriateness of responding to cyber with cyber? But in light of, you know, not wanting to escalate, not wanting to get in for a tit for tat, not wanting to reveal cyber capabilities that this country might have, and yet you want to send a strong message to stop the bad behavior; just cut it out.

MR. BAKER: Michael, let's go to you first. You've written about this topic. What do you think about that?

MR. SULMEYER: We I don't want to wait to be in a responding posture. I want to get -- before you ask your question, I want to say, what can I do to cut it off before it hits me? And that's the degrade part. Now, because the space is very active anyway, it's going to be taken as a response.

But just as a matter of course, I don't see a problem with using cyber operations to either preemptively or in a response fashion degrade how another guy hacks. Now, realize there are limits. I mean, if you want to have a larger impact on national decision-making, if you want to talk about deterring future work, you're going to

have to do a lot more than that. But there's no reason to dismiss the offensive cyber operations as an opportunity to contribute to them.

MR. BAKER: Can I ask a question about that?

Do you think we're smart enough to do that? In the following way: Do we -- the folks that will deploy such technology, let's say, or such activities, or engage in such activities, will they be able to understand the collateral consequences of unleashing a particular cyber tool in a particular context? DOD, the military has a lot of familiarity, obviously, with kinetic weapons and what they do and what you can expect and what the blast radius is of an ordinance of a certain size, and they can understand that they can think about that and they can factor that into their thinking to make sure that they're doing things consistent with the laws of armed conflict. But when you start talking about offensive operations, are we really smart enough to really think through all the collateral things that might happen once you unleash one of these things?

MR. SULMEYER: Yes.

MR. BAKER: And why so?

MR. SULMEYER: Lawyers are everywhere throughout the national security establishment.

MR. BAKER: But are the technologists smart enough to understand, to be able to have those conversations with the lawyers to go through that analysis?

MR. SULMEYER: Yes. And if you want a data point for doing work on this at home, Kevin Mandia did a talk, the guy Mandiant is named after. He very humbly named it after himself. Anyway, he said, look, you compare worldwide employments of this stuff. The Western countries tend to be very clean and very precise about the way things are written to have tailored effects. He said, outside of that it's a much more wanton level of disruption. So you can compare NotPetya with other things. Not

NotPetya.

MR. BAKER: Okay. We'll go to you next and then Professor Lim. What do you think about offensive cyber operations? Active defense, that type of thing.

MS. CHARLET: Well, so to the original question of cyber on cyber, I mean, there's nothing inherently right or wrong about that, right, it's, what is the appropriate tool to respond? And that may be cyber operations or it may not be. I don't think there's anything that's inherently and exclusively symmetrical about responding to cyber with cyber. If you're, you know, because you were talking a little bit about escalatory capacity. I think you could easily identify noncyber operations that are equally or maybe, you know, or less escalatory.

I think to the other question, the conversation with Michael, I mean, we have shown, you know, in my experience, a lot of ability to identify where every possible risk could come from. I don't think that we have a mature way of like getting to the reality of it, which can -- maybe it results in underestimating risk, but just as often I think it is overestimating risk. So one of the challenges that I still see is not like the creativity of imaging what could happen; it's in having the ability to make real solid evidence-based decisions about it.

MR. BAKER: Okay.

Professor Lim, offensive cyber activities?

MR. LIM: When it comes to war, if there is an attack, we can self-defend; right? We can employ whatever method we believe is appropriate. And we will always have to think about the collateral damages to take place whenever we make decisions. When it comes to cyber, Stuxnet in Iran back in 2010, other than that, most cyberattacks are espionages. So when it comes to the people getting hurt, I don't see how people would be physically hurt but there would be loss of information and data. So,

but just because there were damages from cyberattacks, I think it's really difficult for us to actually use conventional forces to counteract cyberattacks. So how many countries are really able to employ or deploy cyberattacks? Russia, China, North Korea, and Iran. Other than those countries, we don't have too many other actors. We can in South Korea, also employ some cyber tools, but we really don't have enough firepower in cyberspace to counteract or to provide for penalties against these attackers.

So that's the problem. The attackers have a lot of tools at their disposal. The defenders do not have a lot of defensive mechanisms. So we are limited by technology that we have. So do we really need to rely on conventional mechanisms? That's a question for us to answer later.

MR. BAKER: So just with respect to the theft of intellectual property or these ransomware, these bitcoin things we were talking about earlier, I can't remember which speaker in the morning talked about it, but if you have a group of North Koreans in a warehouse in Mozambique, would it be appropriate for someone in the United States, Korea, elsewhere, to simply engage in an offensive activity, which is just shutting off their Internet access, for example, or disabling their computers in that warehouse, assuming you could identify it, and just disabling it, shutting off their access? Not because they're engaged in war or military-type activities, but if they are engaged in theft, ransomware, that kind of thing, what do you think about that?

MR. LIM: Well, if North Korea were to carry out attacks against South Korea or the U.S., they would actually be doing it through a third country. They would be using a midpoint. And so, for example, Southeast Asia, and maybe sometimes in China, through their operatives. So if we were to try to address these issues, they would be actually in control of tens of thousands of servers and units. Are you sure you are pinpointing at the possible inflictors, attackers? I don't think so. We don't have the

technology for that. We just don't have enough technology. Maybe the U.S. does, but we need to have higher upgraded weapons when it comes to cyber defense. Or even if it's a preemptive measure that is to be taken. And if the U.S. has such technology available to it, I think the international community could be somehow benefitting with the technologies the U.S. has. But we don't have the parity that was spoken of earlier yet.

MR. SULMEYER: I'm not so sure I'm seeing that there needs to be a revolution in defensive technology. I mean, it's largely, not wholly, but largely about doing the things we know we should be doing. I don't mean that on the individual level, but I mean at a corporate enterprise level, and being forced to live with some inconvenience and some expense to get that going. So I guess I'm less convinced that there's just a magic defense box that the United States has that we're not sharing. (A) We're not doing such a brilliant job of it ourselves anyway. So, yeah, that would be my main reaction there.

MR. BAKER: Kate, before we go on, anything on this now? Okay.

Sure, sir?

MR. WASHBURN: Hi, Rhyner Washburn. I'm with the National Consortium for the Study of Terrorism and Responses to Terrorism, and I'm also with PWC, PricewaterhouseCooper.

So I'm very concerned about this hack back that you keep talking about. In a sense, the ability to disrupt an adversary's cyber operations. This cyber to cyber. Coming from a practitioner's standpoint, I've seen where it goes, and I think when you're talking --

MR. BAKER: What do you mean? Where does it go? What do you mean by that?

MR. WASHBURN: So nation state actors, like Iran and so forth, they are

developing their own ruleset, especially with regard to being hacked or if they are being -- if they engage in an operation and then someone hacks them back, it's not necessarily cyber to cyber. It's cyber to ICS. It's cyber to your SCADA systems. When you have malware that is being developed specifically for ICS, you're going from a talent pool of hundreds of thousands of people in IT cybersecurity to less than 20,000 in ICS security. So when you're doing a hack back, you may not physically resource and personnel-wise be prepared for that, you know, offensive cyber capability. I mean, when you look at nuclear power facilities, when you look at hydroelectric stations, these are prime targets. And kind of borrowing a term from Professor Lim, these are pain thresholds. This is something that nation states will exploit. And I'm just kind of concerned, like, from the panel here, do you feel that if we exploit this hack back, do you think that nation states -- I don't know, do you think they will --

MR. BAKER: Is there sort of an escalation?

MR. WASHBURN: Yeah.

MR. BAKER: Yeah. So --

MR. WASHBURN: Is there a measure to stop that?

MR. BAKER: We'll start with that. Do you want to --

MS. CHARLET: Michael first.

MR. SULMEYER: No, Kate must start with that.

MR. BAKER: Do you fear escalation once you start? It'll be a continuing ratcheting up of the issue as they get angry about us doing this? Is that the best way to go? What do you think about that? And then we'll go to Michael.

MS. CHARLET: I mean, we've always feared that. But sometimes I think that fear is, you know, in that category of overestimated risk. I mean, I think any time you have to take the specifics of the proposal and think about it specifically in the

context of the adversary or whoever you're conducting the operation against, and I mean, I, you know, I do think that there is a role for us in making sure that, especially -- well, let me back up. It's also temporal. Right? If you're seeing an impending cyberattack, like, why wouldn't you try to stop that attack when it's heading on the way to critical infrastructure? So I think what Michael is talking about is in much earlier stages, but I think it really draws out the temporal aspect where that's how imminent something is, what signals you're seeing that there's an impending cyberattack. All those things are going to factor in. And so, yeah.

MR. BAKER: Michael, what do you think about escalation? And then also, just to clarify, when you're talking about this, are you thinking about governments, like the U.S. government, the South Korean government, taking these types of actions? Or do you think it makes sense given how slow the governmental process is in making these kinds of decisions, does it make sense to limit this kind of activity to governmental agencies, or is this something that the private sector should be able to do on its own which it can't do now?

MR. SULMEYER: Correct. Yeah, it's a little misleading to term this, what I would talk about as hack back, because that is the term that's applied mostly to private companies, usually victims, deciding how they're going to hack back at whoever did it. That is not what I'm talking about. I am talking about governments, our government especially, trying to get ahead of an impending, incoming attack, or problem, or intrusion, and degrading the adversary's ability to do that.

The question about escalation I find interesting because the adversaries are escalating already without us doing this. They already are -- there are public DHS reports attributing specific nation actors to doing this already. What is it that isn't happening already short of them pulling the trigger? At a certain point you wonder if we

just do not want to act because we're too risk adverse. That's a very senior policy level decision then you're going to have to make, but I want options on the table to be able to make sure a decision maker knows, hey, if you don't want to tolerate this anymore, you can go break it down. And yes, they may retaliate. They may tit for tat. Guess what? We go break more of their things again. We prevail over the long term. This is not a single engagement. This is a recurring engagement to prevail.

MR. BAKER: Professor, yes, please.

MR. LIM: Preemptive attack requires you having a clear indication and that the attack is imminent. But as an expert in the field, I don't think you can know. There are not going to be signals that these attacks will take place. When you talk about hack back, this is actually illegal in Korea and probably also in the U.S. And Tomahawks cost about 10 million per head, and so do you really want to use $10 million to penalize some attacker? You can actually employ many people, thousands probably programmers to cyberattack back instead of sending a Tomahawk. So for cyberattacks, you will have to respond cyberly.

MR. BAKER: Okay. We are almost out of time. Maybe one -- is there one last quick question?

Yes, sir?

MR. SHANK: Shawn Shank with BNY Mellon.

This question is primarily for Professor Lim but if the other panelists would like to chime in, please do.

What realistically do you think the prospects are for cyber being incorporated into an agreement that would formally conclude the Korean War? And for an agreement of that kind with cyber as an element, how would you envision verification measures actually working?

MR. LIM: Well, in Korean and South Korea there was a communique from Panmunjom in all spaces that there would be no act of provocation, and that was the agreement. When it comes to all space, that includes cyberspace. And one of the powers that the North Koreans have is cyber. And if North Korea were to give up their nuclear capabilities, then now they have cyber capabilities that we need to deal with. And if North Korea would be willing to give up nuclear capabilities, well, why not cyber? Nuclear by any means is big. Bigger than cyber right now. And as such, if North Korea were to turn their cyber capabilities for peaceful purposes, for economic prosperity, I think they would come to realize that they would have more to gain through these peaceful means. And for Microsoft, they have over 3,500 people employed for cybersecurity, so I think North Koreans would be able to realize that by turning the 10,000 or so operatives into cyber economic workers, I believe they would be able to see that there would be more positive to come from such transition. There is a Kaesong industrial complex where North Koreans are working north of the 38th Parallel, and they have gained quite a bit of economic advantage through employment of North Koreans at the Kaesong industrial complex. They can work for North Korea, and also, they can come down to South Korea maybe.

MR. BAKER: Okay. Well, thank you. I'd like to thank our panelists from this afternoon. I appreciate your comments and your thoughts and your time, most importantly. So thank you. Thank you very much.

And I'd like to thank all of our panelists and speakers. Chris, thank you very much for your comments this morning. Jung Pak, thank you for setting all this up. I appreciate it. Thank you for the invitation to do this. It was very interesting and informative. Horrifying in many ways, but in a good way. So thank you very much.

And also, Paul Park back there. Wave your hand, Paul. Yeah, so thank

you for helping with all the logistics for everybody.

So on behalf of the Brookings Institution, thank you to the audience for coming in. We greatly appreciate it.

(Applause)

MR. BAKER: Thank you, and have a good day.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020