DR. JOHN PARK: Welcome to the final day of the 3rd Harvard Korean Security Summit. My name is John Park, Director of the Korea Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs. We have an excellent roster of speakers for you today. For our day three keynote remarks, it's my pleasure to introduce Jean Lee. Jean is a veteran foreign correspondent and specialist on North Korea. She led the Associated Press's coverage of the Korean Peninsula's Bureau Chief from 2008 to 2013. In January, 2012, Jean opened AP's Pyongyang Bureau. She has made dozens of extended reporting trips to North Korea in that capacity. Jean currently hosts the BBC World Service's Podcast Series "The Lazarus Heist." Over to Jean.

JEAN LEE: I want to start by thanking John and Alex and the Belfer Center at Harvard for inviting me to take part in this conference. And thank you so much for focusing on North Korea's cybercriminal statecraft, because I think North Korean cyber is still a blind spot in traditional policy circles. And I do think that that's a vulnerability that the North Koreans prey on and take advantage of. So I, myself, welcome every opportunity to bring together fresh thinking from different disciplines, to get us closer to understanding North Korea's cyber ambitions.

So I am just going to start by saying I am not a cyber expert. My background is in journalism. But I did spend a lot of time in North Korea as a journalist. And this was during the last few years of Kim Jong-il's rule, and the first few years of Kim Jong-un's rule. And as you all know, going to North Korea always feels a little bit like you're going back in time, that you're stepping back in time, in so many different ways, from losing cell phone access, and being cut off from the outside world, not having internet access. But I have to say, it's when you travel outside the capital, that you feel this most keenly. Because forget about internet access. You also don't have electricity, or running water. And this is the kind of place where, when the sun sets, that's it. You go straight to bed.

So, you know, during this period, as I was going out to the countryside, and seeing the disparity between what we see in state media and what we see on the ground, I was also keeping my eye

on what was happening with Kim Jong-un. And I did see something happening, and that was a growing investment in science and technology. Computers, cell phones, digital devices of all kinds. You know, during those years, they even came up with a song, the song of C&C. It was so addictive. It was an ode to computerization. I even tried to learn the steps that came along with it. There's a very specific dance.

And, you know, Kim Jong-un, when he first was unveiled, he wasn't well known at all. He had been kept under wraps. And so my staff would also go to these study sessions. And he's being portrayed as this computer genius. And we could see, at the time, that he was unleashing this very concerted campaign to win the younger generation, win their loyalty with science and technology. He was promising them a better path to the future, using computers.

And I think that this is a good reminder. He is a millennial himself. Kim Jong-un is a young man who was educated abroad, and understands the way that the world was headed, in terms of technology. Even if he's cut off his people's access to the outside world and to the world wide web, he has had access. He understands how it's used. And he wants to incorporate it into his strategy.

And so, during these years when I was in North Korea, seeing all this unfold, I could not help but wonder if there was a darker side to this push for technology. And that did prompt me to consider how he might be looking at cyber as a new modern form of warfare that fits into this legacy that he is trying to build. And so, with the "Lazarus Heist" podcast, I've teamed up with a tech journalist, Jeff White. Now Jeff understands this stuff better than I do. He explores and explains how the North Koreans carry out these cyber attacks that they are accused of masterminding. But I am actually interested in exploring why. Why have they invested so much in creating some of the world's most aggressive and ambitious hackers? Why should that ambition scare us, concern us?

And so season one of the podcast was built around three major cyber attacks that have been pinned on the North Koreans. The Sony hack, the Bangladesh Bank heist, and the WannaCry work ransomware attack. And we did write it as a true crime series, almost like a bank heist. That was what we had in mind. And while the cyber attacks themselves, they serve as a narrative frame, in between, we were able to really explore the history, and the present-day life in North Korea, that I think are really important to helping us understand and put the cyber attacks into context.

And that includes understanding who the Kims are, what their vision for North Korea is, and how they aim to get there. But that strategy does include nuclear weapons and the challenge of raising the funds and producing the parts that are needed to build that program in the face of heavy international sanctions.

And so, you know, one of the other things I wanted to do is also to put a name and a face on these people. Hackers are always these shadowy figures. But I wanted to bring them to life, to make them real. And that comes from a real understanding of who they are. Because I spent a lot of time in computer labs with these young men, possibly some of the young men who are serving as Kim Jong-un's cyber warriors today.

And so I do think about these young men, and what it would be like for them to be given this mission to go abroad and make money for their regime. The pressures that they're under. They're not teenagers in a basement doing this for fun. They are doing this for the state. And that is a very different kind of pressure. I know how clever and also unsophisticated they are. I mean they are from a nation that is possibly the most isolated.

And so, how do they become savvy enough to target us the way we use the internet? And so that is also another fascinating part of the podcast, is trying to understand how they transform these men who have been so cut off, and really been raised in a principle of educating them about computer science, into people who use the internet the way we do? And I think all of that also

helps us understand not only how ambitious they are, but also how clumsy they can be at times. And that might help explain some of the footprints that they leave behind, that help us get to them as the potential source of these hacks.

And so I don't think that they figured out every step—I don't think they figured out every step of this process. And certainly, the drop in the value of cryptocurrency is something that they must be grappling with right now. But we do know, that will be a blow. What we do know is that they have the ambition and the state support to try to figure out how to get this money back to Pyongyang. And I think it's up to us to really put our heads together to decipher who they are, what their mission is, and what we need to do, to stop them.

So I'll just say one last thing, is that I am a storyteller. I use the "Lazarus Heist" as a platform, as a way to reach millions of listeners around the world, to get them interested in North Korea. It's been downloaded in every country but North Korea. But I rely on you, all of you speaking today, to do the heavy lifting with the research. And so I look forward to learning from all of you today in today's session. Thank you.

DR. JOHN PARK: Thanks to Jean for those great remarks today. It's a terrific scene setter for our panel. Before turning to panel three, I invite our speakers to turn on their video, and mute their audio. Our panel today will examine North Korea's cybercriminal statecraft activities, with a group of leading experts from a think tank, government, and private sectors. Alex O'Neill, the co-founder and co-head of the Korea Project's North Korea Cyber Working Group, will be moderating panel three. And he'll be introducing our speakers shortly.

Alex's work focuses on North Korean financially motivated cyber operations, as well as its links between North Korean and Russian speaking criminals. His most recent Harvard publication is *Cybercriminal Statecraft,* the very title of our panel, where he looks at the North Korean hackers' ties to the global underground. Alex holds an MSC in Russian and East European Studies from the University of Oxford, and a B.A. in history from Yale University. Over to you, Alex.

ALEX O'NEILL: Thanks John for that generous introduction. Good morning and good evening everyone. Thank you very much for tuning in. As John mentioned, my name is Alex O'Neill. I'm an associate here at the Belfer Center, where my research focuses on North Korean financially motivated cyber operations. I'm also a co-lead of the North Korea Cyber Working Group and the coordinator of the Korea Project.

It's my great pleasure to welcome you to the third and final panel of this year's Harvard Korean Security Summit, entitled, as John said, "Addressing North Korea's Cybercriminal Statecraft Activities." We have a distinguished group of four expert panelists, hailing from government, the think tank community, and the private sector, who I'll introduce in just a moment. But first, let me say a few words about the subject of our panel today.

The term cybercriminal statecraft refers to North Korea's pioneering model of using state cyber capabilities to generate illicit revenue through theft, fraud, and extortion operations. As the UN Panel of Experts on North Korea has reported, and as Foreign Minister Park said in his opening remarks on Tuesday, North Korea appears to use the proceeds from the cybercriminal activities to blunt the impact of sanctions, fund its WMD and ballistic missile programs, and reinvest back in the cyber program.

While a growing number of countries use cyber capabilities for malign purposes, for now, North Korea stands alone as the only state known to generate illicit revenue through cyber means. The proceeds of North Korea's cybercriminal operations have been alarmingly high. Chainalysis, Ashley's firm, reported in January that North Korea had stolen more than $400 million dollars' worth of cryptocurrency in 2021 alone. This past March, North Korean hackers stole more than $600 million dollars in an operation targeting the Ronan Network, which supports a popular online game.

They've been tied most recently to a major operation targeting the crypto startup Harmony's Horizon Bridge, which reports say may have stolen as much as $100 million dollars in cryptocurrency assets. While the costs of laundering and converting cryptocurrency into fiat, as well as the recent crypto downturn, certainly eat into the hackers' net profits, these are difference-making inflows for North Korea. In sum, North Korea's cybercriminal statecraft has been, and seems likely to remain a critical issue for global security, especially from the perspectives of the US and South Korea.

With that background, I'll now introduce our four panelists. First we have Jason Bartlett, a research associate in the Energy, Economics, and Security Program at CNAS, where he analyzes developments in trends and sanctions policy and invasion tactics, proliferation finance, and cyber naval financial crime, with a focus on North Korea, as well as Iran and Venezuela. Jason is also a contributing author for *The Diplomat* and a member of our North Korea Cyber Working Group here at the Belfer Center. It's great to see you, Jason.

Next we have Ashley Chafin-Lomonosov. Ashley is a cybercrimes investigator at Chainalysis, a blockchain data company that serves the public and private sectors globally, in order to enable investigations and compliance in the crypto space. Ashley's work focuses on East Asian issues, particularly DPRK's tactics, techniques, and procedures on the blockchain. Prior to joining Chainalysis, Ashley served in the US government. Welcome, Ashley. Great to have you.

Also joining us is Saher Naumaan. Great to have you back with us, Saher. Saher is principal threat intelligence analyst at BAE Systems Applied Intelligence, where she researches state-sponsored cyber espionage. Saher specializes in analysis covering intersection of geopolitics and cyber operations, and has produced a number of critical reports on North Korean financially motivated threat actors, including tying them to Russian-speaking cybercriminal groups. Thanks again for joining this evening, Saher.

Finally, we have with us David Park, a senior policy advisor in the US Treasury Department's Office of Terrorist Financing and Financial Crimes. David currently advises senior leadership on policies and strategies that utilize Treasury's tools to compete against China in the national security context. He has expertise encountering illicit financing, money laundering, financial crime, corruption, and human rights abuses on the part of China and North Korea. Previously, David served as the first US Treasury Representative to Korea, advising on North Korea sanctions, economy, and illicit financing, as well as seeking ways to work cooperatively with ROK institutions, to enhance the pressure campaign on North Korea. He earlier served in the office of Senator John Donnelly and in the US Air Force. Thanks very much for joining, David.

So to kick off our discussion, I would like to ask a little bit about how we got here. How has North Korea managed to develop advanced cyber capabilities, especially considering the ongoing sanctions? How did North Korean threat actors become major players in the cybercrime space, especially with regard to stealing cryptocurrency? And Jason, we'll start with you.

JASON BARTLETT: Sure. First, thank you very much, Alex, Dr. Park, and the Belfer Center for this opportunity to join such a distinguished panel. I think I'll start first with your comment about how did we get to where we are. As it comes to basically anything about North Korea, it's the hardest of hard topics. So it really comes into effect the importance of bilingual investigations, and understanding Korean and English, which is very helpful when you're doing this type of research. Because most of the records that are most prominent to how North Korea started cyber will naturally be documented in Korean.

So, according to publicly available sources, North Korea really started creating the cyber program around 1984 and 1986, which also kind of ties into what Jean was mentioning about Kim Jong-il, and how that started then. There was something called the creation of the Mirim College or [KOREAN], which was one of the first kind of state-created establishments to focus on cyber, and kind of weaponizing the ICT and science and technology kind of explosion of interest. And North Korea was having to focus more on cyber. And then that continued

throughout the '90s. We saw more universities being created, the Korea Computer Center, Chosun Computer Center, which the Treasury very rightfully sanctioned many years later for actually being responsible to send North Korean IT workers abroad, to evade sanctions. So it started in the '80s, mainly focused on ICT and IT in general, information technology and that form of cyber.

And the mid-2000s, late 2000, it started to be more offensive, and target South Korean government infrastructure, some financial infrastructure, but it was mainly the government, more political, military type of infrastructure. And then we saw, in the mid 2010s, around 2014, there was a shift to financial institutions globally. And then, 2016, with the explosion of cryptocurrency, namely Bitcoin, then we saw this massive movement towards financial technologies, cryptocurrency blotching technology.

Then there was also records of the South Korean Intelligence Agency declaring that about 90 percent of all their cyber attacks they suffer from are from North Korea. And about 40 percent of them target the financial sector. So there clearly has been this evolution that, despite North Korea being the most isolated country in the world, Kim Jong-un is very aware, as his father was, of acute changes in global finance and the global financial system and in global economics. And they saw that cyber would be an area that it could possibly use to have this asymmetric comparative—competitive advantage to the United States and South Korea.

And then, with the explosion of financial technologies, and their need to evade sanctions in a more creative way, targeting cryptocurrency and using cyber financial crime really seemed to be the best way for them to do so. And that's kind of how we're now at this point, where North Korea has become the greatest state sponsored threat to the global financial system.

ALEX O'NEILL: Thanks for that, Jason. A really great overview. Ashley, I want to go to you next, for your take on basically how we got here today, how North Korean threat actors became major players in the cybercrime space, especially with regard to stealing cryptocurrency.

ASHLEY CHAFIN-LOMONOSOV: Thanks, Alex. As you indicated earlier, DPRK had—I think we're calling it a banner year—last year, in 2021, where they stole over $400 million dollars worth of cryptocurrency from unsuspecting victims, truthfully. In the first three months of this year, we noted, like, $1.3 billion dollars, or something extremely high like that, in all sorts of theft. But, as the year has continued on, we're tallying DPRK's total at about a billion now.

So already, despite the crypto winter that we're seeing now, we're seeing that DPRK is not laying up. So how did we get here? They've consistently advanced. And, despite any effort for sanctions, and you know, a general industry trend towards stopping illicit activity on the blockchain, they've remained dynamic in their actions. And though cryptocurrency tracing, and all sorts of botching activity is technically transparent, it's never truly anonymous. And, from start to finish, we're seeing DPRK steal, even though we're in a crypto winter, more than ever.

ALEX O'NEILL: Thanks Ashley. So I want to put a follow-up to you, Saher. How sophisticated would you say North Korea's cyber capabilities are, especially with regard to cybercrime? And how would you say that they measure up against what we know about other countries' capabilities, especially Russia's or China's or Iran's?

SAHER NAUMANN: Yeah, sure. Again, thanks to the Belfer Center and Alex and John for having me. So yeah. I think a lot of people look at Lazarus and kind of North Korean activity, and think that's pretty high capability. And in a lot of ways, it is. I think that what we've seen from our investigations over the years, is that they are quite interesting and novel and creative techniques that they've used.

I think one of the big things about Lazarus is kind of the amount of in depth research that they do, in terms of the systems that they're targeting, and kind of the ways of getting access to them. And I think that has really helped them. But, on the flip side, their sophistication definitely has limits. There's a lot of instances across the different kinds of activity where we've seen a lot of

operational security mistakes in their code. For example, things like implementing encryption, some of them are basic, and some of them are a little bit more complex. But given the kind of frequency that we've seen those kind of mistakes, I would say that, compared to Russia and China, you would probably see less of them from those countries.

I think the reason why it comes across that Lazarus has very strong capabilities, and especially is because of the state-backed kind of resources. So just the amount of effort, and time, and personnel, and money that they have to put towards these kind of activities, is kind of why those capabilities come across. And to be honest, if other governments, like Russia or China, were interested in financial gain, and kind of making that kind of money as part of a state enterprise, they would absolutely be able to compare, if not exceed, what Lazarus has done.

But that isn't necessarily their end game. There's more kind of espionage, sabotage, et cetera, kind of a strong chase for them So I think it is—Lazarus is a very capable actor. But again, we have seen kind of ways that they have fallen short, I suppose. And that doesn't mean that they haven't been successful. I think those are kind of two different things. But that has obviously provided us a lot of ways to track them.

ALEX O'NEILL: Some great points, especially on that comparison. And if other countries were applying that same effort, that same amount of resources on what they could do. David, I want to ask you the same question about comparing what we know about North Korea's capabilities, with what we know about Russia or China or Iran or other countries, for that matter. From your perspective, as one with a lot of experience working in government, especially on the financial angle, how does North Korea measure up?

DAVID PARK: Thanks for the question, Alex. And thanks again to the Belfer Center, Dr. Park, and Alex for all your efforts in hosting this panel. Let me, before I answer that question, let me just start off, since I am a current US government employee, that the views expressed are

those of my own, and don't necessarily reflect those of the US Treasury Department or the US government.

So let me go ahead and answer that question. You know, as Saher said, I think North Korea is probably one of the most capable cyber actors out there, especially when it comes to financial heists, or cyber attacks. I think that compared to other countries like Russia, China, or Iran, they are probably one of the most capable. And the reason is, as the other panelists have mentioned, is that for the other countries like Russia and China, they have a very—they're more plugged into the international financial system. They have a lot more that they can tap into, in terms of being able to procure resources. They have various means of exporting goods and services.

Essentially, North Korea doesn't have that. They have a limited amount of things that they can export, particularly in the goods and services industry. And when it comes to demand, there's just not a great demand for North Korean goods. As I'm sure everyone here knows, North Korea makes a litany of knockoff items, right. But they're not the highly sought knockoff items, right. And so I think these are some of the challenges that North Korea faced, hence their investment into crypto or cyber attacks. And that's why we see a consistent or constant effort by the North Koreans, unlike in Russia, Iran, or in the case of China.

We also have to take into account, when it comes to Russia and China, they're bigger actors, right. They have bigger strategic goals. It's not necessarily to steal monies, so that they can use to fund various projects that the regime wants to advance. But really, it's to peck away at strategic advantages the US has, particularly in the financial system, but also in other areas.

ALEX O'NEILL: Thanks for that, David. And I'm picking up on a kind of ominous theme based on the comments from you and Saher, that basically it could be a lot worse if Iran or Russia or China or other countries really applied themselves in those areas, that there could be a lot more damage done. I'd like to ask a related sort of two-part question. And Jason, we'll start with you on this one. First of all, what are we underestimating about North Korea's cybercriminal

capabilities? And second of all, what are we overestimating about North Korea's cybercriminal capabilities? Jason to you first.

JASON BARTLETT: Sure. Thanks, Alex. I'll start with the underestimation. I think everyone who's on this panel and watching does not underestimate North Korea. So I think that's very positive thing. I think their access. So yes, they are cut off from the US financial system through very powerful US/UN sanctions, and also other statements and designations from the State Department. However, they're still evading sanctions. They're arguably probably the best sanction evaders that the world really has ever seen, because they've been having to occupy in this space for decades.

And they might not have access to the greatest hardware to conduct these cyber attacks, like Macbooks and things. But you don't need a Mac to hack. And I didn't intend to actually rhyme like that, but it's very true. I mean there's many reports saying that some of the largest cyber attacks we're aware of, like the Sony Pictures and Bangladesh, were from very basic computers that could have possibly been located in hotels in Southeast Asia, right. And it's very hard to actually pinpoint that to an exact location. But you just need good coders, people who know computer science, and a group of software.

The North Korea reuses its malware, but it's still effective, because they rely on human error. And I think that's something that people tend to miss, is the majority of North Korean cyber attacks, cyber intrusions, however you want to color it, starts with email phishing campaigns, social engineering. So that can be an email offering a job application, contacting someone through LinkedIn, Twitter, Facebook. And then they input malware, a virus in an email. And then you download it. And then they'll be able to control your system.

And that's something that I think is highly underestimated, is human error. And that's what North Korea preys on, is human error. You don't need an advanced computer. You don't necessarily need an advanced technological society to be very good at cybercrime. And I think something

else to point out is, I personally don't think North Korea necessarily needs to be completely clean, because it doesn't really care about attribution. In the case of China, Iran, Russia, they're mainly doing information espionage, hacking into government systems.

North Korea is not going to do that, because they're really after money. And it doesn't really have the same diplomatic damage by doing something like that. So even if you find out it's North Korea, we're most likely never going to extradite a North Korean and charge them on US soil. It's only happened a handful of times. So I think they understand that there are legal limits of sanctions. There are legal enforcement limits. If they're conducting this activity in China, Russia, or other countries that don't care about US sanctions, then that doesn't really matter. I am not, in any way, kind of dissing the strength and importance of sanctions. But sanctioning more North Korean targets will not change North Korea's behavior. You need to target third parties or technologies that are helping North Koreans evade the US system. And I think that's an under—a misconception or underestimation of North Korea, is that they're able to get around anything. So you have to then start targeting people that are allowing them to do that.

The overestimation of their strength, I think, is this fact that, "Well, there's nothing we can do." I think there's a lot we can do. There's a lot we can do with South Korea, which continues to be the number one target of North Korean attacks. But there's a lot of other issues that go into working with Seoul on this, because they have a very different approach, politically, diplomatically, logistically, to dealing with North Korea. They only have one agency that deals with North Korea. And that's their intelligence agency, right. So US, we have FBI, Treasury, State Department, DoD, basically any agency can do something about it. So that's a different question. But I think one of the overestimation is that, "Well, there's nothing we can really do." There is a lot we can do. We just have to work with our partners. And that requires a deeper understanding of how countries deal with North Korea.

ALEX O'NEILL: Thanks for that, Jason. And someone is going to poach that line, "You don't need a Mac to hack" for a paper title or something like that in the near future. Saher, I want to

ask the same question to you. First of all, what are we underestimating about North Korea's cybercriminal capabilities? And the flip side, what are we overestimating about their capabilities?

SAHER NAUMANN: Sure. I might start the other way, only because I have less for the overestimating. But I think it's kind of what I mentioned before. I think one of the things to remember is that, you know, at the end of the day, like when we discuss any threat actors, we're talking about people, hands on keyboards, humans who are doing these kind of operations. It's not magic. You know, there is a lot of skill involved. But it's still humans. So again, like I was saying with these mistakes that we see, that can happen to anybody. So I think that is something that we've been able to exploit quite well. And so that's something to continue doing.

And overestimation, as well, I do think that, given kind of the extreme amounts of money that we see—we're talking, you know, billions of dollars over the course of years, and several heists, you know, that does seem quite daunting, as Jason said. So I do think that there are more things that we can be doing. So I agree, in that kind of respect.

But, in terms of underestimation, I think one of the things, actually, that is interesting, that doesn't get talked about as much, maybe because it doesn't have the big kind of financial heist angle, is that there's a lot of parallel campaigns that are happening at the same time. So you know, Lazarus is quite good at targeting the aerospace and defense sector in a lot of different countries of interest, like Russia for example. And you know, I think it's important to remember that they still have espionage capabilities. And they're still using them. You know, they're still looking to make nuclear weapons. Russia makes nuclear weapons. There is a lot of interest there.

And so we've seen good evidence of that kind of targeting. So I don't think we should underestimate their interest in defense. And despite the fact that they obviously need this kind of revenue generation, there is also kind of that research angle, in terms of like building their program as well.

And I think one of the things that Jason touched on, as well, was this social engineering side. It is still true, despite the different kinds of campaigns, and the types of activity that we see from Lazarus, the majority do start with phishing. But I think it is important to note that, you know, even though a lot of threat actors do that, Lazarus does take the time and care to kind of craft these kind of phishes, using different platforms, including LinkedIn, establishing relationships, switching over to WhatsApp. We've seen that before.

So I think there is kind of a lot of thought that goes into it. And just especially, again, as I mentioned, the in depth research, in terms of targeting the cryptocurrency sector, for example, the knowledge that they have of notable figures in the industry, to impersonate, to give the lures credibility, and awareness to kind of what parts of the DeFi system kind of often lie on the end user devices of developers. Just kind of this intricate knowledge of how those systems kind of work. And that's very similar to what we saw when they were targeting Swift systems. And the kind of details that they would have to know to access the alliance access servers, the Swift software that's running on those systems.

So I think just knowing that they have a lot of patience and a lot of time to invest is really important to remember. And the last thing I'll mention is that we've also, you know, given kind of the social engineering aspect of it. And we've seen them be quite bold about some of their targeting as well. So you might remember the targeting of security researchers, and you know, using these creative methods, you know, acting like they were looking to collaborate on some research. And you know, basically sending a payload that was a visual studio project file, and saying, "Oh, would you like to work on this with us?" But it was actually malware.

So they've gotten really creative. And again, targeting security researchers is probably a step further than a lot of other threat actors have gone. So there's kind of that bold element as well.

ALEX O'NEILL: Thanks Saher. Those are all really great points. And I just want to highlight one thing that you said a few minutes back. On the idea that North Korea has been targeting Russia and the aerospace and defense industries, things like that, I think that comment dispels the myth that there's a sort of—you know, some folks have lumped Iran and Russia and China and North Korea, broadly speaking, to this bucket of maligned actors who are targeting other countries, but not really targeting each other. And I think it's just a great point that you made that I wanted to highlight.

Ashley, I saw you nodding along at one point in Saher's remarks. And so I wanted to go over to you. Same question. What's your take on what we're underestimating about North Korea's cybercriminal capabilities? And on what we're overestimating about their capabilities?

ASHLEY CHAFIN-LOMONOSOV: Thanks Alex. Saher, that was extremely well said. Thank you. To her point, patience was my first answer for what we're underestimating about North Korea's cyber capabilities. So, as she stated, all of the hack victims, and all of the stolen funds victims have started with those phishing campaigns. And the patience there is that they take time, to not only build out a relationship with the individuals that end up either the target of the phishing scheme, or the overall target, in some cases, with smaller hacks in individuals.

They build up the patience to build their relationships, and then deliver the payloads. It's never—Well, it's very infrequently a random phishing email, though that does happen, and has happened recently. It's a very carefully concerted effort to build a relationship and establish that trust. So patience—and truthfully, patience is of the utmost importance, too, because we see that in their blockchain activity as well.

So some of the funds from the Ronan breach still haven't moved entirely. And we see that dating back to probably 2015 and 2016, at this time, too, where they have funds sitting in wallets idly, waiting to move. In certain cases in the past, too, we've seen them sit for 18 months, two years, four years at a time. And then, as it coincides with other blockchain activity, they move all the

funds at once. So it's certainly a calculated effort, too. Because while they could cash out, it also could be considered an investment.

You know, the Bitcoin that they stole in 2016 is worth a lot more today than they stole in 2016, even though we are in a crypto winter. So hackers can sometimes sit on funds for years. And we see that especially as it connects to DPRK, too. Other underestimated things, certainly the complexity of their attack vectors. So how deep they build their relationships. And it almost goes without saying this, but I know that North Korea punches far above its weight in traditional illicit finance money laundering, too, which I feel like David could probably speak very well to. We'd be mistaken to analyze and place its aggression on the blockchain, solely on the blockchain.

So as far as overestimating goes, we see an extreme and a very interesting lack of innovation. Truthfully, I spend a lot of my day researching DPRK's activity on the blockchain. And I have—Even though they have changed up some tactics recently, there is almost a predictable method to what they are going to do next. So, while their blockchain activity isn't always 100 percent predictable, we have a pretty good idea any time we see large amounts of funds, especially, what's going on.

So the only thing that we're probably overestimating is that their phishing tactics haven't change. There's some phenomenal open source and just collections of research out there with screen shots that very plainly state that DPRK's wonderful phishing emails are just malicious files. Very, very convincingly attached to emails. So sometimes we see that from—or sent to victims who are presumably receiving an email from another company in the investment portfolio, or a very, very familiar looking email address. So we aren't overestimating the creativity in their phishing, and their initial access and attack vectors. And, you know, education is key there. Please don't click on any suspicious links.

ALEX O'NEILL: Thank you for that. And David, I want to go to you. The same question, on what we're underestimating about North Korea's cybercriminal capabilities, and what we're overestimating about their criminal capabilities.

DAVID PARK: Yeah. I think the other panelists have all pretty much said what's on my mind as well. And they spoke quite excellently about it. So I won't talk too much about it. But I think, in terms of—I think what we're underestimating is, you know, if they're creative enough to evade our sanctions, and find new ways to secure revenue—and in this case, using cyber capabilities, and Ashley brought up a good point, right. They're not—They haven't been all that creative. Their methods have been, for the most part, similar. But I think what we also have to keep in mind is, if they're creative enough to be evading our sanctions continuously, and find new ways to generate revenue, then at some point, they're going to pick up on what we're doing, right.

We look at some of the actions that the US government, and specifically the US Treasury Department has done, and I'm not talking just about sanctions, I'm talking about some of the non-sanctions activities that we've done in the past few years, such as the DPRK IT workers advisory, the cyber threat advisory, with DHS, and I think FBI, the National Proliferation Finance Risk Assessment, there's a bunch of advisories out there that we've posted, that talks about, at a very technical level, talks about how North Korea conducts its cyber business, and what actors on the other side, so entities in the US or elsewhere, and individuals, what mitigation efforts they need to take to counter illicit North Korean cyber activity.

So in that sense, at some point, they're going to pick up, right. And we need to be—we have to constantly be vigilant about it, make sure we take the appropriate mitigation measures, and continue to do research on our end, to see how North Koreans are adapting. And so that's something that we shouldn't be underestimating, that they're a very capable group of actors, and that, at a certain point, they may be able to switch their tactics.

I think on the overestimating part, a little skip there. I think that there are plenty of folks here. And people like Ashley, Jason, Saher are doing excellent work, and wonderful work, that brings to light some of their illicit activities and the ways they do it. So I don't think we're at a point where we feel like we're overestimating. But I do think that perhaps we may have this kind of lull, if we don't hear about certain heists, whether they are because they're smaller amounts, compared to the 620 that were stolen in March, or most recently, the $100 billion from Harmony, then people might feel like, "Oh well, you know, maybe the North Koreans have stopped partaking in illicit cyber activities."

And that's where potentially we could be overestimating, just the sense that, because we don't hear about it in the news, or because they're doing heists of smaller amounts, that you know, we think that they've decided to kind of scale back on their activities. Or maybe their tactics have been thwarted because of the efforts that people in the US and elsewhere have taken to mitigate against North Korea's illicit cyber activities.

ALEX O'NEILL: Thanks for that, David. So David, I want to come back to you for a moment. But if we could get just a bit more technical for a minute. A couple of you have mentioned that North Korean hackers have a reputation for boldness. I think Saher, you used that term, both in terms of financially motivated operations, and in terms of non-financially motivated operations, right, like Sony Pictures Entertainment attack for example. But they also have a reputation for some sloppiness, again, as a couple of you mentioned.

Folks will recall, for example, that in the Bangladesh bank heist of 2016, that operation failed in part because of a typo in the fraudulent wire instructions North Korea sent over, that raised alarms to the New York Fed. And so my question for you all, and again, starting with you, David, is have we seen significant advancement over the last few years, in terms of North Korean threat actors' TTPs, their tactics, techniques, and procedures? Have their tools improved? Have their behaviors changed? Or has it been more of just they're still trying sort of what they've always been working with for the last half decade or so? David, over to you.

DAVID PARK: Yeah. And I'll defer to technical aspects to the experts like Ashley, Jason, and Saher. But from what I've seen, you know, from within Treasury, I think that's—You know, we still see shades of the sloppiness, right. But I think they're getting better. And one example that comes to mind, this is a little bit more in the IT worker space. But there was an incident where there was a LinkedIn client who was interviewing—There was a client who was interviewing a North Korean—happened to be a North Korean IT worker. And in this one instance, they happened to find them through LinkedIn. So they did an interview. But they refused to go on camera. And their LinkedIn profile said they're from San Francisco, or the Bay Area.

Coincidentally, the interviewer was also from the Bay Area. And they asked, "Well, what part of the Bay Area?" And they couldn't specifically say what part of the Bay Area. They just kept saying, you know, "The Bay Area." And that kind of tipped off that to the interviewer that something might be off. And it turns out that that person was a North Korean IT worker.

I think the other thing, too, is that, you know, for a lot of these cyber hackers, there is a lot of incentive for these guys. They have a lot on the line, right. They are put out there. And they're trusted by the regime to really bring in money. And if they don't, they have a lot to lose, right. Their family could be sent to concentration camps. This is honestly a lucrative opportunity, where they could even potentially get money on the side.

And so I think, in that sense, they're incentivized to really—to, you know, be creative, to make these attacks, and they're just operating on a whole different level, in that sense, just because they have a lot more to lose. But they also have a lot more to gain. If they are able to consistently bring in funds for the regime, then obviously, the regime is going to take care of them, as well as their family.

ALEX O'NEILL: Thanks David. And I would just add that I think you mentioned a really important aspect, which is the moonlighting element, where you have folks—and even the case

of North Korean hackers and IT workers, you have folks who are sort of on the clock, and who are working toward a quota, but who may also use—you know, bring things home from work, basically Or, if they're stationed abroad, use the same technologies that they have for their own personal enrichment. So I think that's an important angle that often goes underlooked.

Ashley, I want to put the same question to you. Have we seen significant advancement over the last few years, in terms of North Korean threat actors' tactics, techniques, procedures? Has their tooling improved? Have their behaviors changed, their OPSEC if you will? Has that improved? Or does it seem like they have been largely stagnant and just trying to do the same techniques as before?

ASHLEY CHAFIN-LOMONOSOV: Well, I can't speak necessarily to anything that happens before they pop on the blockchain. As soon as they steal funds, they have advanced a little bit, actually. They're showing an increasing comfort in the decentralized finance space, which fortunately for investigators and regulators, is more transparent. But unfortunately, is not as touchable.

Separately, we have seen them get a lot more creative in terms of how they attempt to cash out or convert crypto to fiat. So, as we've seen, like cryptocurrency exchanges and industry players crack down on counterless at finance at that point, we've seen them become a lot more creative in how they cash out, at which point we lose a lot of transparency and visibility, too. Because whereas we could go for—recommend a subpoena to whichever exchange was facilitating that activity unknowingly, we no longer have the visibility, because we don't quite know how they're converting crypto to fiat, and effectively using that money to fund their economy.

ALEX O'NEILL: Gotcha. Saher, I want to go to you. As someone who's looked, and obviously there are proprietary bits that you can't share here, but as someone who's looked, in the course of IR engagements, at some of the malware that North Korean threat actors are using,

have you seen significant advancement in the tools or the TTPs or the behaviors that some of these folks are employing?

SAHER NAUMANN: Yeah. So actually, one of their main implants, called Beefeater, that's been in use for probably about four years now, is an interesting example. I definitely did mention the OPSEC mistakes. And we do still see some of those. But actually, there have been, especially just looking at the evolution of this one tool, we've seen pretty big strides, actually, on the malware side and a lot on the infrastructure side as well. So, you know, for example, the banners have evolved that we see from the malware that are on those servers. And so kind of tracking them has become more and more difficult over time. I think it used to be a lot more—It was more of an obvious signature, for example. But now they've started to complicate things a little bit.

So the tooling, I think largely, the different kind of versions of Beefeater that we've seen, the functionality does tend to stay the same. But kind of these small tweaks that they're making do end up being actually extremely impactful on the operational security. And I think that – And then that, in turn, kind of makes the command and control infrastructure harder to identify.

So it's clear that they have put a lot of investment into this particular tool. And also, not to mention, aside from the fact that it's a Windows tool, and that we saw that most prominently, there are also Mac lists and Linux versions that they've kind of developed as well. So you know, even these kind of show a lot of improvements. Whereas before, you'd be able to find kind of a goldmine of indicators in them, with function names fully intact, kind of a lot—you know, more obvious. And over time, those have also become more improved. I haven't seen as many mistakes.

So I think, you know, and kind of in parallel to Beefeater developing, which has been used in kind of multiple campaigns, there's other implants that they've developed as well. So I think that the kind of investment into tooling is definitely an ongoing effort in that way. At least I don't

think they're relying necessarily, you know, kind of on old tactics. Some things do stay the same, as we talked about with the phishing. But it's definitely clear that they're putting effort into developing these tools as well.

ALEX O'NEILL: Thanks for that. All great points. And Jason, I want to go to you on the same question As someone who's spent a ton of time looking at the sanctions of Asian angle in particular, you were talking earlier about how basically, it's almost like Whack-A-Mole, right. Where if we figure one thing out, they come up with something else, in terms of sanctions of Asian, in terms of using third parties, especially in China. And so I wonder, in the course of your research, have you seen significant advancement in terms of the threat actors' TTPs, or their tools, or their behaviors, in terms of sanctions of Asian, based on the crypto that they've stolen?

JASON BARTLETT: Sure. So I think first, I just want to make a caveat that, while these—all of these hackers are state-sponsored by Pyongyang, not all North Korean hackers are created equal. And that's because the Lazarus Group is honestly just a blanket term that we use to describe any state-sponsored North Korean hacker. There's many subgroups within the North Korean Intelligence Bureau that focus on different industries. So there are some that focus on the financial industry, some that focus on, as you mentioned, aerospace and defense, some that focus on espionage in South Korea. So we say Lazarus Group, but there's many different subgroups. And they do have different capabilities and different targets.

I know the most about finance, so I'm going to talk about the finance angle, out of the others. So for the research that I've been doing at CNAS, I have seen events that also completely agree with what Ashley and Saher have already mentioned. So I actually authored a report called "Following the Crypto Using Blockchain Analysis to Assess North Korea's Strength and Vulnerabilities." And we looked at three specific hacks, one in 2018, one in 2019, one in 2020.

And another caveat, one hack in one year cannot be a representation of their entire hacking campaign for that year. But what I did see from 2018 to 2020 was this kind of rapid progression,

and their understanding of how to exploit different financial technologies. So, as Ashley already mentioned, DEFI, decentralized finance, really started to be embedded in a lot of North Korean targets in 2020. we didn't really see that as much earlier on. And there are also the different uses of various tools and technologies.

So OTC brokers, or over-the-counter brokers, are essentially cryptocurrency traders. They'll live in different countries that help—they can either help cash out crypto, so turn crypto into fiat currency, or currency that we have in our wallets. North Korea doesn't have access to US banks or US financial systems or the US dollar because of sanctions. So they have to rely on other people to help cash out the stolen crypto. So we saw a lot of using the OTC brokers mainly from China. Then, unhosted wallets and other type of new financial technology.

So North Korea is clearly aware of how to exploit these technologies. In 2018-2019, there really were no global regulations. The US government and governments around the world were still really trying to figure out how and if and when we should regulate these technologies while North Korea just continues to exploit them. So we have seen this use of different tools, domestic tools, new financial technologies, other people abroad.

And I think the interesting aspect about China is now China banned cryptocurrency, right. So in 2018, when they were mainly using Chinese over-the-counter brokers to help launder money on behalf of North Korea, that might—we might not see that in the future. That is not to say, that there might not be Chinese nationals in other regions that are kind of contested whether or not they are part of Mainland China or if they're abroad.

Then there's also the Russia question. But Russia also recently is now passing law to ban cryptocurrency in Russia. But what does that then really mean for North Korean actors? Because now we're having the Russian Ambassador to North Korea say that they plan to send North Korean IT workers and laborers to the two occupied regions of Ukraine that Russia has called independent, and Ukraine severed their political relations with North Korea recently because

North Korea recognized those two regions as being independent. And China still has not done that.

So I think there's a lot more research that has to go into Russia-China. That would be a clear sanction of Asians for Russia to import North Korean IT workers or laborers into those regions. But we already know, according to UN reports, they are still North Korean IT workers who could be hackers, like Park Jin Hyok, who was the one who participated in the Sony Pictures and Bangladesh heist, that have operated, and they continue to operate in China and Russia. So there's a huge sanctions piece to this that is continuing to evolve. But I think that's probably one of the main driving factors for North Korea to continue to do this, is that as long as the potential gains from cyber attacks and hacks outweighs the potential risks, Pyongyang will likely to continue to do this.

And I think no matter what about a crypto winter, or how long it lasts, they are still going to gain more potential funds than it actually costs to launch a cyber hack like this. So I think that's something else to take into consideration as well.

ALEX O'NEILL: Jason, I'm glad you brought up the crypto winter. I was just about to circle back to it. Ashley, you made some comments on that previously. And for the folks who are unaware, crypto winter is a term that refers basically to the big—the massive decline, recently, in the value of a lot of cryptocurrencies across the board. Some have failed outright. Others are down 70 percent. And it's not just big cryptocurrencies, it's alt-coins, all kinds of different cryptocurrencies have lost tremendous amounts of value. And Ashley, to what you were saying before, right, if a term of North Korean threat actors have stolen, call it $100 million dollars worth of cryptocurrency, right putting aside the fact that you have to pay at each point, we are converting, we are laundering but then converting into fiats, you're losing significant chunks there. If the underlying assets value decreased by really substantial percentage, then by the time you reach the fiat currency stage and bring that back to support your WMD program or your ballistic missiles, or things like that, there's a huge drop in value.

But, so Ashley, I wanted to ask you just to expand a bit more on what you were saying about the crypto winter earlier. Could you talk about how that's affected North Korea? And if you think, looking forward, if you think the crypto winter is going to affect their interest in acquiring cryptocurrency, or their behavior for handling cryptocurrency after acquiring it?

ASHLEY CHAFIN-LOMONOSOV: Certainly, yes. So I work with an incredibly talented cadre of investigators at Chainalysis. And we're constantly trying to examine DPRK's activity versus the value of crypto. So something to consider, as I kind of stated earlier, the $600 million dollars that they stole in March of this year from the Ronan Bridge, would have been nearly double that last year. And that's only speaking to the value of Bitcoin, too. If the activity took place in November of last year, Ether, the Native token on the Ethereum blockchain was worth three and a half times what it's presently trading at.

So, it's not to say that they're not vulnerable to a crypto winter. I mean, we all are. But as the converted value of crypto fluctuates, it could be viewed as a carefully calculated investment by DPRK, because the value of crypto will go back up. So they may not have it right now, but if traded, could fund their WMD program with that.

Of the nation state actors that we investigate, DPRK is one of the most sophisticated and methodical. And we've observed how their hacking and laundering strategies have evolved over the years, as crypto and tech has also evolved. I think it's important that before I go on, that I recap their advancements. And so I'm specifically speaking to the last four years. We have noticed an increased focus on crypto other than Bitcoin to include theft, an increased use of cryptocurrency mixers for obfuscation purposes. They're basically services on the blockchain that tumble or mix your funds to separate the source from the destination. And we've noticed, as I said earlier, their growing comfort and increased use of DEFI. So they have both the ability to hack DEFI platforms and use them to launder.

So, in terms of the crypto winter, I think they would be the most shocked, really, by an industry-wide effort to ramp up compliance. And they have essentially a more difficult time finding cryptocurrency exchanges to cash out at. That varies in how they do it. You know, there are a bunch of methods that they may use, be it identity theft, or you know, truly hiding in plain sight. But an industry-wide effort among centralized cryptocurrency exchanges to stop all illicit activity goes beyond crypto. But, since that the industry that I can speak best to, I'll go from there.

They would have a difficult time bouncing back if any of their typical laundering methods would stop. So I give nod to OFAC for sanctioning the first cryptocurrency mixer in April of this year. It was called Blender, which DPRK heavily relied on to launder their funds. So does that cover—start to finish the question? I feel like I might have missed a part of that.

ALEX O'NEILL: No, that's super helpful. And you mentioned OFAC. David, I want to turn to you for your perspective on this. First of all, I guess, how do you think the crypto winter is going to affect North Korean behavior, as it pertains to stealing or generating cryptocurrency, and handling it after? Yeah, your perspective on that?

DAVID PARK: Sure, Alex. I agree with Ashley. I don't see them changing behavior. I mean, the crypto winter had already started when the March heist took place. And then, I think was it earlier this month, there was the Harmony heist of $100 million. And the winter was getting colder, so to speak. And yet they still went after cryptocurrency. So I think this is, until they see that the global community is really putting up a strong front, meaning they are taking their appropriate steps to mitigate and protect against DPRK cyber heists, until they see that, and they encounter that, I think they will continue to do that. Because it's an easy way to steal money, especially from countries who may not have the resources to commit to cybersecurity, or individuals, or organizations who just don't have the knowledge or the resources to commit to the necessary measures to protect themselves from North Korean cyber hacks.

And, like Ashley said, we anticipate cryptocurrency to go back up again. Obviously, we don't know when. But we anticipate it's going to happen. So it's a good investment, right. And you continue to steal, hold it. And in the process of continuing to conduct these heists, they also get an opportunity to fine-tune their skills, and develop new tactics. So in a way, for those reasons, I still see them continuing in that specific behavior.

ALEX O'NEILL: It's a really interesting point. Jason, I wonder if you agree with what Ashley and David have said.

JASON BARTLETT: Yes. I don't have anything to add. Yeah, I agree 100 percent with what they're saying.

ALEX O'NEILL: Gotcha. Well, let me push you a little bit, Jason. On sort of stepping back a little bit, what are other shocks that could affect the North Korean regime's interest in cybercrime and cryptocurrency? And how connected is that interest to the broader geopolitical context, especially regarding things like sanctions or the ongoing developments with weapons of mass destruction in North Korea?

JASON BARTLETT: So if I may, could I change the word from interest to success? I don't know if North Korea will ever lose interest in crypto, so maybe more on the success. I think, once again, like we all just agreed, if it's still beneficial for them financially, I think North Korea is capable of targeting anything. I mean they even apparently were targeting medical institutions that were testing for COVID. So, I mean, they have no—there is no boundaries for them.

I think something else to maybe be aware of, and maybe I kind of briefly mentioned it before, is the China-Russia factor. I think it's very, very crucial in saying that North Korea also targets in so-and-so allies, right. There has been reports of them hacking China and Russia as well. I think there is also this idea that, you know, it's like the Cold War. It's North Korea-Russia. You know, they're together. It's not so warm. It's more kind of like a convenient partnership. I actually think

that might be a Chinese term that has been used before. But it's more about this—It's a partnership. Yes, it is an alliance in certain ways, because the end goal of trying to stymie the West and the US influence in the region is definitely uniform. But they're not as close as they once were. That little brother/older brother mentality is not there. North Korea is an incredibly xenophobic country. They have their *Juche* ideology. They do not want outside influence. They just rely on it, because they know they have to.

So I think that's also something crucial, too, is that they still need to rely on foreign nationals and noncompliance, in order to do this activity I think with China, time will tell. It's pretty interesting. China, for several years, has been cracking down on cryptocurrency, starting with mining first, then actually trading Actually, one of the cryptocurrency exchanges that we looked at for the 2018 hack, was in China, and then offshored abroad to, I believe, the Cayman Islands, to continue to do their crypto work, because they couldn't do it in China.

So I think that's something to definitely keep an eye on, is kind of, what will the role of maybe non-state actors in China and Russia be? Because now, if Russia is passing this law that will effectively try to ban cryptocurrency in Russia, well, would that then extend to the two regions in Ukraine that Russia has now declared as independent, that North Korea has diplomatically recognized, and that the Russian Ambassador to North Korea is talking about possibly sending North Korean workers there? And there's a long history of the Soviet Union and North Korea working together to send workers to and from each of the countries, which would be a clear sanction violation.

So that's something interesting to watch, too. Well, then, what would that mean for cyber then? We already know that there are about 6,000, according to US army stationed North Korean hackers overseas. Obviously, it's very hard to exactly pinpoint the exact number. But, then, what would that then mean for those areas of Ukraine? And that's, I think, something that the Ukraine and Russia analysts can focus more on. But I think those are two possible shock areas. And that really, how will Russia and China want to work with the crypto space and the financial

technology and blockchain technology space? And I think that will then impact North Korea's ability, maybe to expand its operations.

I think North Korea will always continue to have illicit operations within Chinese and Russian jurisdictions. But I think the amounts that the governments will be kind of turning a blind eye, I'm kind of curious to see if any of their domestic policies will affect how they treat North Korean activity. And that is still, I think, too early to call.

ALEX O'NEILL: Thanks Jason. Before we get back to that same question on the other shocks, and the geopolitical context that you were referring to, I want to ask Saher a question, based on something that Jason brought up. Jason mentioned the non-state actors in Russia and in China and other countries. Saher, you've done some really great work on the ties between North Korean threat actors and foreign non-state actors. I'm thinking especially some of the work that you did on the GraceWire-TA505 connection. I wonder if you could talk a little bit about what you found in that regard, and tell us how important that is, whether it's quite important, somewhat helpful, or not that important to North Korea's cybercriminal capabilities.

SAHER NAUMANN: Yeah. That was a really interesting, I guess, development. And it was a few years ago, now. And it's worth noting that that overlap that we saw between kind of Lazarus activity at the GraceWire tool and TA505, which is a cybercriminal actor, you know, was, for a short period of time, maybe a matter of months. And after that, at least from our visibility, I am not aware of that same kind of relationship, although I imagine it does exist in certain forms when, kind of as and when it's needed.

But at the time, there was quite a lot of debate, or even internally for us, around what the nature of that relationship was. So the fact that we could see kind of Lazarus tools, along with TA505 tools on the same victim networks, you know, in the same timeframe, the question became whether this is kind of a collaborative relationship. Is it transactional? Is it kind of buying tools

or selling access? What is kind of the relationship there? And to be honest, I don't know if we ever found an answer.

But the fact that kind of that overlap was seen across multiple different victim networks just made it too much to be a coincidence. So I think that it's definitely likely that, you know, Lazarus was using, to whatever extent, probably multiple cybercriminal actors for different purposes in their operations And that is the connection that we happened to see. And we've seen kind of Lazarus do similar things in other capacities. So some examples are things like ransomware.

So in the Taiwan bank heist in 2017, you know, Lazarus used a variant of Hermes, which is a ransomware that they didn't themselves develop, but they could have bought. So it's not—You know, there are multiple actors who kind of take advantage of that market to either buy tools or buy access. And there's quite a lot of actors who, you know, build their entire business models around that kind of trade. And you know, selling access as a service, for example. So there's a lot of criminal actors who kind of operate that way.

So yeah, it's definitely something that we've seen in the past. I wouldn't say it's something necessarily recent. But yeah, I imagine that when that's beneficial, then they would probably turn to it.

ALEX O'NEILL: Gotcha. Thank you for that. And I think you make, on the one hand, an important caveat, right, that this is a relationship that is limited, both in its time scope and in the sort of the number of operations that it seems like that was involved in. but at the same time, it's a really significant finding, right, in the sense that you have North Koreans who are working with external partners, whether the external partners know who they're working with or not is a different question. But just the fact that there's some external involvement, be it the malware, Hermes ransomware you mention, that may have come off a forum, or the connection to TA505, or that other researchers have found, a group that operates malware called Trickbot. It's believed to be based in Russia or nearby. It's a really important point.

I'm going to go back to the previous question, just because I want to ask Ashley and David for their opinions as well, on other shocks that could come to the North Korean regime, and potentially affect their interest in cybercrime or in cryptocurrency. David, we'll go to you first on that question.

DAVID PARK: I think one shock that—and this will likely take time, so you probably won't see this happening—maybe it's not the best way to describe it, using the word shock. But there are obviously efforts ongoing throughout the USG, and with allies and partners, to implement, for instance, the FATF standards, the Financial Action Task Force, which really started off as a sub-organization under the OECD, to develop these guidelines for countries to adopt through domestic legislation, measures to protect against terrorist financing. It started in, I believe it was in the '80s. And then, since then, it's expanded to cover proliferation of financing, anti-money laundering, financial crimes, and a whole litany of other threats to the global financial system.

One of the efforts that my office is engaged in, is to implement FATF standards, when it comes to virtual assets. And then, there is a thing called the Travel Rule that the FATF has put out. And it encourages every member of the FATF, as well as non-members, to take appropriate measures according to those guidelines and recommendations, so that there is some sort of global standard that gets put in place in due time for countries to protect themselves against illicit cyber activity, such as those that we see from North Korea.

So assuming that happens relatively quickly, that's a shock that North Korea could potentially see. But again, that's going to take time. I think some more immediate areas that—or immediate ways that North Korea could potentially see a shock, are efforts that the US government has with allies and partners to make sure that we push, through international organizations, or bilaterally, or multilaterally, whether it's capacity-building with other countries or organizations, to really put the measures in place that would protect themselves and ourselves as well, from North Korean cyber activity.

And I think the other ways is, if the US Security Council is able to put in very strong measures that require member states to take certain measures, particularly related to cyber threats. But that, itself, is going to be a challenge, as you know. And most recently, the draft UNSCR passed, had a vote of 13 to two. And, you know, the two countries that obviously vetoed that UNSCR. So there's going to be a little ways to go in that realm.

But I think those are some of the areas that potentially North Korea could see a shock, you know, short of them just all of a sudden losing some sort of capability on their own—So I'll go ahead and stop there, and turn it over to Ashley.

ALEX O'NEILL: Thanks David. And we'll circle back in just a moment on some of those other points you made. But Ashley, over to you. Any other shocks that you might anticipate things that could affect the North Korean regime's interest in cybercrime or in cryptocurrency?

ASHLEY CHAFIN-LOMONOSOV: Yeah. Thank you. I briefly touched on this earlier. But, as exchanges beef up their compliance, DPRK is having a harder time cashing out. So what they try to do is obfuscate themselves on the blockchain. So I would think that, for what we can do with what we know right now, sanctioning mixers—well, sanctioning Blender was extremely successful. In fact, nearly 10 percent or something of all funds sent from illicit addresses are sent to mixers. So this may extend to illicit activity beyond DPRK.

If mixers, because there are individuals writing these programs, or softwares in some cases, block transactions, or if they cease to operate, DPRK's blockchain activity would be completely transparent. And they would have to resort to entirely to like decentralized protocols to convert currencies to the most desirable types. And then, on the back end, have someone facilitate that either fiat conversion, or item-based conversion for crypto.

But then, if decentralized protocols leverage these other smart contract-like functions on the blockchain called Oracles to screen for sanction addresses, and OFAC is working as hard as they do, taking that one step further and deploying machine learning to catch the incoming transactions from DPRK, they wouldn't be able to launder funds that way any longer. So it'd effectively ruin their MO on the blockchain as it stands now. It would be very difficult.

ALEX O'NEILL: Thanks Ashley. And that's a really interesting point, just the one there that you made, on integrating things like machine learning and AI into the defenses. I think there's been a lot of research, especially recently, on potentially automating attacks, and how can you use AI and machine learning, things like that, to be more efficient, if you were a cybercriminal, right. But on the flip side, for defenders, where it's important to have those capabilities as well, to anticipate, be able to block attempts at intrusion.

I'd like to go back, building on what you said, Ashley, and on what David was saying before, I guess I'd like to pivot a little bit to the defense with cybersecurity angles. And so the question is, what can the US and South Korea do—and I guess the global community as well, to address these kinds of harmful activities? And Saher, I want to start with you. Things that the US and South Korea can do to address these kinds of activities.

SAHER NAUMANN: Sure. So I think there's a couple of ways to look at this. I think we have kind of the intrusion side, and the money laundering side. And I think on the intrusion side, what we've seen is, over the years, with bank heists—you know, SWIFT put in a lot of different kinds of security controls to kind of deter that activity. And, you know, those were pretty successful, although I think the most successful deterrent was actually the pandemic. So that was kind of a lucky break there.

But I think that, as banks here, for example, have kind of mandatory requirements to fulfill things called CVESTs for example, so this requires—involves kind of testing their security and different protocols, and you know, doing the research to see where they're vulnerable, and

shoring up critical assets to kind of apply similar things to the cryptocurrency industry, or the exchanges. Because, you know, the reason—One of the big reasons, as we discussed before, that Lazarus probably isn't going to lose interest in this industry, and cryptocurrency, is because it's still relatively new. And you know, security, again, hasn't been built in from the beginning. And there are a lot of vulnerabilities. And whether that's the exchanges, or the ops, whatever it is. But, you know, those are still pretty high value targets, because they are not as mature as traditional banking. So I think that's a really key point.

And I also think that, you know, Ashley kind of touched on this. But you know, there's a reason that Lazarus doesn't use traditional—or rather kind of the mainstream exchanges, like CoinBase for example, and they're going to these smaller, more privacy-oriented ones that launder money, because they either can't or won't respond. Whereas the bigger exchanges will kind of freeze the funds, cooperate with law enforcement, et cetera. So again, the kind of sanctioning wonder was a great move. And I think ones like Tornado Cash also would be kind of the logical next step there, just given how prominent it is, in terms of being used as a mixer to kind of obfuscate those transactions.

So I think, just like on the intrusion side, it's about, you know, making the process harder. Everything we do, as threat intel analysts and investigators, is you know, to try and trip up the attackers, to make their kind of process more difficult. So if you do the same thing on the money laundering side, you know, whether it's publishing advice on how to secure cryptocurrency, or how it's developed, you know, publish what Lazarus does post-compromise, its exfiltration methods, those kind of things will be really valuable to defenders everywhere Because, you know, if they can't cash out the funds, they are going to get frustrated. That is the key point. So I think, you know, there's things kind of on the policy side and on the technical side that can be done. And it just has to be kind of a mix of those.

ALEX O'NEILL: So Saher, I have a follow-up question that I'd like to ask you in just a second. Before I do that, I want to invite our audience to please submit questions using the Q and

A function. We'll be moving to audience Q and A in about 15 minutes or so. Saher, you made a point, at the very beginning of your remarks just there, on how the pandemic has had a deterrent effect on some of these activities. I just wonder if you can expand on what you mean there. It's a really interesting point.

SAHER NAUMANN: In probably, you know, February, March, April, 2020, you know, kind of just as the pandemic was getting going, and becoming kind of global, we saw quite a noticeable drop in Lazarus bank heists. And, you know, I don't want to push the correlation is not causation. But there was quite a strong correlation, in that we're seeing heists quite regularly. And, you know, given the kind of shutdown of a lot of kind of transports and other things, and the lockdowns that were going on around the world, the problem ended up being not the intrusions side, which obviously can be done remotely, but the cash out side.

So, you know, for a while there, Lazarus was quite interested in making quite successful attempts at using ATMs for their cash outs. And this was obviously across a number of countries, and using different kinds of money mules, probably different groups that they were hiring or cooperating with. But that was all physical. And that's quite difficult to do. If you cash out the money, what are you going to do with it after? How are you going to get it to places where it needs to be used, whether that's Malaysia, China, or all the way back to North Korea?

So yeah, what we saw there was quite a break, because of those physical restrictions, and the barriers to travel, and things like that, we kind of saw that dropoff in heists, which never really picked back up again. And I think, you know, the pandemic only accelerated the interest and exploitation of cryptocurrency because that's something that we saw Lazarus interested in, you know, as far back as 2017, and maybe even before. So they were quite forward-thinking in that regard. But I think the pandemic just accelerated kind of using that as a primary target, just because of the issue of cashing out.

ALEX O'NEILL: Appreciate it. Super interesting point, that I think goes under-discussed in a lot of the conversations on cyber. Again, you made the great comment before, Saher, in the very beginning, that we're dealing with folks who are sitting behind computers, that they're real people, right. And so we have to think about the effects on human beings. It's not just something that happens. Like you said, it's not magic that these things take place.

David, I want to go to you on the defense and cybersecurity angle. You mentioned a bit earlier in the conversation some of the threat advisories, the cyber advisories that treasuries put out. I know you guys have been quite active recently with some new ransomware called Maui that's been discovered, and a couple other North Korean cyber threat advisories. I wonder if you could speak a little bit to the value of those kinds of things, or if the advisory is—And even more broadly, of indictments, other things that aren't quite divisible steps, like sanctions, or asset seizures. But in terms of that information sharing, can you speak to the value of those measures?

DAVID PARK: Yeah, absolutely. I think, from our perspective, those advisories are opportunities for us to engage with the private sector, both individuals and organizations. It's an opportunity to share information that we have been able to discover and assessments. And methods that we think that the private sector could use to protect themselves. And in so doing, also help our efforts to counter North Korean illicit cyber activities, or in general, illicit financial activities.

So I think those are very helpful. It's also a tool that we can use when we do direct engagement with certain sectors of the industry to highlight some of these nefarious activities. I think you mentioned earlier the ransomware—or maybe it was Jason, I think it was ransomware. Yeah, around ransomware against the healthcare sector. And just showing that there's a variety of ways that North Korea could use illicit cyber activities to conduct [inaudible]. And it doesn't necessarily always have to be them going into a bank to steal money or steal cryptocurrency. It could just be, you know, something as simple as phishing attacks, ransomware. And these are also opportunities for them to fine-tune their skills, right.

So these advisories are useful opportunities for us to share with the public and the private industry that these are the things that you need to be aware of. But it's also an opportunity for us to share that, look. This is what's happening. If you decide to, most likely unknowingly, you know, pay the ransom amount, you could be subject to US sanctions violation. So letting them know, as well, what our regulations are, what our laws are, particularly when it comes to sanctions, and potentially even—and this would be more in the FBI lane, but in terms of asset seizures, just letting them know what they could potentially put themselves into by engaging with the North Koreans, and falling victim to some of their demands. Hopefully that will give them enough reason to be more alert, and to practice more greater due diligence, so that they don't fall victim and inadvertently advance, not only North Korea's capabilities, but their ability to acquire funds to advance their nuclear weapons program.

ALEX O'NEILL: Yeah, David, those are really excellent points. And I think it's something that we as folks who research North Korea, and look at various different angles of the sanctions of Asian, and the particular operations, all kinds of different elements of this North Korea issue, it's something we maybe take for granted, right. But the folks who are becoming victims, whether they're operating crypto exchanges, or banks, or private companies, things like that, right, they're probably not thinking on a daily basis what the threat posed by North Korea. So getting that information out, and sharing, especially in foreign countries, the capacity-building element, I think is really important.

Ashley, I want to go to you next. In terms of what the US in particular can do to address these kinds of harmful activities, I wonder if you have anything to add on that.

ASHLEY CHAFIN-LOMONOSOV: I don't have much to add. But I'd like to reiterate two things. Education is key. Everyone should be investing in very, very robust IT and infrastructure security training. You know, preventing—creating training programs to bring awareness, as Saher said, and publishing all sorts of activity and things to be on the lookout for. I briefly

touched on it earlier, and it's been stated very, very eloquently by the rest of the panel. Implementing THAAD's recommendations for both traditional financial institutions, you know, as much as possible, training appropriate onboarding for new customers, taking risk-based approach, and ongoing monitoring of regular and account activity that aligns with the behavior that it should have. But also, you know, encouraging centralized exchanges for cryptocurrency to better audit new accounts and account activity, and stop facilitating illicit activity.

Separately, something that I briefly mentioned earlier is, if you know someone, or if you have contacts that are developing decentralized finance protocols, or just other protocols on the blockchain, adopt code audits. Employ like decentralized oracles, like I had mentioned earlier. And, most importantly, ensure that your security, the security of your code cannot be breached or broken. That's exactly how Ronan happened. It all comes down to education, though. And that is key to preventing cyber attacks in the future.

ALEX O'NEILL: It's super helpful. And even though it seems like, in 2022, the topics of cryptocurrency and hacking and things like that are very much center stage, still definitely important to get the word out.

Jason, I want to go back to you, in particular, on the collaboration angle, what the US and South Korea can do jointly to counter these kinds of harmful activities. I know you've done a lot of research, especially in this space. What do you have to add on that?

JASON BARTLETT: Sure. I think that is a fantastic question, because United States's cybersecurity strategy against North Korea will only really be effective if we're doing it in partnership with South Korea, similar to any US policy on North Korea, and as well as South Korea as well. When Seoul and Washington are in agreement, our policies are much more ironclad. They're much more easily enforced. And they're more long-lasting.

And kind of going into that, I think there are three current obstacles that are very important for both Seoul and Washington to be aware of, when it comes to enhancing cooperation. And I'm specifically mentioning cooperation with South Korea for several reasons, the first being that earlier this year, President Biden and President Yoon, the new President of South Korea, met to discuss the US-ROK alliance, and specifically mentioned cyber. And this was kind of an add-on to a 2021 meeting between President Yoon—or President Moon, excuse me, the former President of South Korea, and Biden. They talked about making a joint separate working group that never materialized, as far as I'm aware. And then, in 2022, when President Biden met with President Yoon, they talked about bringing this back. And, for the first time, they mentioned cryptocurrency, North Korean cybercrime, and blockchain technology. And that was not mentioned in the first cyber working group.

So it is clearly a stronger interest now in Seoul, to work together with Washington on these issues. Which is very important, because some of the obstacles that Seoul and Washington will have to navigate are very long-stemmed issues that US and South Korea have struggled with before. The first is, unlike in the US, where our stance on North Korea really doesn't change that much, whether we have a Democratic or a Republican President, a Democrat or Republican President. Whereas, in South Korea, it does fluctuate pretty significantly, depending on which party is in power. And South Korean Presidents are only in power for five years, once. US it can be four to eight.

So there's also a difference in terms of that, kind of logistically, how politics are run. There's a very different domestic atmosphere when it comes to North Korean politics and South Korea that will affect how much Seoul is able to engage, and what might seem as hawkish policies. The second is that, the US and Seoul also categorize the threats very differently. North Korea will remain and permanently is, and has always been, since there's been two Koreas, the greatest security threat to South Korea. And it is, third, that's the number one security threat. It's also the number one intelligence collection that the South Korean Intelligence Agency does, is on North Korea.

China and Russia also pose very serious cyber threats to South Korea. But, once again, about 90 percent, according to South Korea's Intelligence Agency, of cyber attacks targeting South Korea, are conducted by North Korean actors. So obviously, South Korea is going to collect a lot of intelligence on North Korea. The US does that as well. But we also have to worry about China, Russia, Iran, many other countries that might pose higher cyber risks.

I personally do not believe that North Korea is on the top list of cyber issues for the US government. And, when it comes to security, I think there's more focus on China and Russia, because they tend to focus more on espionage, which has a little bit more of an immediate risk, as opposed to financial crime, which I would argue is equally as dangerous. But I don't think that really translates when it come to US policy. So there's also a difference in terms of really categorizing these threats. And Seoul views North Korea as a much greater threat, in terms of their intelligence collection than the US currently does.

And then the third is also how they deal with it. So, as I mentioned before, the US, we have the Treasury, which does fantastic work, State does fantastic work, FBI, DHS, CIA, FBI, Homeland Security, says that they all can deal with North Korea. And South Korea, it's mainly done by one organization, NIS, [KOREAN], so their intelligence agency. And there's many other agencies in Korea that can lend their expertise in financial crime and cyber to it. But nine times out of ten, whenever it's a North Korea-related security threat, it's then taken over—the response is done by the Intelligence Agency, which has a Cyber Bureau. And they definitely have different capabilities. But that makes information sharing difficult.

And this was conversations that I had when I was actually in Korea about a month or two ago, for a current report that I'm doing on this specific issue, of how to strengthen US-ROK collaboration against cyber-enabled financial crime. And it was one of the conversations that I had with the very wonderful people that I was able to meet from Korea, that talked about kind of information sharing versus information taking.

And I think there is still a lack of understanding between Seoul and Washington, and how the countries deal with this issue. And the US can 100 percent benefit from having more information on the different TTPs we talked about, where the North Korean actors might be stationed, what their education is like, where are they going, where are they traveling. South Korea will almost always have more information and intelligence than the US will. So we have sanctions. We have more course of tools. We have a stronger hold on a cryptocurrency infrastructure because of the US dollar. South Korea has the knowledge. We have the tools.

And then something else, when it comes to standards, South Korean government doesn't necessarily function the same way in the US, in terms of the US will typically talk first with the private sector, before creating laws that impact the financial structure of our country. South Korea tends to create laws and then just expect the companies to abide by them. We saw that with VASP, so virtual asset service providers in cryptocurrency exchanges. All of a sudden, this law passed that then required them to register with banks, which was great for transparency issues, and know your customer protocol. But they weren't really given that much time to do so. That wouldn't necessarily be very popular in the US to do that type of approach.

So there's also different ways, too, that I think Seoul and Washington need to communicate more about how they deal with these issues. And I think more public research, as the other panelists mentioned, is crucial. Because we are two similar but different countries. And we have different strengths that I think haven't been fully used the way that they could be. And North Korea has been exploiting that.

ALEX O'NEILL: Thanks, Jason. That was super comprehensive. David, I want to turn back to you. You made some kind of similar remarks earlier, speaking about international cooperation. And I wonder, not just in terms of US-ROK cooperation, but more broadly, US cooperation with other foreign partners. I wonder what concrete steps the US either should take, or is hoping to

take, and sort of working toward implementing, in terms of cooperation with foreign partners on dealing with these kinds of North Korean cyber activities.

DAVID PARK: You know, in addition, obviously, to the ROK, the other country that most comes to mind is obviously Japan. To them, the North Korea threat is real. And it's maybe not as big as—perception-wise, maybe it's not as big as what it is for South Korea. But, nonetheless, it is still a major threat for the Japanese. And, you know, they too, I'm sure, have experienced some form or a variety of North Korean cyber attacks.

So I think enlisting the Japanese, they are a developed country. They're a member of the G-7. So they certainly have the means—And right now, they have the political will. And their Prime Minister Kishida can really take a larger step on the international arena. So I think Japan would be another one of them.

Obviously, reaching out to the Southeast Asian countries, particularly Vietnam and Singapore were involved, you know, unfortunately, of course, in the March heist, the cryptocurrency heist. And so I think those are some of the countries that come to mind. And in general, I think where we can really, really make an impact would be working with the developing world, right. They just don't have the same level of resources that the developed world has. And you know, working with countries like South Korea, like Japan, who have the know-how and the resources to work with the United States, and other members of the international community, to help build cyber resiliency, especially in the financial sector, so that their banks won't be subject to the type of attacks or be victimized, like we saw in the Bangladesh bank heist.

So, I think those are some of the areas where we can work with allies and partners. And even, you know, countries that may not be allies and partners, but you know, do have a genuine concern, in terms of protecting their financial system, I think those are some of the areas that the US government should really focus its energies on.

ALEX O'NEILL: So I have a follow-up question. And I think we have the perfect group to address this. My question is, what role can public-private partnerships play in addressing these kinds of issues? And I want to go to Ashley first, as someone who has experience, both in government, and now in the private sector, how do you see the role of public-private partnerships playing out?

ASHLEY CHAFIN-LOMONOSOV: Communication is the first thing that came to mind, Alex, honestly. When you have an existing partnership with a company, it's a lot easier to talk to them when something maybe goes wrong. So in some instances, you know, having great connections with the cybersecurity industry, or incident response companies, may help us connect one of our potential customers to them faster. And when we have that partnership established already, they can get answers faster. We can get to investigating faster. And, ultimately, you know, work to stop any activity possible. So public-private partnerships go a long way, especially when you're in close contact in establishing that sort of relationship early.

One other thing that I would say is, that the more transparency that we can provide, without having to formalize our communications, and you know, really, really be careful with what we say, is when we have these working level relationships with some partners, again, we develop that closer bond. And it's a lot easier to communicate in times of stress, and when we need to move quickly.

ALEX O'NEILL: That's really interesting. Jason, over to you. Same question on the value of public-private partnerships in this space.

JASON BARTLETT: Sure. I don't have really much to add beyond what Ashley just articulated. I think communication is key. I think I will continue to harp on the Korea angle. I also agree, 100 percent, with David about the importance of bringing Japan into the fold. There are obviously geopolitical issues with any type of trilateral agreement, especially right now. But I think that it is key for the future. But I think focusing right now on the cyber working group

already promised to be established between Seoul and Washington, I think having public and private sector researchers involved in that process would be incredibly helpful. Because I think that public space like the think tank, and then private firms like TRM Labs or Chainalysis or Elliptic, that can offer really intensive and investigative-driven analysis on malware use—and that extends beyond just North Korea. This extends to China, Russia, Iran, many other countries that also use kind of similar tools, but in a different way.

And I think having some type of advisory board, where they're able to communicate with US government officials or South Korean government officials or any government official that really wants help, I think would be really beneficial. Because usually, we have regional programs that are focusing on one thing. That's not always the case when it comes to like the cyber working groups. And it's not their day job, right. They're volunteering to participate in these kind of bilateral talks. It's not their number one job unless you're an ambassador. So I think that more engagement with NGOs and the private sector is key, because we can offer our expertise. And we can also attribute hacks to countries with having less diplomatic blow to it.

If you're going to attribute a hack to a Russia state-sponsored actor, or a Chinese state-sponsored actor, that has a lot of diplomatic weight. North Korea doesn't really matter, because we don't have diplomatic ties with North Korea. But it is a big message to say Beijing hacked this company. I think that probably went into why it took so long to really fully publicly attribute the Microsoft hack that China did to China. Because there's a lot of diplomatic backlash that can come from that. But if it's a public or private sector doing that, you're still getting the message across, without kind of making that diplomatic bargaining chip kind of useless.

So I think that is also important, too, is that really finding out what's the best suits that the government can have for us? And how can we help inform our governments to make a safer crypto and cyber space?

ALEX O'NEILL: Yeah, I think those were all really important points. And Jason, I would just commend you, in particular, for the work that you and your team have done at CNAS, to bring together a lot of those folks. Of course in the public-private realm, I think think tanks sometimes get left out. But there's a sort of central node there. I think you and your team have done an awesome job of bringing folks in the private sector and in government together, to sort of build those relationships, and conduct some research in that area.

David, I wanted to go to you as well, more, and obviously in your personal capacity But from the government perspective, generally speaking, what value does the government see in those public-private partnerships?

DAVID PARK: Yeah. Personally, I think that we have under-utilized those partnerships. I think they are a tremendous tool for the government, one, from a messaging perspective. You know, the work that Jason does, the work that Ashley does, I mean imagine if we are like attached to the hip. And we're able to combine our efforts, really get the information out there, in a timely, consistent, and expedient manner. The amount of knowledge and potentially resources that industry and individuals can have as a result of that effort, can really, really make quick and big headway, in terms of countering illicit cyber activity, particularly from the North Koreans.

But, at the same time, it's also an opportunity for us to—you know, having that partnership, it's also good for the government, because we can learn from the experts. People like Ashley and Jason, they get to—they find it frustrating when, I would imagine, to a certain extent, they do working on DPRK issues. But you know, they put so much effort and are able to produce so much good work. And, you know, in government, we just don't have the same amount of time or the resources to be able to commit to such research.

And so being able to learn from them, and have these discussions—And I like what Jason proposed in having private groups be part of working groups, and to be able to leverage their expertise and knowledge, it's basically a two-way street. And I think that we, as a government,

can do, and should do a better job of reaching out and working more closely with those in the private sector.

ALEX O'NEILL: So just a quick follow-up. You mentioned that basically, there's room for growth. And I wonder, in concrete terms, is there anything that you're hoping will take place over the next year or so, or in the longer term, in terms of, as you said, getting more joined at the hip, being able to act more quickly, and work in tandem in a more efficient way?

DAVID PARK: Yeah. I think in the immediate future, what we can do is get, you know, experts like Jason and Ashley and others involved in some of the working groups, right. Yes, it's important for governments to be talking to each other, and making sure allies and partners are aligned in their efforts and policies. But at the same time, it's also important that we get buy-in from, you know, the private sector, and experts at think tanks, and in academia.

And so I think inviting them to these dialogues, and maybe what we can do is have a public-private sector dialogue, right, where one day we have a dialogue with just the government folks. And another day we open it up where government officials can come and present their thoughts and make suggestions. And we can learn from them, and they can learn from us. And so I think those are some of the areas where, in the immediate future, that we can really benefit from.

ALEX O'NEILL: And Ashley, just because you have the different perspective, as someone in the private sector now, I want to put the same question to you. We're talking about room for growth in the public-private partnership. I wonder if, from your private sector perspective, at this point being the private sector, what do you see as sort of immediate steps for growth that you'd like to see taken?

ASHLEY CHAFIN-LOMONOSOV: Certainly communicating forward. And while it's impossible, especially in the nature of blockchain to predict what you need to combat in a year's time, having a general sense, and communicating openly and freely about what you expect to

come, you know, with due respect, and to sensitivities, and you know, methods, and the inner workings of the government, the better we can position ourselves to pivot when the time comes, the better we all will be in the future.

ALEX O'NEILL: Gotcha. It's a good point And I'm hoping that there's going to be some productive response after this. In particular, I'm sure we'll follow up on a couple of different ends. But I'm hoping this conversation can lead to our taking some of those steps.

I want to move—There's a question from the audience, which has to do with cryptocurrency exchanges and OTC brokers. And the question is, is crypto vulnerability to North Korean hacks structural? I.E., it is sort of built into the fabric of what cryptocurrency is, and of innovation in that space? And I guess part of the question has to do with, there's an ethos, broadly speaking, in the tech sector. But I think especially in cryptocurrency, it's sort of moving fast and breaking things, as the saying goes. And I think folks are often more concerned about either profitability, or growth, building a user base, and less concerned about pesky things like cybersecurity, of having multifactor authentication on people's phones, things like that. And so I'll put this to all of you. Whoever wants to go first can jump in. But do you see this as a problem basically that can be resolved? Or is this something that's baked-in and structural that we're going to have to learn to deal with?

Jason, why don't we start with you first.

JASON BARTLETT: Sure. I think it's an interesting question about the structural aspect. I think that North Korea's kind of driving reason to continue to do this is essentially defined new ways to procure currency, right, because that's what's lacking. And we're able to ascertain that, because the majority of globally-facing cyber attacks—and when I say globally, I mean off of the Korean Peninsula, tend to focus on the financial industry, right, financial institutions, traditional and non-traditional. So banks and cryptocurrency exchanges, which means financing. Need money.

This change really started to happen around 2015 to 2017, when the US and UN sanctions really started to gain a lot more teeth. And there were expansions of different sanction programs, specifically also targeting cyber, after Sony. So I think that North Korea will continue to try to exploit whatever type of vulnerabilities there might be in the infrastructure. I think that—I mean as Ashley very nicely elaborated on before, is that it is-- cryptocurrency is transparent if it's on the blockchain. It doesn't mean you can completely see everything. It's still numbers. But you still have to do the investigation and the tracking. But because it has that transparency factor to it, then they can use other technologies to hide that.

So I think that where the vulnerability really lies, and maybe that's something that I can speak more on, is that it's still not as regulated as other forms of finance are. North Korea is still targeting other forms of finance, as Ashley also pointed out. So it is traditional sanction of Asians, and things of that nature. But I think that, because of the lack of kind of this enforced global understanding, and also enforced policies on crypto, they're able to exploit that. I do think it's changing now, compared to 2016. But I think that there are very licit uses of crypto. But North Korea will always focus on the ways to exploit different technologies.

So I think whether it's crypto, whether it's something else, they are just constantly looking to exploit. So I don't think that crypto is this inherently bad thing. I have a very different opinion about mixers. But I think cryptocurrency, in general, I think it's neutral. It's just how it's used. And then, it's up to the facilitators of cryptocurrency, whether you're trading it, whether you're mixing it, whether you're buying or selling it, you need to be aware, just like any other type of industry, you have to be aware of what you're doing. Because you're responsible for it. So I don't think crypto should be kind of neglected from that responsibility. It's a form of finance. So it should be treated like any other form of finance, in my opinion.

ALEX O'NEILL: That's a really interesting perspective. Ashley, your take on that same question, whether vulnerability to hacks—I suppose be they North Korean or otherwise—But if

you think that vulnerability is built into the nature of crypto, and the sort of highly innovative tech sector and DEFI sector, or if you think that there's nothing that we can do about it to sort of mitigate this issue?

ASHLEY CHAFIN-LOMONOSOV: Alex, you know that the nature of crypto is move fast and break things. And when there's still such a slow adoption to cryptocurrency, especially, you have early adopters wanting to make a profit on it. And truly, the move fast comes right before the break things does. What we've seen a lot with North Korean activities, specifically in the last couple of years, especially as decentralized finances become more accepted and more popular and more accessible, is that they're breaching protocols that weren't secure in the first place.

So you have perhaps individuals who wanted to get in on the early action and make a profit, but maybe weren't as educated or as well resourced to create safe and secure protocols. And that extends to cryptocurrency exchanges, too. There's a lot more vetting and a larger number of people involved. But you move fast, you break things. And sometimes if you don't break them hard enough, or you know, on the defensive side, protect them well enough, you become vulnerable.

ALEX O'NEILL: I think it's a really good point. And I just mentioned that there's a ton of focus in the threat intel world and in the research world, on the idea of what some people call big game hunting, right, going after these massive companies, especially with ransomware and things like that. But, on the flip side, the North Koreans have shown a proclivity toward going after low-hanging fruit, right, the easiest option. And so, if you have—and I sort of always use this analogy. But if you have ten big crypto exchanges, right, and nine of them have top-notch cybersecurity, they have the best vendors, they have incident response, they're ready to go, there's defending forward and communicating forward, like you said, Ashley, before. And you have a tenth that doesn't employ those same top-notch high level protocols, then hackers are going to go after the tenth one. And they're still going to be able to take in a bunch of money for their nuclear program, WMDs, what have you. So I think it's a really important point.

I want to put that same question on whether the vulnerability to hacking is structural, is baked in, to you, David, as well. And then we'll move on. We have more audience questions to get to.

DAVID PARK: I don't know if it's baked in on purpose. But I think the very nature of the ecosystem being relatively young, compared to the more traditional financial system, where there have been years and years of scrutiny and measures taken to protect it, and building those measures that make it a lot more difficult for illicit activity to occur. So, you know, compared to that system, this is a relatively young system, right. And like Ashley and Jason have mentioned, there's still a lot that needs to be done, in terms of implementing standards, putting in the proper measures, both from a security perspective, but also just in terms of also measures to protect the ecosystem, from a regulatory perspective.

And so, you know, until all of that kind of comes together, and we get a system that matures, this is a wonderful opportunity for North Korea to continue to engage in this type of behavior, until the system matures, and gets to a point where it is relatively similar, if not close to what the traditional banking system is like. And so I think we're going to continue to see that.

ALEX O'NEILL: It's a good point. I guess, to go back to I think what either Jason or Ashley was saying before, just the nature of cryptocurrency, and not just the actual technology behind it, but also, I think, what a lot of the folks who have bought into it believe, is that fundamentally, it's not meant to be, you know, the same as the US banking system and traditional banking system, right. There's meant to be at least some level of independence or decentralization or even anonymity, although that's tough because of blockchain. But so, there's a sort of tension there, right, between the regulation that you're talking about, which really would be effective in a lot of ways, versus I think, in some ways, what it's created to do.

Just moving along to further audience questions, we have another that asks, what are effective mitigation practices that the US public should employ to address the threat posed by North Korean cybercriminal activities? Ashley, we'll go to you first on that one.

ASHLEY CHAFIN-LOMONOSOV: Please stop clicking on suspicious looking emails. You know, truthfully, from a public perspective, from an end user or, you know, or employee perspective, that is educating yourself about DPRK's phishing tactics specifically, whether you're in the crypto industry or not, is definitely important. As far as the larger public goes, pay attention to what your regulators are focusing on, right. Like there was a reason that Blender was sanctioned. And though I don't necessarily share Jason's same sentiment that all mixers are bad, a lot of illicit activity rolls through mixing services. So the more you educate yourself, the easier it will be to combat DPRK's activity. That goes for the general public.

ALEX O'NEILL: Gotcha. And David, same question back to you.

DAVID PARK: Yeah, no. I'd go with what Ashley said. Don't click on suspicious stuff. Make sure your systems are up to date, right. Make sure you have the latest software, that you implement multifactoral authentication, updates. Make sure that you do those in a timely manner. And you know, look at the advisories that we send out. Yes, some of them are very technical. And yes, some of them are very long. I realize those are areas that, especially on the length part, we could do a better job of proving.

But, you know, go through that stuff. Because in the advisories that we've published—and when I say we, the US government, we lay out mitigation efforts. And they're not difficult ones, right. They're relatively simple steps that you can take, that the general public can take, to protect themselves. If you do this, you'll be at such an advantage. That's not to say that North Koreans aren't going to still try and attack you, you know, through the cyber realm. But it will be a lot more difficult for them to gain success.

So do pay attention to those advisories in the mitigation plans. And the reports that, you know, come out from organizations like CNAS, and from Ashley, right. They put out, you know, amazing stuff. And sometimes they do it a lot faster than the US government does. So then, you know, take heed to what's in those reports and analyses. And I think that, if the general public does that, they'll definitely be in a much better place.

ALEX O'NEILL: Definitely. Jason, same question over to you on what the general public can do in this regard.

JASON BARTLETT: I mean, for lack of better words, I mean, just the same thing that I was just reiterated about. Just think twice before clicking. If something it says, "Urgent. Download now. You must do this now," probably not legitimate. That's kind of a scam to try to make you feel fearful to download something. That goes for not just North Korea, but just general email phishing scams. Look for typos. Look for rude phrasings. North Koreans are getting better. They might actually look like they're coming from a reputable organization or a person. So just do your research. If they really need something from you, they'll probably then email you again. So if you're kind of unsure, you can always check with a colleague.

I know at our organization, CNAS, we kind of do these bimonthly cybersecurity checks, where our Director of Operations sends fake email phishing messages to us. And if you click on the link, then you have to retake your cybersecurity training online. And it's very private. No one knows if you fail it. But that's kind of one way that you can kind of do that personal education. But if you're an individual, and you're not employed at a company, if you're self-employed, self-education is really key. Always think twice. Read the advisories and public guidances at the Treasury and the State Department and FBI publish. I know they take a lot of work. And they're really informative. So just—It's all about self-education and just understand that anyone can be a target of any form of cyber crime. And for North Korea, there's no target too big or small. It's just about money. So just got to be smart.

ALEX O'NEILL: Those are all good points from the three of you. And I just say too, it's great credit to the work that Chris Krebs and Jen Easterly have done at CISA. A lot of the work that not only on building some of those public-private partnerships we were talking about before, but also the communication, in terms of what the more recent threats look like. You know, instead of taking six months or a year to get out and say, "Oh, this has happened, or that has happened," we're seeing, in just a matter of weeks, "Oh, there's a new threat. Be prepared for it. Here are the indicators of compromise," or things like that.

We have a couple more questions. But we're running out of time. We have about seven minutes left in the panel. We have a question from Doyong, who is a rising second-year student at the Fletcher School at Tufts. Doyong focuses on geopolitics in the Korean Peninsula. And the question is essentially, what is North Korea's Achilles heel, if there is one, in the domain of cyber crime? Or in other words, what are the areas the regime worries most about? And then, conversely, what is our Achilles's heel? What and where should we work to fill up the cyber vulnerabilities? We'll go to David first.

DAVID PARK: I think our Achilles' heel is that the US government is large. It's a large bureaucracy. And it takes time to move things through the system. And by the time that happens, you know, North Korea could have already moved a significant portion of the money that they've stolen, whether that's fiat currency, or digital currency. So I think that's one of the challenges. And we also have limited resources. You know, we operate off of the taxpayers' money. And as much as we would love to ask the American taxpayer to fork over more of their hard-earned money so that we can commit more resources to ensuring higher levels of cybersecurity, you know, there's obviously a political dimension to that. And we've got to work with what we have.

And so those are some of the limitations I think on our end. In terms of their Achilles's heel, you know, it's—I think that it's—you know, they're not learning their tactics. And Ashley mentioned this earlier, right. A lot of the methods that they use have been similar, right. And it's getting well

know their methods. And so I think, if they continue to use those same methods over and over again, that's certainly going to be an Achilles's heel for them over time.

ALEX O'NEILL: Ashley, same question over to you.

ASHLEY CHAFIN-LOMONOSOV: That's a very difficult one to speculate on. But, to David's point, the more we study, and the more we research, especially speaking from a blockchain perspective, and publish their activity, we make our jobs harder, in that they may not repeat it in the same way. But it forces them to change up their tactics. And though the nature of blockchain technology is ever-evolving and getting better and more creative, and there may be more solutions out there for them someday, if we work fast enough, and you know, partner with everyone who we need to, to make this as public as possible, though they're pretty locked down, they pay attention to this stuff. And they may change their tactics, or run out of solutions. They may not have an option anymore.

And I don't necessarily see criminals, period, or North Korea specifically, pivoting away from cryptocurrency any time soon. But this is the best that they have for right now. So the quicker that we can work ahead, the more likely we are to maybe prevent this someday.

ALEX O'NEILL: And Jason, same question to you.

JASON BARTLETT: Sure. I think for me, just adding on what both of them just honestly perfectly answered, was more about the bandwidth issue. And that's something that they both just mentioned. The United States, even if we just boil down national security to cybersecurity, we then have to boil down cybersecurity to cyber-enabled financial crime. As many people work on cybersecurity, they don't do anything with cryptocurrency or blockchain. It's about, you know, Russian or Chinese state-sponsored hackers, hacking into government facilities, to try to get employment information, and try to ID officers that are abroad.

And so cybersecurity is a huge field. And we have many resources that are divested in, or invested in all of these different regions. But if, for North Korean hackers that are targeting institutions out of the peninsula, if their number one goal is to steal money, and the US's goal, and England's goal, and other countries' goal is to deal with all these other cyber issues and other national security issues, we're never going to win that fight. If it's a one-on-one, we're never going to win it. Because if it's one goal against a laundry list of 100 other cybersecurity issues, North Korea will win that fight.

So I think that's where the compliance and enforcement comes along. That's where multilateral partnerships come along, is that. But, if we work together, then no matter how much North Korea—Because what we've seen, no matter how much North Korea innovates domestically, it still needs help from abroad. It still needs outside technology, outside nationals to help them launder funds.

So, if we're able to really clamp down on that activity, then that's really where we will be able to be successful. Because it's asymmetrically, it won't work, unless we have support and we're able to work together with partners. Or, if these partners honestly just strengthen their own national protocols, in my opinion.

ALEX O'NEILL: Thanks. No, it's a really important point. And that term "asymmetrical, right, people use it both in terms of sort of North Korea's focus, right. They're not using conventional capabilities, or at least not focusing as much in that area. Cyber, nuclear weapons, things like that, right, is fundamentally sort of asymmetrical But there's also an asymmetry in terms of the US or South Korea versus North Korea, right. Jason, you kind of mentioned this. But there's a clear asymmetry in terms of connectivity, right. That the US, all of our critical energy, critical infrastructure, broadly speaking, is plugged into the internet, runs on electronics in some capacity. For North Korea, in a lot of cases, it's just not the case So their vulnerability, right, is not the same as ours. They have a lot less to lose, I suppose. And even though, and the US has done in the past, of taking North Korea offline, basically, for certain periods of time.

There just isn't the same level of sort of day-to-day interference, just because of that connectivity gap.

So I'm looking at the clock. It looks like we've basically run out of time. But before we end, I want to say a huge thank you to our four panelists, to Ashley, Saher, Jason, and David. Thank you guys so much. This was a really interesting discussion. I want to say a big thank you, as well, to the Korea Foundation, for their generous support of this week's conference, and to John Park, for his great work putting this together. And then finally, many thanks to all of you in the audience for tuning in today. We hope you enjoyed the panel. And we look forward to having you back for more soon. So with that, John, I'll hand it back over to you. Thank you all again. Appreciate it.

DR. JOHN PARK: Thank you. That was a terrific panel discussion. Really appreciate all of the insights that you shared. And a group that we look forward to continue to engage, as we grow the North Korea Cyber Working Group activities under the co-leadership of Alex.

For our closing remarks, I'm very glad to introduce Consul General Kijun You, a great partner and friend of the Korea Project. Consul General You leads the Korean Consulate General here in Boston. Previously, he served as Director General for International Legal Affairs at the Ministry of Foreign Affairs. He received his B.A. In French language and literature at Korea University, Master of Law from Korea University, LLM from the University of Edinburgh, and LLM from the London School of Economics and Political Science. Great to have you here Consul General You. Over to you. Thank you.

CONSUL GENERAL KIJUN YOU: Distinguished participants, ladies and gentlemen, I am so glad to have this chance to offer a few reflections at the close of the Third Annual Harvard Korean Security Summit. It has been an honor and a privilege for me to be a part of this summit. It has brought us together to reflect on the theme of global interest, Korea: A Catalyst of Global Trends. Our deep thanks go to the Korea Foundation and the Belfer Center for Science and

International Affairs, Harvard Kennedy School, in particular, Dr. John Park and his team. It is thanks to his unswerving devotion that this meaningful event proved possible.

I have been particularly looking forward to this occasion. In May, President Biden visited the Republic of Korea. His carefully arranged vision was very, very successful. The summit meeting between President Biden and President Yoon took place only 11 days after President Yoon had assumed office on May 10th, making their meeting the earliest summit ever to be held between leaders of the two countries. And without that, we'll have de facto further deepening the alliance between our two countries.

Some seven decades ago, the ROK-US alliance was forged in blood. It has long served as the very linchpin for peace and prosperity on the Korean Peninsula. And indeed, in the Indo-Pacific region, it has evolved into a global comprehensive strategic alliance, which spans many dimensions. And more than that, was cemented by bonds of true friendship. It is my sincere belief that the alliance today stands stronger than ever. And the unwavering support of our peoples is the great foundation of its flourishing.

I believe that our summit was perfectly timed and roped together during this summit. All topics touched upon have been truly thought-provoking. And the dynamic discussions have deepened our understanding of policy options for announcing security on the Korean Peninsula, including by further expanding the role of the ROK-US alliance, and the need for the US and its key allies to build resilient technology supply chains. And they have, as well, shed some valuable light on practical aspects of North Korean cyber threats, to name but a few.

In conclusion, I would like to take this opportunity to thank all our keynote speakers, moderators, and panelists for their wonderful contribution. [inaudible] It is not every day that one gets to have eminent researchers in the field of Korean security issues, senior ROK and US practitioners and next generation scholars together at the same time. Their input has been invaluable. And

without doubt their insights have made this event a great success. Since this summit is annual event, I very much hope to have the opportunity to meet in person with everyone again next year.

Thank you very much indeed.

DR. JOHN PARK: Terrific closing remarks. Thank you so much. To conclude, I'd like to convey another set of important thank yous. Special thanks to ROK Foreign Minister Dr. Park Jin for his excellent speech on day one, as well as Belfer Center Executive Director Natalie Colbert and Korea Foundation President, Dr. Geun Lee, for their outstanding welcoming remarks.

Over the past three days, our amazing speakers and moderators skillfully examined how Korea acts as a catalyst of global trends. We're grateful for their insights. I'd like to specifically thank the Korea Foundation for their strong support of the Korea Project here at the Belfer Center. Our deep thanks to you, our audience, for joining us, and further growing our policy research laboratory on Korea.

On a final note, I'd like to thank Alex O'Neill. He has always been an amazing force multiplier in convening the Annual Summit. As co-founder and co-lead of the Korea Project's North Korea Cyber Working Group, Alex has been a thought leader in this fast-moving field. He has also been very generous in sharing the mic. Next year we look forward to bringing you another cast of really dynamic experts and sharing and engaging their discoveries. See you at the Fourth Harvard Korean Security Summit. Thank you.

END