OVERVIEW REMARKS

[00:01:13]

DR. JOHN PARK: Welcome to our second Harvard Korean Security Summit. My name is John Park, Director of the Korea Project of the Belfer Center for Science and International Affairs. It's great to have you join us today.

The goal of this annual event is to grow the Korean Security Studies Field by bringing together top researchers, senior ROK and US practitioners, and next-generation scholars. We seek to build on John F. Kennedy's observation, that we enjoy the comfort of our opinion without the discomfort of thought. We'll be placing the spotlight on the thoughts of our speakers over the next three days. These thoughts are rooted in our speakers' path-breaking Korea-focused academic research and policy work. Convened by the Belfer Center's Korea Project, the Summit is the anchor event for Korean Security Studies at Harvard University. Our thanks to the Korea Foundation for their generous support of the Korea Project and the Second Harvard Korean Security Summit.

[00:02:07]

This year our theme, Korea: An Oracle of Global Trends, explores how non-traditional and traditional security challenges evolve quickly on the Korean Peninsula, and provide broader insights for the global community. We'll see these dynamics at play during our panels, which cover the following topics:

One, Understanding North Korea's Leap in Cyber Capabilities.
Two, Examining the COVID-19 Lessons from the Korean Peninsula.
Three, Reading Kim Jong Un, which focuses on recent books by leading authors.
Four, Negotiating With the Nuclear North Korea. What's Old? What's New?
Five, Advancing the US-ROK Alliance in the 2020s.
And Six, Deterring a Nuclear North Korea. What's Old? What's New?

[00:02:53]
Our keynote speaker on day three will be Sydney Seiler, the National Intelligence Officer for North Korea at the National Intelligence Council, and the Office of the Director of National Intelligence.

For our kickoff today, it's my pleasure to introduce Secretary Ash Carter, who will be giving the US opening remarks. Secretary Carter is Director of the Belfer Center at Harvard University's John F. Kennedy School of Government. At Harvard he leads the Technology and Public Purpose Project, and serves as the Belfer Professor of Technology and Global Affairs. He served as the 25th US Secretary of Defense, after serving in the number two Chief Operating Officer, and number three, Weapons Czar positions in the Pentagon.

[00:03:37]
To make the Pentagon more innovative, Secretary Carter created the Defense Digital Service to bring tech experts into the Defense Department for a tour of duty. He opened Pentagon outposts in Silicon Valley, Boston, Austin, and other tech hubs, to reconnect the government and military with private sector leaders and companies. He has been an early leader in the US policy towards North Korea.

Secretary Carter earned his B.A. From Yale University and his Doctorate in Theoretical Physics from Oxford University, where he was a Rhodes Scholar. We are delighted to have you launch our summit today. Over to you, Secretary Carter.

[00:04:13]
ASH CARTER: Thanks very much, John. And welcome everyone. Thank you for being here. I thank President Lee for working with us to put this together, John Park, who is our spearhead at the Belfer Center for Science and International Affairs, for the very important domain of Korea studies.

[00:04:39]
I have decided, in my post-Pentagon life, to dedicate myself to the mission of this, the Belfer Center. And basically, we do two things, both of which are exemplified in this conference. The first is, that we bring together people to give the best—to develop the best policy ideas we can, so that those, in my case, who come after me as policymakers in Washington, but also others around the world, have better ideas than were available to us when we dealt with the problems of the world. And I am still committed to solving those problems of the world. And this is my way of helping to do that now, with wonderful colleagues like John Park.

And the other thing we do is produce the next generation of practitioners and thinkers about these important issue areas and parts of the world. Mentoring them, developing them, and launching them out into the world.

[00:05:46]
One side of this, which won't surprise many of you, is that there are a large number of Belferites and Harvard Kennedy School people and other people from Harvard, and also MIT, where I am also affiliated, who have joined the new Biden administration in important positions. And that is a sign of the pertinence of both of our missions, both the ideas that are developed here, and the people that are developed here.

This is not unusual in administrations of either party. It was less pronounced in the case of the Trump administration, only because the Trump administration did not draw heavily from the—what I'll call the usual body of expertise in the Republican party, which might have populated the senior positions in the Trump administration. But that was unusual. And certainly, the previous administrations of both parties, all of whom I worked for, starting with the Reagan administration, drew on our expertise and our people. So I'm really pleased to see that.

[00:06:59]
There are a few people on the program that I can't mention all of them, lots of really quality people. But I happened to have worked with Victor Cha over the years, in many different ways.

Also, Abe Denmark, when he was at the Pentagon. And, of course, we've all benefited from Robin Wright many times. And all of you who are going to populate these panels, this is the A-Plus team. And I congratulate John on getting them all.

[00:07:28]
I'll say a few things myself, if I may, about North Korea. I started my early deep involvement with the North Korea issue, when I was an Assistant Secretary of Defense. It was 1994. And I spent about half of that year preparing for war on the Korean Peninsula. I would have giving you 50/50 odds at that time, that there would be a war over the North Korean nuclear program at Yongbyon. For reasons we don't have time to go into, that didn't eventuate, and there was no war on the Korean Peninsula. But, in the course of preparing for that war, I became deeply impressed—more deeply impressed with the gravity of it. It is a war that no one can want. I know who will win, we and our South Korean allies. But it's a very miserable circumstance. And we avoided it if at all possible.

[00:08:27]
I next rejoined that area in 1998 in a serious way, that is, when North Korea launched a ballistic missile over Japan. And President Clinton asked Bill Perry to run the so-called Perry Process. And I served as Bill's Deputy. And Madeleine Albright sent as her Deputy Wendy Sherman, who is right now taking a position, or shortly will, as the Deputy Secretary of State in the Biden administration. Wendy, Bill, and I made many trips to the region at the time, including a very memorable trip to North Korea, one of several times I've been there.

I know you all are going to be talking about many things regarding North Korea. I'll just tell you in a nutshell the essence of my recommendations to any of you who is thinking about policy towards the North Korean puzzle. A few critical ingredients. First, I always felt that a policy towards North Korea that was effective could not be a purely American policy. That is, for us to be successful, we had also to make sure we were closely aligned with our close allies, South Korea and Japan. But also, the other major party in the region, namely China. Russia less so, but also, if possible.

[00:10:10]
And that that was an important source of strength, because we collectively, if we could agree on a negotiating strategy towards North Korea, were more potent in negotiations, because we could pool our carrots and sticks. That was helpful to the United States, because the United States is long on sticks and short on carrots, bsically. We have military power, but we don't do very much for North Korea and are not prepared to do very much for North Korea.

If we do do anything for North Korea, in the course of those negotiations, we should get something for it, which is why I thought President Trump's embrace of North Korea, basically giving them legitimacy as a leadership that they'd long sought for free, was a strategic mistake. But what's done is done, but that was a mistake. And we now have to proceed from that point. But you need to marshall your carrots and sticks, and we're better off doing that when we have friends and partners with us.

[00:11:30]
And the last thing I'd say is, the US forces on the Korean Peninsula are important to deterrence. We really need to make sure that, at no point, or any combination of circumstances, anybody gets the idea in North Korea, that it would be a good idea to begin a war on the Korean Peninsula. As I said, I know who would win. But that's a very ugly circumstance, and to be avoided if at all possible. And deterrence is a good way to do that. US forces are critical to that deterrence, although the South Korean forces have steadily increased in power and competence in my lifetime of working with them.

US forces on the Korean Peninsula are more generally useful to the United States and to our friends and allies in the region, by signifying US engagement with the region. So they have a larger value than Korea itself. So I think those are the ingredients of a good strategy towards North Korea. But there's a lot more towards policy with respect to North Korea. There's humanitarian policy on food and other aspects to policy that are just as important. It's very—It's essential to gain all the understanding you can of this very mysterious place. A lot more known

than when I first started out, but still pretty mysterious. And that's another place that this meeting can shed light.

[00:13:04]
So John, I congratulate you on putting together this conference. I'm pleased to welcome you all to it. And I look forward to learning what the results are.

[00:13:21]
DR. JOHN PARK: Thank you very much, Secretary Carter, for officially launching the second Harvard Korean Security Summit. Much appreciated. We'll now move to brief remarks from Dr. Geun Lee. Dr. Lee was appointed President of the Korea Foundation in September of 2019. Prior to his appointment, he was Professor of International Relations at the Graduate School of International Studies at Seoul National University, where he was also former Dean of the Office of International Affairs.

Dr. Lee was also former Chair of the Global Agenda Council on the Future of Korea at the World Economic Forum, and is a current member of the Global Future Council of the World Economic Forum. He earlier served as a professor at the ROK Ministry of Foreign Affairs' Institute of Foreign Affairs and National Security. Dr. Lee received his B.A. From Seoul National University and his M.A. And PhD in Political Science from the University of Wisconsin at Madison. We'll now turn over to Dr. Lee's recorded opening remarks.

[00:14:25]
DR. GEUN LEE: Distinguished participants, ladies and gentlemen, good afternoon. As President of the Korea Foundation, it is my great pleasure and honor to sponsor the Second Harvard Korean Security Summit. On behalf of the Korea Foundation, I would like to express my sincere gratitude to the Belfer Center for Science and International Affairs for organizing this meaningful annual event as part of the Korea Project.

[00:14:52]

The KF is very proud to support the Korea Project, which was inspired by the late Ambassador, Stephen Bosworth's impressive vision for security on the Korean Peninsula. Since its establishment nearly 30 years ago, the KF has consistently extended support to Korea-related academic research. Our goal is to invigorate Korea-related research in the United States, and strengthen US-Korea academic ties, in collaboration with prominent universities and institutions in America.

As the field of Korea studies grows increasingly diverse, the KF has responded by expanding our focus, supporting research on a wide spectrum of areas, from traditional regional security and trade issues, to the environment, energy policy, technological innovation, democracy, and more. Of course, the KF remains aware that, because of its foundational importance, security was and will always be one of the most critical issues in US-ROK relations. Scholars and policymakers alike will attest that the scope of these challenges, too, has grown, first with the introduction of the term “non-traditional security,” and then with the emergence of COVID-19 and cybersecurity.

[00:16:18]
Some top tier moderators, and an excellent mixture of established and emerging expert panelists, are here today to start off this event. As we work together, we will witness the exchange of diverse ideas, perspectives, and insights Above all else, I expect that the discussion over the course of this meaningful occasion will help the new Biden administration in shaping its policy toward the Korean Peninsula, as well as the Indo-Pacific, ultimately contributing to a closer bilateral relationship.

In closing, I would like to express my sincere gratitude to all our invited guests and experts who are coming together here and now. In particular, my appreciation goes out to all scholars and practitioners for your devotion, passion, and expertise, as you help build an even better future for the US-ROK alliance. Thank you very much.

[00:17:24]

DR. JOHN PARK: Our thanks to Dr. Lee for the ROK opening remarks. Before turning to our first panel, I ask our speakers to remain muted with their videos on. Our first panel today focuses on a puzzle. It's a story of how North Korea leaped forward in its nuclear—its cyber capabilities. My apologies. We have an excellent group of experts dive into this puzzle. Moderating Panel 1 is the award-winning correspondent Nick Schifrin, who will also be introducing our experts. Nick is the foreign affairs and defense correspondent for PBS News Hour in Washington, D.C. He leads News Hour's foreign reporting. The PBS News Hour Series, *Inside Putin's Russia*, won a 2018 Peabody Award, and the National Press Club's Edwin M. Hood Award for Diplomatic Correspondence. In November of 2020, Nick received the American Academy of Diplomacy's Arthur Ross Media Award for Distinguished Reporting and Analysis of Foreign Affairs. We're glad to have him here today. Over to you.

PANEL 1: UNDERSTANDING NORTH KOREA'S LEAP IN CYBER CAPABILITIES

[00:18:21]

NICK SCHIFRIN: John, thank you very much. And thanks to everyone for joining us, and thanks to the panelists for joining us. I see you all populating there. So let me introduce the panel. Understanding North Korea's Leap in Cyber Capabilities. And we will talk about Leap in a second. I just want to introduce our three panelists.

First, Priscilla Moriuchi, the Threat Intel Lead at Apple, a nonresident Fellow with the Cyber Project and Korea Project at the Belfer Center, and the former Enduring Threat Manager of the National Security Agency. Welcome. Dr. Ben Buchanan joins us. He's the Director of the Cyber AI Project at Georgetown Center for Security and Emerging Technology, and the author, most recently, of a couple books, *The Hacker in the State: Cyber Attacks and the New Normal of Geopolitics* and *The Cybersecurity Dilemma.* And Jenny Jun joins us as well, a PhD candidate at Columbia University. She's researching the Bargaining Model of War, Strategic Dynamics of Cyber Conflict and Security Issues in Asia, East Asia rather. And she is the co-author of the CSIS Report, *North Korea's Cyber Operations, Strategy, and Responses.*

[00:19:33]
And so let me just take us through a couple of early points to get us started. Again, Understanding North Korea's Leap in Cyber Capabilities. We've gone from, in the 2000s, North Korea focusing on R&D. 2009 we saw the White House website defaced. 2011, the DDOS attack on South Korea. By 2013, North Korea cyber actors were using wipers, like those introduced by Stuxnet. We had, of course, Sony hack in 2014, and WannaCry in 2017. so that's now three and a half years ago.

And so, in talking to intelligence officials and others, people describe significant improvements to the effectiveness of cyber operations and the scope, and reports that the internet is used, not only for revenue generation, but acquiring knowledge and skills. And the internet in North Korea has become a professional tool for the leadership. And intelligence officials describe a few goals, regime survival, as we'll get into. And that requires money, of course, to avoid sanctions.

[00:20:42]
About a year and a half ago, the UN Security Council report estimated that North Korea had two billion dollars in illicit cyber operations, mostly cryptocurrency, financial transactions Another motivation, of course, improving life for citizens. And the most recent example, perhaps, that we'll get into, is targeting COVID vaccine research. But there is more than that, those two motivations. Just in the last couple weeks, we have seen Google say that North Korean hackers targeted researchers across the world, believed to be researching the vulnerabilities in Google.

And of course, because we're the first panel, we should just mention the strategic implications. We have a new administration. The Secretary of State, Anthony Blinken, has mentioned a review of all options for the US, whether it's sanctions, coordination with allies, what Secretary Carter called a pooling of carrots or sticks, and possible diplomatic incentives. And, of course, North Korea has threatened to create more advanced nuclear weapons. And most experts believe this could be a tense year.

[00:21:49]

So, with all of that as our frame, Priscilla Moriuchi, let me begin with you. Can you describe how North Korea's cyber operations are different from other countries, as you see? And that timeline that we just quickly went through, how do you believe they advanced so quickly?

[00:22:08]

PRISCILLA MORIUCHI: Sure. So to go back, I guess to the beginning, North Korea developed its kind of indigenous information technology program on its own, right. So the operators, the hackers, the software developers, right, everyone involved in internet technology in North Korea was largely trained right through their own system. There's been sort of some back-and-forth, right, in the academic community about where it came from.

[00:22:35]

And we should give them that credit, right. They took the initiative in the late 1990s, and developed a series of schools, right. And that has allowed them, one, to sort of create their own system of indigenous training and operators. But two, they also embraced a model that was completely different than other nations, in which, for a long time, I would argue, probably up until the last year or 18 months, the vast majority of their cyber operators were stationed overseas, right, in third party countries, where they had more open access to the internet.

And they were able to leverage that access to, for example, conduct operations, to—what's the best way—to engage with the internet community, including cyber criminals, right, gaming operators, and stuff like that. So you, one, you have this indigenous development of IT professionals, right, some of whom became sort of offensive cyber operators. Two, you have a system in which many of the operations that were conducted, in a really risky manner, right, from overseas.

[00:23:41]

And then third, as that—while in sort of the unclassified world, we know relatively little about the traditional cyber espionage that North Korea undertakes as sort of government-to-government spying, we know a lot more about non-cyber espionage. And for North Korea, that is

centered on generating revenue, right, for the Kim regime. And that's completely different model than any other country. By and large, you won't see many other countries who utilize the internet to circumvent international sanctions, right, to steal—essentially to conduct, right, bank theft, right. You know, these really overt criminal actions, right, in support of the regime. So for me, those are the three most distinguishing points. North Korea is not a traditional nation-state when it comes to cyber ops.

[00:24:31]

NICK SCHIFRIN: Jenny Jun, that focus on generating revenue, we've absolutely seen that. And North Korea operators are more creative, more adaptive, more contemporary, I think, is the word that you've used recently, than they get credit for. What do you mean by that? And what's the implication of those skills, I guess?

[00:24:51]

JENNY JUN: Right. To add onto what Priscilla said, I think another thing that kind of sets them apart is sort of the—their destructiveness and their dedication. And so, you know, in comparison, North Korea as a particular groups are perhaps not as technically sophisticated as Russian APT groups And they do make sloppy mistakes from time to time. We saw some of this in WannaCry in their campaign in the Bangladesh bank heist. And more recently, in their ransomware encryption algorithms, and things like that. So they're not perfect.

But to them, it doesn't matter, right. A break-in is still a break-in, regardless of whether you can do it without, you know, anyone knowing, or if you can do it by tripping off all the alarms, and breaking stuff in the process, you know, North Korea is less deterred by sort of this possibility that they might be burning some tools, and tipping off the other side of the process. And what other nation-states may not touch, you know, North Korea has relatively little hesitancy in going there. So I think that's another difference.

[00:26:05]

And part of, sort of a phenomenon that comes out of that, is because they're less worried about secrecy and sort of being discrete, what they'll do in compensation for that, is they'll destroy a lot of things in the process. And so that's, I think, one other difference, if I can add to what Priscilla said, is going on.

NICK SCHIFRIN: And Ben, how do you believe the North Korean regime developed these capacities so quickly? And I know that you've also looked at the destructiveness, and also seen examples where North Korea hasn't done so well at what it meant to do. So do we know, really, how they compare to other countries—obviously China and Russia, but to other countries when it comes to absolute capacity and what they actually can do?

[00:27:01]

DR. BEN BUCHANAN: First of all, thanks for having us and this conversation. I think there's no doubt that the North Korean capacity in this space is probably less than other nations like the United States and China or Russia. What's remarkable about North Korea is their willingness to use those capabilities, as both Jenny and Priscilla have said, and some of the blow-back they are potentially willing to court in using those capabilities. So the brashness of these operations.

I think one way of looking at this is their desperate—or seemingly desperate, but still capable nation in this respect And I think—I'm sure we'll talk about the Bangladesh bank heist. Jenny mentioned it. It's a significant part of understanding North Korean operations to gain revenue, as Priscilla said.

[00:27:44]

But, what's remarkable about that operation, I think, is because it's gotten so much public attention, it's easy to see it as an outlier. Whereas I think it's more properly viewed as part of a broader campaign. As you said, Nick, in your opening comments, it's a campaign that the UN report suggests has reached and upper one and a half or two billion dollars in revenue for the regime. It's a campaign that has hit a lot of cryptocurrency exchanges and the like, as well as other banks, as well as ATM withdrawals through Cosmos Bank.

[00:28:13]
And what's striking about that campaign, I think, is how the North Koreans have a remarkable willingness to try a lot of things, and see what works, all in service of getting revenue for their regime. And that makes them a very different kind of actor than the other countries that you mentioned. Even a country like Russia, that's still aggressive, I think has a higher bar for operations and greater capability in executing those operations than North Korea does.

NICK SCHIFRIN: So Priscilla, back to you. Do we know the extent of North Korea's capabilities? And it seems to me that we haven't been necessarily good at predicting next steps when it comes to these things in general, but especially North Korea.

[00:28:52]
PRISCILLA MORIUCHI: So I'd argue we don't, right. And to sort of—We only know what gets discovered, right. So, when it comes to cyber operations, nobody is perfect, right. The United States is not perfect. We've seen China, Chinese groups, Russian groups, right. Everybody makes mistakes. And we can only assess, right, based on what we actually catch, right, from a defensive perspective.

So what we know there, right, is that, to sort of jump on what Ben was saying a little bit, North Korean operators are largely willing to take risk, right, both with their tooling and their capabilities, but also with the scope of their mission, right. China and Russia do not have a mission scope that encompasses generating revenue for their government, right. So therefore, they have a different set of tools, with different set of objectives.

[00:29:42]
For North Korea we know that they possessed what we would call sort of the full scope minus a supply chain capability. So looking at disruptive and destructive capabilities, certainly, right. Traditional cyber espionage tools, most definitely, right. We know, for example, that they are

willing, operationally, right, as sort of Jenny said, to destroy machines, right, and really execute that extreme extent.

[00:30:14]
I mean if you think about the Sony Pictures Entertainment attack, for example, in 2014, you had, you know, this foxing campaign, the release of documents on Hollywood actors and Sony elite, along with the traditional espionage campaign, and sort of physical threats, right, threats to movie theaters at the time, to prevent people from trying to go to see this movie.

So I would say, like certainly, that North Korea is not in what we would consider kind of the top tier of cyber actors, not on par with the United States or China or Russia. But is very close behind. And because they have a different set of requirements and strategic goals, that's where we get into this era of sort of, we make some comparisons, right, that are nation-state comparisons. When I would argue that the Kim regime is more like a criminal regime, right. And the tools, methodologies we see in the cyber operations, are sort of a combination of both, right, nation-states and criminal.

[00:31:11]
NICK SCHIFRIN: And Jenny, but at the same time, we have two incidents, which don't necessarily fit into the model of a focus on stealing money, most recently. One is, COVID vaccine targeting, the intelligence community said that that's been targeted. And this most recent incident, which you and I were talking about as well, which was just a couple weeks ago, targeting what seems to be researchers working for Google, trying to find vulnerabilities. And talking to US intelligence, it's not clear what they stole, or what they were targeting. But it seems to be something, you know, maybe related to Gmail or Chrome or something, presumably, that you could actually expand the aperture of what you might target as well. So talk about that.

[00:32:05]
JENNY JUN: All right, certainly So, I think in many ways, looking at what North Korea is targeting, in terms of their cyber operations, I think is really good open source data on what the

regime's priorities are. And given how North Korea is a really hard intelligence target, I think even NK watchers focusing on other areas, such as nuclear or leadership analysis, this is something that they also might be interested in, because this is a—usually a less noisy manifestation of what the regime is interested in. And we don't really have things like proxy actors in North Korean cyber operations.

[00:32:44]
And so, having said that, I think their interest in COVID vaccine research is very indicative of the domestic situation that they're facing within their country. And with regards to the second incident you asked, so basically what happened was, you know, beginning of maybe—you know, middle of 2020 last year, North Korea set up an elaborate sort of social media scheme. You know, they would have fake YouTube accounts, several Twitter accounts that would sort of speak to one another and gather followers. They would set up these fake research blogs. And they would basically use that to interact with vulnerability researchers in the US, but also abroad, so Europe, Middle East, China as well.

[00:33:37]
And they would basically use this to build up credibility and get the vulnerability researchers to click on seemingly normal-looking blogs, and ask them to collaborate with them. But really, it would be a vector to download backdoors into their own systems. And so we don't really know exactly the full extent, the full consequences of this activity just yet. But some details are emerging, right.

So (a) it seems as if they targeted these vulnerability researchers for information. And what's worrying is that it might be that they were targeting vulnerabilities, right. They were looking to steal, exploit, and possibly other zero days. Another thing that's interesting is that they are willing to burn very precious zero days in the pursuit of this activity, right. So this must have been quite high on their priority list, in order to basically go with this operation

[00:34:49]

We know that in at least one occasion, they used either a visual studio or Chrome X zero day exploit. We know, also, that they used a Internet Explorer zero days exploit. And so this is worrying, because we don't fully know what the intentions of the North Koreans are when we see incidents like this. And because the signaling value of these actions are quite murky at this stage. And there isn't a shared understanding of, if you do this, both the US and the North Koreans know exactly what's intended out of this. And the worry is that, you know, this is a precursor to some other big event that the North Koreans are planning, so important to the point that they're willing to burn more than one zero day in the process.

NICK SCHIFRIN: Ben, is that how you see the recent cyber espionage that Google unveiled? And if I could take a minute, Priscilla argued about the indigenous capacity. Is there any question about whether this capacity that we're talking about, just from two weeks ago, or even a couple years ago, is indigenous?

[00:36:02]

DR. BEN BUCHANAN: I have not seen any indication it's anything but indigenous, provided we define indigenous to include North Korean operators located overseas. So I think it's probably fair to say that a fair number of North Korean cyber operations, and we're going here based on a lot of the media and private sector reporting, are carried out from places other than North Korea. And there would be good technical reasons why, given how relatively sparse the connections are in North Korea, and so forth, North Koreans would want to do this.

But we have not seen, to my knowledge, North Korea using private sector companies and the like to carry out their operations in the way we've seen some autocratic regimes elsewhere in the world rely on the private sector. As for what comes next for North Korea, I think it's probably fair to say these operations, at least aspirationally, were trying to enable the country's broad spectrum cyber capabilities, gain access to vulnerabilities and the like.

[00:36:55]

I think the real question for North Korea is, we haven't seen a notable attack since 2017's WannaCry, which was a very complicated attack in its own way, in terms of what the intention was of that. Was it an accident? Was it something else? And WannaCry certainly showed, intentionally or not, a remarkable and aggressive capacity to hit a large number of targets. As you said, and as Priscilla said, they have come a long way in their scale and scope of operations, from 2009.

[00:37:24]
And I think the question that emerges, that Jenny was hinting at, is well where are North Korean capabilities in 2021, should they have cause to use them? I don't think anyone, at least outside the intelligence community, has a credible claim to answer that question But it does seem to me that taking WannaCry as a snapshot of what they were thinking in 2017, they are likely further ahead than that now. The form of those capabilities, and their willingness to use them, are both still uncertain.'

NICK SCHIFRIN: And Priscilla, back to you. Before we get into kind of policy indications of the fact we don't know some of these things, and what we should do about them, and sanctions, I want to take a minute just to talk about this, The Recorded Future Report, and have you put some of this into context. So the findings in the last few years are that North Korea's use of the internet has gone up about 300 percent. Internet has become a more professional tool for the government. And they specifically cite the fact that, in the past, we would see internet usage peak in evenings, and on the weekends. And instead, now, it is nine-to-five, give or take. So what's the implication of that, for cyber capacity in North Korea?

[00:38:38]
PRISCILLA MORIUCHI: Sure. So there are a number of implications. So one, just on a day-to-day basis, right, internet is becoming a professional tool for those who can access it, right, with the caveat that, in North Korea, it's a very, very tiny number of people, right. I like to call them sort of the point one person, right. You're talking about the senior leadership and their family's party, military, you know, some researchers and students, right.

[00:39:03]
But largely, we're looking at a very small number of people. For a country of about 25 million people, when you look at their internet footprint, it's unbelievably tiny, right. There's no ability to profile the internet usage of another country of 25 million people, because most of those 25 are accessing the internet and using it every day. So for North Korea, it's a very unique case, because, you know, such a small number of individuals, and has regulated access.

And a few years ago, there were relatively few egress points, right, actual physical cables that connected DPRK, right, to the rest of the global internet. That has changed substantially over the past few years. So in 2016 and 2017, there were largely two cables run by a Chinese telecommunications company. There was a backup satellite connection, right, from DPRK, that was used as a backup, and relatively sparsely.

[00:39:56]
And over the course of the last four to five years, you know, the capacity, the ability, the bandwidth, right, just nuts and bolts of reaching the internet, right, has scaled tremendously. We've gotten another provider that's TTK Trans Telekom, it's a Russian company. So kind of layering a bunch of backups there. The capacity is being built on the hardware side on the North Korea end, right, installing of the basic things like name servers and mail services, like the boring stuff that you actually have to use, right, to access the internet. So right, that hardware is being established, the bandwidth and capacity that we see more usage, right. Not just kind of the entertainment, streaming videos, and social media. But the ports and protocols associated with working services, like I said, emails and surfing, research, and things like that.

[00:40:45]
And so, from a capability perspective, one, you obviously have sort of a level of leadership who are willing and more engaged, right. I think we always think of North Korean leadership as so isolated. But I think the reality is, they may be physically isolated. But, when it comes to

information, right, and access to the outside world, they aren't isolated. They are aware. They're reading news. They're engaged in the internet society. So that's one, right.

[00:41:13]
Two is that the actual military and political elite, the commanders, right, they are researching, right, techniques, information, security techniques, nuclear techniques, agriculture techniques, coronavirus, for example. And as an implication, right, we can no longer kind of assume that North Korea conducts their operations in this kind of information bubble, right. We have to understand that they are aware, largely of their role.

And going forward, I think as long as the sanctions hold, right, and we continue to employ sanctions regime, North Korea will continue to use the internet as a tool to circumvent it. So that will include, from territorial North Korea, and the leadership there, as well as the networks that they have spent decades, both the physical and the virtual networks, right, establishing in the rest of the world, outside of just their traditional kind of partnerships in China and Russia. So that's one.

[00:42:15]
I think we will—It's probably one of the reasons why we haven't seen one of these kind of flashy attacks WannaCry style, in my opinion, right, is that the focus has been on revenue-generating. And two, to be honest, North Korea has employed a strategy at the tactical level, as have a lot of nation-states, in incorporating more of what we would call commodity tooling. So now, where in infrastructure, that is used by criminals, that's commercially available, that you can tweak, right, and utilize for your own purposes, that makes it a lot harder, one, to detect intrusions when they occur, and two, to actually beat them with a high degree of certainty. So it's probable that we have seen North Korean operations over the past few years. But we don't have a very high degree of certainty that it was actually them, right. And maybe we have low certainty in that case.

NICK SCHIFRIN: Jenny, I saw you shaking your head in agreement. Hard to detect, hard to be certain. It was then. What are the implications of that moving forward?

[00:43:18]

JENNY JUN: Right. So sort of adding onto what Priscilla said, we have, in the paste few years, we have seen that North Korea is not shy about collaborating with—not only using commodity tools available, but also collaborating with non-state sort of criminal groups that we usually, you know, traditionally haven't really seen much. And so they would rent out initial access from gangs like TrickBot and things like that. And so this is absolutely true, that North Korea is not shy about mixing and matching tools in order to get what they want.

And so that, I think, you know, obviously has problems for protection, but also attribution. And which means we are at risk of not only, you know, some are getting through the cracks, but also that it's going to be hard if we make—to make attributions with a high degree of certainty. And the less ability to do that, is going to work towards North Korea's advantage on that end.

NICK SCHIFRIN: Ben, is that how you see it, that that could work toward North Korean advantage?

[00:44:41]

DR. BEN BUCHANAN: I am less worried about attribution, I think, than others, generally, in cyber operations And I don't think North Korea is a particularly significant exception here. I think in general, attribution, at least for a government level—and it's different for the private sector—attribution is less difficult than people think. And essentially, two ways in which you can do attribution if you are a government. The first is, you can rely on forensic data after an incident takes place. And the second is, you can surveil the infrastructure of an adversary as they are carrying out the operation.

[00:45:16]

And, while I don't think it's the case that all of North Korean infrastructure is covert, I'm sure some of it is, in fact, covert. I do think that the US government probably has more capacity to attribute than sometimes is portrayed in popular reporting. And I think back to the Sony case,

where there was a lot of discussion, is this Russia? Is this someone false-flagging as North Korea? And I think it was pretty clear to the US government, reasonably quickly, that this was, in fact, North Korea. And there was a fair amount of evidence for that.

[00:45:46]
And even if you look at some of the attempts of others to false flag as North Korea, I'm thinking here of Russia's Olympic Destroyer malware in 2018, I think that was pretty quickly sniffed out as a false flag. So not actually North Korea, but someone pretending to be. So in general, I think attribution is more doable than people think for a nation with the signal [?] intelligence capacity of the United States.

NICK SCHIFRIN: Priscilla, you mentioned that sanctions—I'm sorry, not sanctions—hacks and cyber espionage as a tool to circumvent sanctions. Let's talk a little bit, for a few minutes, as we kind of transition to the more strategic questions, can sanctions be a tool to signal? Can sanctions be part of North Korea's communication with Washington and the world? Has it done that in the past? And could it do it in the future?

[00:46:41]
PRISCILLA MORIUCHI: Certainly. And so my perspective is that sanctions have been a useful tool, right. So the current sanctions regime that we work under focuses on, one, territorial North Korea, right. So the physical territory of North Korea. And two, the traditional commodity shipping, right, coal, oil, revenue generators of North Korea. And that's been an effective hammer for a while.

But we are at the point where North Korea has developed this sanctions circumvention model, right, where there is no doubt that they are still under a lot of pressure, because of the sanctions regime, because of the—for example, the forced pullback of foreign workers, right. There was a lot of dependency on North Koreans living abroad, working on jobs, and sending money home, right.

[00:47:40]
But the use of the internet, right, by leadership, by cyber operators, it allowed them to create a system outside, largely, of international financial and government control, in order to generate the funds and, more importantly, to move the funds. There are a lot of gaps, a lot of places we don't know. For example, how do the funds from a cryptocurrency op, right, get back to North Korea? We have some idea from some FBI indictments that there are intermediaries, right, who essentially wash the cryptocurrencies, and take a fee, and send them back to North Korean individuals.

But largely, we don't know. Can you purchase? Can you purchase oil and coal, right, with Bitcoin, or Monero, for example, which is another currency? When you move the currency, cryptocurrencies, just for example, right, between mixers, right, which are essentially digital launderers, right, you mix them up between different currencies, you exchange them, right, there's a fee at every single step.

[00:48:43]
So there's a calculation that every time, you know, North Korea moves, conducts an op, or generates revenue using cryptocurrency, exchanges it—runs it through a mixer and exchanges it into only one other currency, you're losing anywhere from 10 to 20 percent, right, of that revenue

So, you know, that's the same thing with sort of the SWIFT, right, the fraudulent SWIFT transactions. In many of those cases, if you look at banks in the Philippines for example, there were physical individuals, right, who took that money out, and moved it through the Macao Casino system, right, to kind of clean it off. So there's these networks, right. And this is not a new thing. It's just that we have managed to use the internet, right, to layer on the networks, the physical sort of smuggling and illicit networks that Jenny was alluding to, that they had established for four decades, right, and just used the internet as the tool, another tool, right, to move the money around and get it around international financial controls.

[00:49:38]

I think we're moving in a direction, though, as the international community, with know your customer, or KYC rules, in the cryptocurrency sphere. For example, right, where we're kind of trying to put the squeeze from some countries, right, onto this kind of illicit market of revenue, moving revenue. But largely, we see them—I see that it's still effective, right, in circumventing sanctions.

NICK SCHIFRIN: And so Jenny, if that is a successful circumvention, or they've figured that out, what do you believe the Biden administration should think about when it comes to the pressure points it can use, in order to change North Korean behavior?

[00:50:21]
JENNY JUN: Right. So I think we can think about this, you know, as sort of a tactical/operational level issue, versus a strategic issue. And I think, you know, sanctions we can think about in multiple ways. But I think one way to think about it is, you know, it's currently used as part of a wider set of tools that the US is currently using under the umbrella of counter-cyber operations, which includes things like naming and shaming, exposing North Korean TTPs, taking down some of their infrastructure, including botnets, you know, indictments, going after its cryptocurrency earnings, make it difficult for them to cash out.

[00:51:04]
So sanctions are part of that wider sort of package. And the goal there, I think, is to disrupt any operations that North Korea is planning, and to get North Korea on the defensive, basically. But we also have to see the implications of these actions that the US government is doing, at the strategic level. And also, in relation to other domains, such as what they're doing in the [00:51:29] program.

So I think, you know, at a basic level, I think it has to be understood, and clearly communicated to the North Koreans, that these sanctions are to be conditional, right. And so, because, in the end, these sanctions are, in the end, just a means to another end, which, as you have said, Nick, to get them to change their behavior in some way, whether we apply sanctions to their human

rights violations, to their nuclear missile programs, or to cyber operations. And if we don't really clearly communicate that these sanctions are applied at a conditional basis, rather than simply just an unconditional, sort of punitive retaliation to a past wrong-doing.

[00:52:14]
And what this basically does, is this doesn't really provide them a way out. And so sanctions will, you know, tacking on more sanctions will only make North Korea sort of double down on its current ways. And this is, I think, where a lot of the diplomatic efforts come in, to really communicate that at a very high level.

NICK SCHIFRIN: Ben, do you believe that there are sanctions that could change North Korea's cyber posture and actual cyber operations?

[00:52:43]
DR. BEN BUCHANAN: I think I'm the role of skeptic here. Once again, I am skeptical that there is a lot that the United States and its allies can do to change North Koreans' cyber behavior. And I think that the reason for that is, we are struggling, it seems quite evidently, to contain the country's nuclear ambitions, and nuclear program, and missile program, to say nothing of its human rights abuses.

And I think one of the remarkable things about cyber operations, perhaps the defining characteristic of cyber operations, in my view, what they take place between, in this gray zone between war and peace. And oftentimes, I think nations, including North Korea, have recognized that, provided they stay in that gray zone, there's not a lot other countries can do to respond to it. And I think we have shown, over the last couple decades, not just with North Korea but more generally, that sanctions and indictments really haven't slowed the ambition of adversarial nations in cyber operations. And I'm not sure why North Korea would be different.

[00:53:43]

I could imagine a couple of things related to the banking system and like that, that might have some narrow effect. But more generally, I don't think that's going to change their behavior. And I think that the meta point here is really important, because your original question was about sanctions as signaling. And I do think sanctions can have a signaling effect. But the thing that doesn't have a signaling effect in many respects, despite a lot of academics [?] leaders [?] saying it is the case, is cyber operations. And I think cyber operations are best seen as a tool of shaping, gaining an advantage in this arena of international competition. Certainly, that's how North Korea has used them in many, though not all, respects And I think we shouldn't be surprised when they continue to use a tool of shaping that they think is beneficial to them.

NICK SCHIFRIN: Priscilla Moriuchi, I have kind of set up Ben Buchanan as the skeptic. Do you want to respond to that?

[00:54:24]

PRISCILLA MORIUCHI: Yeah, sure. No. I think, maybe as the token private sector rep here [laughter] One of the things I also wanted to inject, is like for North Korean cyber operations, most—many of the victims are actually private individuals and private companies. So that's largely different than traditional nation-state cyber operations that we look at with Iran or Russia or certainly the United States, in that many of the activities, I think anyway, that the government is undertaking, the naming and shaming, the publishing of IOCs, right, is for the benefit of the private sector to be protecting itself.

So some of this non-sharing, some of the attribution, there's no doubt, right, that the government, the intelligence services of the United States can perform attribution much better, have much higher confidence, right, when they see indicators of North Korean activity, than in the public—the private sector, right. But the private sector doesn't have access to that. And largely, when you're looking at an intrusion, and you're a private sector company, or you're in private sector Intel, you don't have the benefit of anything beyond a North Korean endpoint, right. So you have a computer, an IP address, if you're lucky, right, that you understand was either command-

and-control, right, controlling a piece of malware, an exfil point for some data, right, or if you're super lucky, maybe an IP in North Korea, which almost never happens anymore.

[00:55:58]
So certainly, right, we are not effective as governments or the international community, in countering, right, cyber operations. Not great with North Korea. But I think it's sort of about raising the bar in the private sector, to enable the private sector to protect itself better, to understand what the parameters are, the TTP, the tactics, techniques, and procedures around North Korean operations are, and to help them.

And so, you know, that's kind of my perspective. Like cyber operations is a weird domain, right. It exists between war and peace, but it also exists between public and private. And government doesn't own most of the infrastructure. Government is not typically the most impacted in a cyber operation. And I do think a lot of it is about helping private sector protect itself.

[00:56:46]
NICK SCHIFRIN: So, as we're talking about protection and defense, you know, Jenny Jun I know that you also have been thinking about that in a much more strategic and cyber way. And maybe we could expand out a little bit even before we go, zoom back in, which is that, you know, as of 2018, the United States has a cyber strategy, which is much more dependent on defend forward, as the phrase goes, that has been borrowed from decades past, reliance on counter-cyber operations. This has been discussed a little bit before, but exposing toolkits, taking down botnets, naming and shaming, we've talked about with sanctions.

So in your response to Priscilla, talk about that. Is that a good strategy for the US to pursue? And how does that impact how the US should see, how we all should see the interaction with North Korea cyber capacity right now?

[00:57:50]

JENNY JUN: Right. So the slew of actions that the US government is doing right now as part of their counter-cyber operations, come out of this 2018 shift in sort of a high level US cyber policy towards a recognition that cyber space, you know, is a space characterized by constant contact. There is no—It's not as beneficial to rely on threats of punishment to achieve a deterrent. But, because, as Ben said, a lot of these activities are occurring in the gray zone. And therefore, it's going to be a fact of life that these intrusions and attacks will continue.

And one of the sort of implications that came out of that was, we need to defend forward, right. We need to not be static in our defenses, but actually go outside of US networks to actively disrupt enemy capabilities. And so these operations are all sort of part of that. And so as Priscilla said, I think we have to kind of calibrate our expectations as to what that's going to do, and what that isn't going to do. So I think absolutely, as Priscilla said, you know, some of these are critical, to bring up resiliency and defense in the private sector, in the visuals, and in the general community as a whole. And that's going to have a positive effect, in terms of the overall offense-defense balance between North Korea and the US.

[00:59:24]
At the strategic level, however, I think we need to still—You know, there are a few more kinks we need to think about, in order to really take this forward. So first, we haven't really thought enough about the risk of escalation that comes from misperception, right. So what we believe to be completely non-escalatory, purely defensive actions we are doing to degrade North Korea's capabilities, may be interpreted by North Korea as a very escalatory measure that cuts off their vital funding stream, which would leave them in a more sort of vulnerable position at the negotiating table. And therefore, they perceive this as much more escalatory than what the US intends it to be.

[01:00:011]
So a lot of these, you know, hypothetical scenarios haven't been sort of thought out properly, or have been explored empirically even, as this is a relatively new phenomenon. And so we have to be wary when we're doing all these sorts of actions, coming from the US sort of strategic

mindset, we have to think about how the North Koreans might be interpreting some of this, and whether that's going to lead to any sort of misperception, and therefore miscalculation between the two countries.

NICK SCHIFRIN: Ben, it seems to me that that, and we'll stay a little bit wide here, and then we'll zoom back in, because I've still got about 20 minutes before questions. But it seems to me that that problem, that concern of misinterpretation, does not only apply to North Korea, right? I mean, you know, you don't only look at North Korea when it comes to cyber. How do you see that problem, not only with North Korea, but perhaps other places you look at?

[01:01:10]

DR. BEN BUCHANAN: Not only does that not only apply to North Korea, it doesn't only apply to cyber. I mean this is a version of a problem that goes back at some form to Thucydides. And Graham Allison at Harvard has written about that Thucydides trap. Robert Jervis down the hall from Jenny, of course, has written about the security dilemma, the cyber security dilemma, as I like to call it, certainly is a significant problem. It doesn't, I think, invalidate the approach of defend forward. It's really something that senior people in government are tracking.

But I think the broad fact here, the strategic bird's eye view fact, is that cyber operations are often very hard to interpret. And that makes them hard to use as signals, that we talked about before. But it also means that operations that are undertaken with genuinely defensive intent on the receiving end can look intrusive and offensive. And the challenge for defend forward in general, certainly the challenge for defend forward with regards to, let's just say a peculiar state like North Korea, that has its own interpretations of things, is how is the other side going to see the activity if it's uncovered?

[01:02:13]

And certainly, I think the US policymakers are well aware of these risks. Doesn't mean they can manage them well, necessarily. That's, I think, yet to be seen. But there's no doubt that this is an obvious challenge of a more aggressive strategy. As Jenny said, there's a risk of misinterpretation

and misperception. And as you said, Nick, that's a risk that is endemic to operation in this domain beyond just North Korea.

[01:02:37]

NICK SCHIFRIN: So we've got about 15 more minutes or so. So everybody start thinking about their questions in which we'll go to at about 20 minutes or so, to the hour, and have decent amount of time for those. I wonder if I could pose to each of you a dual question. And that will open up, I think, a couple of points that we've gotten to., by zooming back into the cyber capacity. So Priscilla, why don't you start. Do you believe that we're underestimating any of North Korea's capacities? And, to a certain extent, at the beginning we talked about—and I asked, I think, multiple of you what don't we know. And is there anything that we're overestimating, in terms of North Korea capacities?

[01:03:22]

PRISCILLA MORIUCHI: Certainly. I think largely, when you look at North Korean cyber operations, they're far more agile, adaptive, innovative, right. They're more leading-edge, in terms of embracing technologies that are embraced by both larger consumer-based, and, for example, cyber criminals, right. So an example I like to use is that, if you talk to South Korean researchers in 2015, they were already seeing a North Korean developed crypto miner, right, which is a tool that corrupts someone else's machine and uses it to generate cryptocurrency, right, on South Korean computers, in 2015. I don't know how many of us were necessarily even aware of Bitcoin, right, and cryptocurrency as an entity.

[01:04:17]

And North Korean operators had already not only found it, right, but created a way to hijack someone else's machines and mine it, right. So it's an example, I think, and there are other examples that I can prove also, in which we really—because I think we were just stuck on this, this sort of isolated, sort of hermit regime idea, right, for a long time, that we missed this sort of agility and this adaptability and this kind of leading-edge, especially when it comes to the cyber operations side, of using easily available tools, like the internet for example, right, to do things—

to circumvent sanctions to do these things that we just hadn't really saw a need for, right, in the past.

[01:05:00]
So one, I think we're constantly underestimating North Korean cyber operations for their innovation, for their agility, for their ability to try a bunch of things and move on, right. So to me, if I look at, for example, the latest Google reporting about targeting security researchers, I see that as an experiment, right. Hey, it's relatively low-cost, right. We set up a website, right. We put together some blogs, some Twitter posts and LinkedIn profiles. They approach people. It didn't really work, but they didn't really lose a lot, right.

And not to degrade exploits. But if you're—if you're looking at it like a hierarchy of exploits, browser exploits are pretty low, right, there's a lot of browser exploits out there, relatively easy to develop. And so burning a Chrome exploit versus burning like an OS exploit, operating system exploit, is a much lower cost. So there's a willingness, in all cyber operations, there are operations that are going to work, and there are operations that are not going to work. And to me, that's that. So that's one.

[01:06:04]
And I think we always overestimate North Korea's capability or willingness to conduct a critical infrastructure attack, right. This kind of cyber—I hate to use that cyber Pearl Harbor—but scenario, in which, sure, we know North Korea has destructive and disruptive cyber capabilities. We understand that they have the intent and they have employed it, or at least they've tried to employ it in the past, right, North Korean operators have conducted operations against South Korean utility company, for example. They never got onto the control system networks, right, they were only able to reach the commercial networks. So we see that ability. We see the capability and the intent. I think we extrapolate, when we look at our own power grid.
And then, to me, that's sort of a step, that would be highly escalatory. And the one that's not North Koreans are largely not really willing to take minus, you know, these really extreme circumstances.

NICK SCHIFRIN: Jenny Jun, what do you think we overestimate and what do you think we underestimate?

[01:07:11]

JENNY JUN: So I think, I mostly agree with Priscilla on the underestimation point. Basically, North Korea is not bound by the same norms or limits as a lot of other actors are. And that frees up North Korea to experiment, try a bunch of different things, and be a bit more risk-accepting, when it comes to their operations. And we see, you know, things like the first destructive – the publicly attributed cyber attack on US soil was done by North Korea against Sony, not by Russia or China, which were believed to be, in terms of pure technical sophistication, maybe a little bit up there beyond North Korea.

And I think everyone, I think in the past, underestimated the lengths to which North Korea would go in cyber crime. And so we knew that individual North Korean hackers were moonlighting to generate some side revenue on the side, as far back as maybe 10 years ago. But even then, we didn't expect North Korea to literally go ahead [?] with cyber crime, to the extent that they're doing right now. So I would agree with Priscilla on that, on the underestimation part.

[01:08:27]

Overestimation, I think you know, relatively speaking, I think North Korea has poor OpSec. And they don't spend as much time defending their own networks, or their own tool sets. And that's, I think, a great opportunity for both the private sector and the government to leverage this fact, and to do more to expose North Korean TTPs, to get them to develop new tools faster, and get them on the defensive, and take down a lot of North Korea controlled infrastructure and things like that.

[01:09:03]

Also, another point, which is not necessarily about overestimation of capabilities, but something that I want to point out, is that because revenue from a cyber crime, or you know, information

that they're getting, with such as COVID vaccine research, through cyber operations, is becoming sort of a major, you know, source of income, as well as source of valuable information. This kind of increases their reliance on this channel being opened. And therefore, you know, in some ways, compared to what it was 10 years ago, it kind of erodes some of the asymmetric advantage that North Korea enjoyed in cyber space, ironically, because now they're reliant on this for revenue generation and for access to outside information. So this dependency means now North Korea has a little more to lose, compared to the US it's still way, way, way less, but has little more to lose from having these things disruptive.

NICK SCHIFRIN: Ben Buchanan, I wonder if I could ask you the same. What do we underestimate and overestimate? But that last point that Jenny Jun made is interesting. The conventional wisdom is, of course, the US has a lot more to lose. And so that's what enhances the risk of escalation to the US. But yeah, I guess I'll let you kind of describe, what do you think we've overestimated or underestimated, or take on Jenny's last point?

[01:10:27]

DR. BEN BUCHANAN: Happy to do all the above, or whatever you'd like. But I think the overestimating point, both my colleagues in the panel have done this well. So I'll give you something different. I think it is possible that we overestimate the risk of North Korean operations to the traditional banking sector. Which is to say, because the operation against the Bank of Bangladesh was so noteworthy, right, this aspiration to steal a billion dollars in hard currency, I think it's easy to overlook the fact that that was, in fact, a failure, that they walked away with substantially less than that.

And that, in a lot of other subsequent operations against conventional banks, they did not come close to getting that much money. In many cases, they weren't able to cash out in times. And in the Cosmos operation, they were able to withdraw a lot of money from ATMs, but it didn't reach the scale of the Bangladesh operation. And I do think we made a substantial number of improvements along the SWIFT interbank system and the like, such that I think we have probably gotten better at securing the traditional banking system.

[01:11:27]
On the flip side, I think we probably have not gotten much better, and we probably underestimate how much North Korea is stealing out of view against cryptocurrency exchanges and the like. And that's why the UN report that you mentioned at the top, Nick, is so significant. And I'm sure it's only continued since then. Because not to shill [?] for cryptocurrencies, but Bitcoin hit an all-time high today. I think it's clear that, you know, these currencies have an extraordinary amount of money, or a lot of value, rather, perceived or real. And that has benefited North Korea.

And there would not be the same kind of forensic investigation or after-action investigation or public reporting around North Korean operations against cryptocurrency exchanges. And my guess is, that those are quite easy to underestimate, and hard to find.

NICK SCHIFRIN: So are you agreeing with that? Does that mean that the challenge is even larger than we've admitted?

[01:12:24]
PRISCILLA MORIUCHI: Yeah, certainly. So I agree with Ben. I think SWIFT would, up and down, say that there was never a vulnerability in their system, right. And that it was always the access point, right. So it was always the machine that hosted the SWIFT instance, right, and which that was where the compromise took place. And all of the transactions were either duplicate, or fraudulent in some way, right.

So not to speak for SWIFT. But like, you know, I've been on—They will say it wasn't their software, right. And it's not their fault. And they're right. And I agree with Ben, you know, that for the most part, right, I think the SWIFT system and banks have done a good job at securing that particular system. There are many other smaller regional national level interbank transfer systems that we have seen North Korea looking at. For example, there's Mexican systems,

Chilean systems, right, that we've seen them poking around in. We believe that they probably have had some degree of success with.

[01:13:24]
So like for the financial industry at large, right, I think there are a lot of instruments in which North Korea can utilize to execute fraud. And again, which they're really creative about, right. So one of the things that we've sort of known about them, or came across my sort of internet optic, was this insurance fraud. I mean like if there is a fraud, a scheme, right, that can generate revenue, right, in some capacity, I think there's a likelihood we will see North Korean involvement. And I think part of that is because this is a diverse system, right, in which there's lots of different people and points and networks, right. They're all working together, but separate from each other for one goal, right. So we see that in networks of embassies and consulates. We have individuals overseas, right, whether they're hackers, or whether they're business people nominally, right. And we have government officials. And we have this movement. And they all kind of individual—work individually, but you know, collectively together.

[01:14:28]
And I do think the other side of that is, we tend to focus on the really high profile ops, the Bank of Bangladesh, right, the Cosmos Bank. But, for the most part, from what I have seen, from defector interviews, and the data that I have seen, the day-to-day of a North Korean cyber operator is a lot more—a lot less sexy, right. It's very mundane, right. It's about stealing snippets of code. It's about scamming people on online casinos and videogames. And it's this whole other sort of lower level of crime that, collectively, the information, security, and law enforcement community, we don't spend a lot of time in, with the vast majority of time, and even revenue.

[01:15:09]
I mean there are legitimate North Korean information technology companies out there. They don't present themselves as North Korea. But are developing websites, and running mail servers for corporate—for small companies around the globe. So there's this idea that, like, like oh, these are tied to your operations, right, are the ones that are important for North Korea. But I would

sort of argue the opposite, that it's the kind of day-to-day that we really don't spend a lot of time on, and that we're not seeing, right.

[01:15:40]

NICK SCHIFRIN: So we've got four minutes before starting Q and A. So just, I'll give you each two minutes, just Jenny and Ben, just to quickly kind of set the stage for the future, right. The Biden team is reviewing its strategy options. What should they be looking at? What should they be fearful of, in terms of cyber actions? And what should they be thinking about, in the days, weeks, and months ahead? And again, just take a couple minutes each to answer that. Jenny, you want to start?

[01:16:17]

JENNY JUN: Sure, I'll start. So I think first of all, if the Biden administration is looking to start talks in any way with the Kim Jung Un administration, any time in the next four years, I think it's absolutely crucial that cyber ends up in the agenda alongside the nuclear and missile problem. And I think, you know, cyber is important enough, I think, in the relationship between the two countries, that it merits a place, a firm place in the agenda.

I think another thing that the administration should do, I mean they already are looking at, to a certain extent. But in curbing, as Priscilla said, the curbing, the cashing out of their exploits. So just like what they did with the shipping networks before they were in cyber crime, you know, there could be more things that can be done in order to (a) track, you know, the movement of the money in different Bitcoin wallets, and also at the endpoint, at the cashing out stage, different things that the Biden administration can do, unilaterally, right, to make that as difficult as possible, and talk to cryptocurrency exchanges, to make sure that things like know your customer rules are in place. And more compliance measures to—it's going to be difficult, but to work with international partners to basically get that going, in order to make cyber crime a little bit more difficult than as it is right now.

NICK SCHIFRIN: And Ben Buchanan, just the last two minutes or so that we have before we open up to questions, what are you fearful of? What are you looking for, in terms of cyber capacity and cyber actions? And what should the Biden administration be looking for or thinking about, when it comes to that?

[01:18:14]

DR. BEN BUCHANAN: I think that the fear here, is pretty straightforward, which is, how have North Korean operations continued to grow? As Priscilla said, potentially more than any other foreign actor, that they evolve very quickly, very continuously, in their cyber operations. There's a variety of explanations for that. So how have they continued to evolve? How might they adapt their motivations? For example, would they—We had discussions several years ago, you know, what if they didn't want to steal money from international banking system, but wanted to corrupt the records and whatnot, and sort of caused some kind of damage to that system? All these things are plausible fears.

But more generally, I think the—as flattered as I am to join a great conference like this, and to talk about North Korean cyber operations, the other panels at a conference like this probably have more to say about the North Korean relationship with the US and what the Biden team is looking at. And I think that the challenge for the Biden team is going to be getting the various components of that relationship right, in conjunction with one another, in the same way that, with Iran, you know, Iranian cyber activity has continued. In many respects, it's gotten worse. But the Obama administration, on a separate track, was willing to compartmentalize and pursue a nuclear deal.

[01:19:28]

I don't know that a deal was plausible with North Korea the way it was with Iran. But it does seem to me, like the challenge for the Biden administration is going to be identifying where cyber ranks on their list of priorities in the North Korean relationship, what level of discomfort they can tolerate from North Korea n the cyber front, and how they're willing to trade the different parts of the relationship against one another. And, you know, as important as cyber

operations is to the three of us, maybe the four of us, it's only one part of a very complex relationship as the next couple days [01:19:58] pretty well.

[01:20:00]

NICK SCHIFRIN: Yeah, absolutely. All right. So we've got about a little – just under 30 minutes now. We've got about five or six of your questions. Keep them coming. All right. So let's start with a question from William for Priscilla Moriuchi. Several panelists mentioned that North Korean hackers operate, in some ways, like a criminal group. Do they work with foreign partners? And how do those foreign partners, if applicable, enhance North Korea capabilities?

[01:20:31]

PRISCILLA MORIUCHI: Sure. So the large answer is yes, right. We have fewer details on the ones and zeroes of the work with foreign partners. So let me break that up into two sort of bins. One, are the foreign partners nation-states? China, Russia, Iran? Largely, no. So this is a question that comes up when we sort of talk about cyber operations largely as, you know, nations, particularly China and Russia and Iran, like to issue these statements, right, where they're collaborating on information technology, or informationization, information security, right. But at the operational level that almost never includes tools and tactics, right. Pieces of malware, infrastructure, that stuff doesn't get shared, right.

[01:21:20]

So largely, when you look at North Korean tooling, and North Korean infrastructure, it's very unique from Chinese tooling and Chinese infrastructure, and Russian tooling, and Russian infrastructure, right. And they are not the same. So those are not the foreign partners that North Korea works with. The foreign partners that North Korea does work with, are criminal organizations, open source, malware providers, commercial entities.

[01:21:46]

So, for example, in North Korea, it's like you and I maybe, if we run our own website, right, we'll register the domain, right, for malicious website, with a corporation, with a company, right. They

will lift. They'll buy snippets, or lift snippets of code, for example, from open source, freely available projects, and insert them into their own tooling. We know that they've worked with criminal organizations, both in the real world, right, like Yakuza in Japan, right, to facilitate the distribution of the illegal drugs that they are producing. And, you know, in the sort of internet world, right, where they've purchased or leveraged tools, pieces of malware, for example, that they have bought from criminal groups.

[01:22:29]
So that distinction, I think, is important, from my perspective, is not this nation-state cooperation, and I don't even think there's enough focus there, really, to understand how integrated in the sort of cyber criminal underground North Korean operators really are. And if they were more focused, that we would have a better understanding of sort of what should we expect on kind of the revenue generation side, the ops side, right, if we really truly were looking.

NICK SCHIFRIN: Jenny Jun, do you want to take that question as well? And then the next one is directly directly to Ben Buchanan. So again, I'll just repeat it. North Korean hackers operate like a criminal group. Do they work with foreign partners? And how do those foreign partners, if at all, enhance North Korean capacity?

[01:23:13]
JENNY JUN: Right. I don't have too much to add, other than the same answer that Priscilla already gave. I think it's important to remember that, you know, that North Korean infrastructure and tools are not shared with that of Russia and that of China. I think, you know, I don't get this question as much anymore. But earlier, back five-six years ago, this was the question that I got a lot, right. Are the North Korean capabilities indigenous? Or are the Chinese government or the Russian government actively helping out, in terms of training, sharing tools, and things like that? And I think it's important to remember that.

NICK SCHIFRIN: So we have a question for Ben. In your book *The Hacker and the State* you explain how cyber operations can be "effective without being flashy." In the aftermath of major

recent cyber attacks, like Solar Winds, and sort of just parenthetical, I'm sure all of you guys know, but it's believed that Russian SVR has done an espionage campaign that we had never seen before, through the back end of Solar Winds, which most of government uses. So, in the aftermath of major recent cyber attacks, like Solar Winds, do you think North Korean cyber operations can continue to take place largely out of the public eye?

[01:24:35]

DR. BEN BUCHANAN: Yeah. I think North Korea can always court publicity should it choose to court publicity. And Sony is an example of it choosing to court publicity. But I think if North Korea wants to remain largely out of public view, I think they probably can. It doesn't mean they can evade the signals intelligence apparatus of the United States, or even many of the private companies. But I think their capacity to carry out campaigns, for example, again, it's cryptocurrency exchanges and the like, that really don't get a lot of media and public attention, doesn't seem to be diminished at all.

[01:25:08]

More generally, I think the Solar Winds case, and what a lot of North Korean operations show us, is that, again, these cyber operations are not great tools for signaling, or changing how the other side plays its hand at the international relations poker table. But they're very good tools for shaping, for stacking the deck, and the like. And I think that's really where North Korea, especially in its revenue generation operations, has put a lot of time and effort, is into shaping the international environment, in just a small way, to be a little bit more favorable to them, by bringing in money for the regime, even if that money is Bitcoin.

NICK SCHIFRIN: Priscilla, there's a question from Patricia for you. We have heard a lot in the news about the nuclear threat from North Korea. What's the main threat from North Korean hackers to middle class America? And if there is any, what can we do about it?

[01:26:00]

PRISCILLA MORIUCHI: Yes. So I've had to make this argument to the Senate Committee a while ago. I firmly believe that the people who bear the brunt from a cost perspective of North Korean cyber operations are your everyday average consumer, right. So when your financial institution, or the Fed, or the bank that you all could operate with, is the victim of a cyber crime, right, money is stolen from them, right, they are not the ones who bear the cost, right. It's the consumers. And it's the same for almost every other sort of aspect of cyber crime, right, that regular cyber criminals and North Korean actors are perpetrating.

[01:26:40]
When you go on gaming websites, right, the cost that you pay for games, for the accounts, for the armor and everything you buy, is reflective of the cost, not only it takes the company to develop that, but the cost, the fraud, right, around that ecosystem. And so it is the normal people of the world, right, not just the United States, who bear the cost, largely, of North Korean cyber operations. And not as much—granted, from my own classified perspective, we don't know as much about the traditional cyber espionage, nation-state to nation-state work. But it's largely regular consumers. So this is why normal people like us should really care about countering North Korean cyber operations, because we are the victims, and we're actually paying the cost.

NICK SCHIFRIN: Jenny Jun, Jacob Webber asks, is it possible sanctions are causing greater investment in cyber attacks? Meaning, our attempt to solve one problem is exacerbating another? And, therefore, could easing sanctions in the IT sector make it more profitable for North Korea to redeploy IT resources and the legitimate work, rather than hacking? And Ben, I'll give that to you as well.

[01:27:58]
JENNY JUN: Sure. So I think we could answer this in two separate questions, right. The first part is, I think, absolutely true. It's sort of like a wack-a-mole situation. Like when you first go after their ability to use international shipping networks, to generate revenue. And then we did that, and then so North Korea turned to cyber crime.

And some years down the road, we're going to crack down on that as well, by regulating cryptocurrency exchanges, making it hard for them to work with intermediaries, and sort of some of these mules on the ground to cash out. So that's going to cause North Korea to seek a different alternative revenue stream in one way or another, in some creative way that's unknown yet.

[01:28:47]
So I think that that's, in a way, in a way, true. The second part, I think, is more—I'm a little more pessimistic about that prospect, right. So could easing sanctions in the IT sector make it more profitable for North Korea to then do legitimate IT work for money rather than hacking? I think you just have to compare the money you can earn from doing sort of these one-off consultancies in IT, and then earning profits that way, versus stealing from entire cryptocurrency exchanges, or stealing from entire banks.

The reward on that operation is just so much greater than the other way. That's not to say that North Koreans are not working as legitimate IT workers. There are some who do that. It's just, you know, as a state enterprise, that's directly to coming directly from the top leadership, I'm a little more pessimistic that sanctions are going to lead them towards a legitimate [?] path.

NICK SCHIFRIN: Ben Buchanan, same question from Jacob Webber to you. Is it possible sanctions are causing greater investment in cyber attacks? And could easing sanctions in the IT sector make it more profitable for North Korea to redeploy IT resources into legitimate work, rather than hacking for profit?

[01:30:17]
DR. BEN BUCHANAN: I think Jenny has this one right. I think that there's no doubt North Korea has pursued historically a wide variety of different mechanisms for getting revenue. I'm sure many at this conference know that at least the reporting around North Korean counterfeiting schemes and the like, going back decades, a very aggressive international effort to crack down on the counterfeiting, that sort of preceded some of their efforts and shifting a cyber operation.

So one could imagine, if they had easier ways of getting revenue, they wouldn't be doing this. But I think I agree with Jenny, that they're unlikely to become the next cloud provider, or IT services company. And again, as I noted before, so much of the challenge in managing North Korean relationship is weighing these different parts of the relationship against one another. And I think this is the case where that applies. So I don't think you would see sanctions or impositions lifted on their cyber operations any time soon.

[01:31:20]

NICK SCHIFRIN: Priscilla Moriuchi, we have a question from TJ. I'm a graduate student from Yale University. Suppose we have another cyber attack from North Korea on a private entity, such as Apple, and private users are critically affected. Who would be liable? Users? Apple? US government? What is the current legal regime in the US to handle a situation, if there is one?

[01:31:47]

PRISCILLA MORIUCHI: Okay. I'm not a lawyer, so I won't – [laughter] Liability, I don't know, right. So there are so many large companies who have been victims of cyber attacks, in which their consumers have borne the brunt, in which the impact to their business model has been relatively small. I think—Well, let's just take Target for example. In 2015, right, Target was the victim of—or Target users, right, Target customers, through point of sale malware, right, on their credit card machines, Target users and customers were the victims of a huge cyber operation, right. And how many of us don't go to Target today, because of that, right? Minimal. Maybe there are some people. But most of us still go to Target.

[01:32:37]

So, from a—from a operational perspective, sort of like I was saying before, when there's an attack on a company, it's always the company's clients, customers, users, right, who bear the brunt and the impact of that operation. Liability is another thing, right. And I think this comes up sort of the kind of cyber insurance, and market, is that many companies are looking for attribution, because they want to be able to point and say, "We could never compete against a

government," for example, right. "How can we possibly defend ourselves when there are 30 Chinese military units, right, who are going to be targeting our industry and trying to rip us off, and get our data, right?" Or the same could be said about North Korea. So, I don't have a great answer on liability. But certainly, it's always the users, right, who bear the brunt.

[01:33:35]

NICK SCHIFRIN: Ariel Petrovix [?] asks, and I'll direct this to Jenny Jun and Ben Buchanan. Ariel Petrovix asked, what do you think it would take for North Korea to start using their capabilities for more explicitly disruptive purposes? They have used cyber crimes for financial gain, petty disruption. They could conceivably use the same capabilities for sowing problems for and within the international community. Do you have any predictions for the conditions under which the regime would decide to do that? Jenny, why don't you start.

[01:34:10]

JENNY JUN: Right. So I think the question is actually a little reversed, right. So we used to see a lot more disruptive actions in the early phases of their operation, beginning in 2009. I mean it was rudimentary, but it gradually sort of – the disruptiveness of it gradually built up, all the way up to, you know, Sony, basically, in 2014. And after that, we haven't really seen much disruptive/destructive operations coming out of North Korea as much as a lot of their efforts shifted to cyber crime.

So the question, then, is, will they ever go back to the way they used to do things in the early phases of their sort of operation? And I think, you know, that's kind of an open-ended question, right. I think the one thing that we should not do is to take the current lull in sort of disruptive/destructive operations, as sort of definitive evidence that deterrence is working against North Korea. And that some policy that the US [01:35:13] the international community did, you know, is actively deterring North Korea from launching something more disruptive/destructive, should it choose to. That may be the case, but it's hard to have concrete evidence to sort of to say, this is, you know, deterrence working, right.

[01:35:33]

So that possibility has to be always open. And I think, especially as the administration changes, especially the one in South Korea, possibly changes with the end of the Moon administration, we could see a change in the political climate that warrants such a disruptive/destructive provocation coming in the new political climate. We just don't know that. And so I think it's premature for us to say that this current model is a product of deterrence, or something like that.

NICK SCHIFRIN: Ben, what do you think about that?

[01:36:11]

DR. BEN BUCHANAN: I mentioned before, that I was very skeptical of the notion that cyber capabilities would be terribly useful for signaling. And I'm interested in this argument that they're more useful for shaping in international affairs. But as on many other things, the North Korean regime and I don't see it the same way. I think that there's no doubt that they have, in the past, turned to disruptive operations. I'm thinking here of the Sony operations, but certainly others, as a tool of signaling, as a tool of trying to make their point. I don't think they're terribly effective, in that they do a lot of damage, but they don't achieve the political end that North Korea wants. And in that case, it was the failure of those operations to stop the release of the interview.

[01:36:54]

But I do think that, as Jenny suggested, we will see a return to disruptive and destructive North Korean cyber operations when they feel the political climate warrants it. And I don't know if that's an increase in pressure from the Biden administration, from the South Korean government, some kind of military showdown or the like. It's hard to guess what the environment would be. But I'm sure the capabilities are still there. And I think North Korea has shown, in the past, that it, incorrectly in my view, views these operations as tools of signaling, that can help it achieve the political ends it desires. And even if it, once again, falls short of achieving those ends, it would still not change the fact that those operations are disruptive.

NICK SCHIFRIN: So we've got about 10 more minutes. There is a moderator's prerogative here, and the staff behind said moderator, have combined a couple of your questions. And so we can give you each a couple minutes to answer this, because I think it does—it might be a good way to end. And it'll give each of you a chance to say some closing thoughts. But also, you know, engage with the specifics here. So Priscilla, starting with you, what misperceptions exist in our analysis of North Korea's cyber? And is one of them a tendency to group disparate actors under the same umbrella? The question specifically asks about the Lazarus Group in regards to that.

[01:38:25]

PRISCILLA MORIUCHI: Yeah. I mean this could be a whole 'nother discussion about private sector attribution and naming of groups. So, okay. Largely, I think I've touched on what I think are some of the misperceptions. If I go back to the last question, actually, a little bit, I think it's important, going forward, to make a distinction between disruptive and destructive operations. So we certainly have seen North Korea deploy disruptive tools in more recent operations, specifically, again, in a bank operation, against a bank in Chile, for example, in which they deployed piece of ransomware, right, which is that it took all the network defenders and the attention, right, to try to solve that current crisis, right. It actually bricked some machines, right, some of these not usable anymore, as kind of a cover, a diversion, for actually stealing from people's accounts, right, so stealing from the bank, and executing banking transactions.

[01:39:25]

So that was very disruptive. And we have seen them deploy that particular technique in a number of cases, right. So one, yes, disruptive operations, I think, are ongoing, right. They don't raise to the level of national level, or healthcare, or systemic disruptions like WannaCry. But that's a different calculus than destructive.

And touching on Jenny's point earlier, I think one of the misperceptions, because North Korea was so disruptive and destructive in their cyber operations in the early 2000s, there's a lot of

misperception that there's a lot of political motivation, right, still, within North Korean cyber operations. And I think if there is a political motivation, much of it is targeted against South Korea, right. A lot of these financial attacks that are taking place, right, I think we think of them globally, right. But South Koreans are really at the pointy end of the spear. There are many operations that South Korean citizens and corporations have experienced, that we in the west, and the rest of the world, have never experienced.

[01:40:31]
Point of sale malware, for example, ATM malware, these revenue-generating operations that are on the smaller scale, and they were more targeted at South Korea. So one, right, misperceptions, I think, you know, we tend to—we don't think of North Korea as very adaptive, right, and all the other kind of descriptions that I was saying before. But also, we tend to over-prescribe, right, political kind of motivations to North Korea. And I forgot the second half of the question.

NICK SCHIFRIN: Do we group disparate actors under one umbrella? And he mentioned this Lazarus Group is the point. Is that one of the misperceptions?

[01:41:11]
PRISCILLA MORIUCHI: Okay. So yeah. So largely, there is not one umbrella term, if you're talking to private sector people. Most people in the private sector have adopted, like, HIDDEN COBRA, which is the FBI cover term for all North Korea state sponsors cyber operations. And we, like collectively lump a lot of things, operations, groups that we believe are affiliated with the RGB, the Reconnaissance General Bureau, or other North Korean intelligence and military apparatuses into this, because we don't know very much about these organizations, right.

Jenny can talk probably at length about the RGB, right, and whatnot. But comparatively little we really understand. So when it comes to private sector attribution, we can get to a point of knowledge, an IP address, a specific piece of malware, code snippets, infrastructure that's been reused, right, in these campaigns that we largely understand are North Korean state sponsored.

But we can never get you to a machine or an individual, right, or even a sub-unit of the RGB or the intelligence services or anything.

[01:42:16]
So largely, we're taking that a logical leap in the private sector, that because military operations, government, right, are so centralized and heavily controlled in North Korea, that there is not much moonlighting, or off-the-book cyber ops. They're gone. And that mostly, this is state-directed. And that does—that is, without a doubt, an intelligence gap in the private sector side, is that we just don't understand, and we don't have the data to tell you, if there is an active non-government, non-Kim regime supporting revenue generation going on, right, from the North Korean operators.

NICK SCHIFRIN: Jenny Jun, again, combining Brenda and Alex, what misperceptions exist in our analysis of North Korean cyber? And is one of them the tendency to group disparate actors under the same umbrella?

[01:43:10]
JENNY JUN: Yeah. So I don't have too much to add, other than what Priscilla already said. I think there is a tendency to kind of group the subunits of Lazarus Group, whether it's whether we call them ATP 37, ATP 38, you know, based on the targets that they're going after. And so some of them will be going after cyber crime. Or some of them will be doing sort of industrial espionage. Some of them will be targeting South Korea.

And I think, so I don't really know—Priscilla might know about this much more than I do. But it used to be the case that these sort of target-specific groups used to be a lot more pronounced. But I think, you know, going back a couple of years from now, I think that's starting to blur a little bit. And I also think it's true that these different units share a lot of their tools together, share a lot of their methods together.

[01:44:06]

And so, from that perspective, it might be a little outdated to group these behaviors according to what the targets are. But in another way, if you start grouping them, in terms of their code similarities, or in terms of the infrastructure that they shared, that could be also, you know, not a complete way of grouping these groups either. So I don't know what the answer is, or what the correct grouping methods should be. But in whichever way you slice and dice it, I think we are about to have some gaps. Because we don't, in the end, fully know, you know, how exactly these groups are organized under the larger sort of umbrella group of the RGB.

NICK SCHIFRIN: Ben Buchanan, you've been set up as the critic, but also the last word. So you get the last word. And again, this is the last question. But feel free to take it as you wish. What misperceptions exist in our analysis? And is one of them the tendency to group disparate actors?

[01:45:13]

DR. BEN BUCHANAN: So I have enjoyed the last sort of six minutes on this question, because this is exactly the kind of down in the weeds, cyber threat Intel, that I think Priscilla, Jenny, and I all love. I recognize that it might not be terribly interesting or comprehensible to folks who are Korea experts first. So I'll try to just take a step back and say, what is this question? Why is it important? And then Priscilla and Jenny are both right in their answers. What does it tell us about North Korea?

So, taking a step back away from North Korea, what the private sector often does, is they will come up with cover terms or code names to describe activity that they see. So Priscilla mentioned that a term you often hear associated as a general catch-all term for North Korea is HIDDEN COBRA. Jenny mentioned some subsets within that, of APT 37 and the like. And these are general terms that correspond to activity observed by the private sector, and their kind of forensic analysis.

[01:46:10]

And what's important here to recognize, is that breaking these sectors of activity, breaking these operations into clusters, is often important for doing attribution we talked about before. But the challenge, as well, is the linking those questions to some kind of political actor. And this is a struggle, in many cases, with a lot of actors. I think it's particularly a struggle with North Korea. And I think there was an assumption amongst people who were not terribly focused on North Korea, that hey, everything in North Korea had to just roll up into one well-organized group of cyber operators, one term. Often you'll hear the term, the Lazarus Group, to describe this.

[01:46:49]
And I think, as Priscilla and Jenny mentioned, that is no longer a great way to look at this. I think it is clear that North Korea does have different kinds of subunits, does have a different kind of organization that's far more disparate than just one single grouping would suggest, with different teams focused on different targets. In this respect, this actually tells us something about North Korea, that's interesting, even if you don't care about the mechanics of attributing cyber operations, which is that North Korea, as the theme of the panel has shown, has evolved to a reasonably sophisticated actor in this space, with different teams focused on different tasks, just in the same way that we see different Russian groups, even within the same military intelligence unit of the GRU, focused on different tasks.

[01:47:32]
And the difference with North Korea, as both Priscilla and Jenny said, is that we don't know a lot about how the mappings between our cover terms and the political or intelligence organization works. And there is that lack of knowledge there. But I think with this question and its answers get at, it's a great place to end for a panel like this, because it shows how far North Korea has come in competing in this new aspect of state craft and international relations.

NICK SCHIFRIN: Fantastic. And I couldn't agree more. That was a perfect last combined question So on behalf of everyone, Ben Buchanan, Priscilla Moriuchi, Jenny Jun, thank you so much for taking the time. And I see John just popped up. I guess back over to John Park.

[01:48:17]

DR. JOHN PARK: Thank you so much. That was a terrific job, in terms of framing and shaping this panel discussion. And big thanks to Ben and Jenny and Priscilla. A lot of food for thought. We have a number of students on the call, who are basically doing research in this area, either for thesis projects or dissertation projects. And so we will be reaching and following up after this.

I'd like to announce, we're going to take a quick break. When we return, we'll start Panel 2. We'll be examining the COVID-19 lessons from the Korean Peninsula at 5:50 PM. Thanks very much.

END OF PANEL 1

[BREAK]

PANEL 2: EXAMINING THE COVID-19 LESSONS FROM THE KOREAN PENINSULA

[side remarks]

[02:19:55]

DR. JOHN PARK: Welcome back. We'll soon start our Panel 2. Our second panel today examines the COVID-19 lessons from the Korean Peninsula. South Korea is one of a small group of countries that has largely been able to keep both its economy and society open, while dealing with the COVID-19 challenge. In contrast, North Korea sealed its border in January, 2020, and instituted a self-imposed quarantine. The economic impact from the self-imposed quarantine has been severe with this massive drop in trade with China.

We have an outstanding panel today to join us, to explore the respective set of COVID-19 lessons. Moderating Panel 2 is the award-winning correspondent Laura Bicker, who will also be introducing our experts. Laura has been a BBC correspondent for 20 years. She is currently based in Seoul, where she reports on both North and South Korea. Laura has produced award-

winning reports on sexual abuse in South Korea and most recently took part in a documentary on the country's COVID-19 response entitled “How to Fight Coronavirus.” Laura was previously North American correspondent for the BBC. She hails from Scotland, where she started her career, and covered the country's 2014 Referendum on Independence. We're excited to have you and our other experts onboard today. Over to you, Laura.

[02:21:07]

LAURA BICKER: Thank you very much. Really honored to be here, and honored to be joined by two panelists, two esteemed panelists. I think we'll start with Dr. Youngmee Jee. Now she is CEO of Institut Pasteur of Korea. She's a special advisor to the Prime Minister on health affairs, as well as the special representative of health and diplomacy of the Korea Foundation. She is a member of the WHO International Health Regulator, IHR Emergency Committee on COVID-19 Outbreak. She's also an advisor to the Global Center for Infectious Diseases at Seoul National University College of Medicine, and long-term expert advisor of the Korea Research Institute of Bioscience and Biotechnology. So we couldn't have someone more qualified to talk to us about the outbreak in South Korea.

[02:21:57]

And if you cover North Korea, Dr. Kee Park is the Director of the North Korea Program at the Korean American Medical Association. He leads the collaboration between the US and North Korean physicians. And since 2007, he's made 18 visits to the DPRK, most recently in May, 2018. And Dr. Park is also a consultant for the World Health Organization and serves on the WHO Expert Advisory Panel on Surgical Care and Anesthesia. So thank you very much. And welcome to you both. Thanks very much for speaking to us.

And good morning from Seoul, where the sun is rising. And happy afternoon where you are. And I think when it comes to the COVID-19 outbreak, this time last year, I was at a little known cruise ship called the Diamond Princess, where we were all slightly concerned about a COVID-19 outbreak on the cruise ship. Little did we know that things were going to spread as they have. And life has changed to the point where we're now all speaking on Zoom.

[02:22:59]
So, if we can first start off-- I mean I rushed back to South Korea, Dr. Jee, to cover the outbreak here. And one of the things that I noticed was how prepared South Korea was. Why was South Korea so prepared for a pandemic?

[02:23:16]
DR. YOUNGMEE JEE: Thank you, Laura. And first of all, I want to thank Dr. John Park for inviting me to the Harvard Korean Security Summit today. Back in 2015, during the MERS outbreak, actually, I was directly involved in the government outbreak response, especially with the WHO Korea Joint Mission on MERS Outbreak, and also technical collaboration with US CDC and the government of Kingdom of Saudi Arabia.

So, after the painful MERS outbreak in 2015, government made great efforts to strengthen the emergency response capacity, in terms of governance, testing and tracing. So government also made the amendment of national infectious disease law. So, to enable Korea CDC to collecting, and sharing the information on cases and suspected cases to each people's right to know.

[02:24:23]
And based on MERS experience, Korean government immediately knew that our reactions would be very critical for COVID-19 response. And government was really determined to take prompt actions right after the initial report from China to WHO, even before WHO declared a public health emergency of international concern on 30th of January, last year.

And especially extensive testing was possible, because of emergency use authorization, in collaboration with the Ministry of Drug and Food Safety and Korean pharmaceutical companies. And, on January 27th, when we had only four cases, Korea CDC organized the meeting with the pharmaceutical companies to produce diagnostic testing kits, and distributed nationwide, to speed up laboratory testing.

[02:25:24]
So I must say, the public/private partnership and transparency in risk communication, and with the media and public, was very important part of the response. And so through, as the [02:25:43] of testing, tracing treatment, and transparency, we were able to keep our society open, without complete lockdowns.

LAURA BICKER: I mean one of the things—So I've been to the testing lab, where they—I think you're even underrating your own achievements there, because it was within ten days, I think, that you had a test kit ready to manufacture and get out. So within ten days of January the 27th, you had the test kit ready. Isn't that right?

[02:26:16]
DR. YOUNGMEE JEE: That was the day we had a meeting. Then we did, about ten days, we were able to produce a kit and distribute to nationwide testing lab.

LAURA BICKER: One of the other features, obviously having been here, and being surprised, and I think it's probably my westerner outlook, was the text messages that we started to get. So as I was traveling to Daegu, my phone kept beeping all the time. And for those who are unaware, what they were doing in Korea was sending you out messages about where nearby cases were. Now that was allowed under the Infectious Diseases Act, as you said. But when it came to that, were there any issues and discussions over privacy, when it came to the use of that kind of technology?

[02:27:09]
DR. YOUNGMEE JEE: So I know there has been some criticism on the use of personal information. But I must say, the use of those advanced technologies such as [02:27:21] tracking system and mobile app for quarantine people and [02:27:26] system has been extremely useful, by improving efficiency and reducing time for investigation. So I think without those systems, without those technology, it was not possible for us to maintain current level. For instance, I

don't think it was possible that those systems was really helpful for us to really have such efficiency in our system. So do you want me to explain further on that?

[02:28:12]

LAURA BICKER: No, no, that's fine. [simultaneous conversation] about this privacy aspect. And it's difficult, I think, outside of Korea, for people. I mean certainly in some aspects, they called it draconian. And then, now I think when the western outbreak got so extreme, and people were subjected to lockdowns, I think things—the main shifted slightly. Is that your perception of it? Or perhaps in Korea there was no—there was certainly no huge—there was no outrage in Korea over the idea of these text messages, was there?

[02:28:59]

DR. YOUNGMEE JEE: So those systems was introduced because of people's need. People really wanted to know those information during the MERS outbreak. And governance was actually a bit late in releasing those information. And that was the reason there was a lot of transmission already happened before releasing those information. So government had to do something. So that's why government, it amended the law. And so those informations was based on people's need.

LAURA BICKER: Yeah. I mean MERS, in many ways, yeah, MERS in many ways was your learning curve. It allowed South Korea to see how bad this could possibly become, right?

[02:29:47]

DR. YOUNGMEE JEE: So, if I can just add a bit more. So while learning of the track people is actually publicized, current system could—not current system. Actually, when we first started the system, actually those systems might have some danger of allowing the other curious people to stigmatize those confirmed cases. So to address those concerns, with the information released to the public, maybe too specific. So Korea's CDC actually distributed guideline on local government to—on the time frame, which is maximum of 14 days, and discovered information

accessible by the public. So government actually made the full effort to find the deidentified method that enables the effective tracing while minimizing privacy issues.

[02:30:45]

LAURA BICKER: Thank you. So in contrast, when we had—we knew everything about South Korea's outbreak, they even produced a handbook for the rest of the world. One place that we knew nothing about, Dr. Kee Park, was North Korea. We knew that they closed their borders this time last year. What did you know about what was going on in North Korea? And how devastating, having been in hospitals, and having been—performed surgeries there, how devastating would an outbreak be in North Korea?

[02:31:17]

DR. KEE PARK: Right. That's a really good question. You're really asking about, what is the state of North Korea's healthcare system? And we try to unpack this for you a little bit. By the way, I was in Pyongyang in November of 2019, just a couple of months before they locked down. And that was my last trip.

So, you know, if you looked at a country like North Korea, it's a low-income country. And any low-income countries are going to have trade-offs on what interventions to provide, and what kind of things to invest in in the health system. So North Korea invests heavily into their public health system, right. High population value and low cost. So things like vaccinations, they do that incredibly well. They do that in conjunction with GAVI. And we can talk about the vaccine situation a little bit later. But it's a low-cost, highly effective, preventive—preventative strategy, very cost-effective. And they do that nationwide, 97-98 percent vaccination rates with children's vaccines. And this has been verified by UNICEF.

[02:32:15]

But then, if you look at things that are what we call curative services, right, we call it case management, treatment, healthcare, actual healthcare, this is where it's high-cost and then per case, right, so let's say cancer surgery, even treatment for COVID, these are highly infectious and

ICU ventilator care, very, very well extensive, high-tech care. They don't have as much in those things. It's a trade-off Now, so that's that whole idea of public intervention versus curative services, that dimension.

[02:32:51]
But then, you also have to look at the skill levels in North Korea. So you have some of the best hospitals, some of the best doctors. And they've been trained from all over the world. And they know how to do just about everything, heart—They do open heart surgery, brain tumor surgery. I've seen these myself. And they do a very good job of it. The problem is, those kind of services cannot be available for everyone, everywhere. And this is a trade-off that they have. It's typically centralized into Pyongyang.

So that's that rural-urban dimension, right. So the healthcare is there. But it's not evenly distributed. So let's say you introduce a disease like COVID into North Korea. And if you have a massive outbreak, the system cannot handle the curative aspects, the case management aspects of it. There's not enough ICU beds.

[02:33:42]
For instance, I worked at the Pyongyang Medical College, which is their premiere teaching hospital. It's the main teaching hospital for the entire country. I would imagine they had no more than two dozen ventilators for the whole hospital. This is a major hospital in Pyongyang. So you could sort of do the extrapolation of the provisional hospitals, and they just don't have those capacities. So they're smart, because they recognize their weakness, and they try to prevent it. And I think they did a very good job of preventing the virus from coming in.

LAURA BICKER: Are you aware of cases within North Korea? Or is there any information that you've had about any outbreaks within parts of North Korea?

[02:34:23]

DR. KEE PARK: Right. So this is a point of contention, right. We hear this all the time. The North Korea's official position is that they have not detected any cases of COVID-19 in the country, and that there's a lot of prevailing thoughts saying that that may not be true. I tend to think that they did. They are able to keep the virus out. Remember, they locked down. The time that it took the South Koreans to develop their test kits, North Korea was figuring out how to prevent the virus from coming in, within days of understanding there's a virus outbreak in Wuhan, they closed the borders. Tourism, trade, everything, within days. And at the end of January, everything was closed.

[02:35:04]
And, you know, do you remember the video from CNN, it's a promotional video. And there's a footage where Sanjay Gupta is asking President Trump, then-President Trump, you know, "Are you ready for this? Are you concerned about this new virus?" And Trump goes, very confidently, "No, because we're ready for it." And that's exactly what he says. [laughter] Well, we weren't ready for it. [laughter] We did not take the virus seriously, and that we would pay a deep price for that. We're going to reach a half a million deaths pretty soon in the US.

We didn't take it too seriously in this country. But in North Korea, they took it very seriously. And in some ways, maybe even too seriously, because they have now considered this a matter of national survival and threat. And there's some implications of them taking it too seriously. But we can talk about that later.

[02:35:53]
LAURA BICKER: We'll get onto it. I think one of the key things has been, really, how seriously each country took the virus. And we had that North Korea took it seriously, South Korea had already had experience with MERS. And I mean, you talk about the ICU capacity, and the ventilator capacity. In terms of kind of rural—you said extrapolated out, what is it like in the kind of more rural areas, especially, perhaps, around more vulnerable border areas, where it could have come from via smugglers, for instance, along the border with China? Is there any

indication that they would have been able to cope if it was—if the virus was able to kind of make it through the blockade that they put in place?

[02:36:36]

DR. KEE PARK: So let me walk you through their testing protocol and capacity. As of today, I think they have about between 15 to 20 machines, the gold standard machines. And I think they may be spread out, now, around the country. About as of last summer, I think they only had one machine in Pyongyang. So their testing capacity is scaling up. But certainly not a nationwide, you know, test on demand, or test everyone like in some parts of China. They don't have that.

But what they do is they detect patients, people with symptoms that are suggestive of COVID. This is just respiratory illness, the coughing, sneezing, some fevers. And they immediately quarantine those people. And then, when able, they do the test. And they repeat the test first. And then ten days later, while they're in quarantine, they repeat the test. If that's negative, they'll release you from quarantine.

[02:37:24]

They did that for a while when the testing machines, they were able to get a hold of more machines, they actually did what they called enhanced surveillance. And I think what that meant was contacts of people with, let's say, cargo from overseas, you know, foreigners, any people that had potential contact, they would quarantine and test these people.

What they were finding is, none of these tests are coming back positive. So they have a very thorough testing capacities of what—One possibility, and I'll give you this, is that in a remote province somewhere, there's some kind of a virus, a viral infection. They quarantine that patient. And then, wait and see if they get better, and then release them. But they don't have the testing capacity to confirm, right. I think in that situation, it's possible that it could be COVID-19, but no one would really know.

LAURA BICKER: Right. I mean in terms of the kind of speed, I have many of us here sitting in the South were extremely worried about the situation in North Korea. Meanwhile, in South Korea, they kept their borders open. But they did so with very interesting quarantine procedures, having been through it serious times. Dr. Jee, can you talk us through, when did they decide to kind of close the border? And how they managed to kind of keep people flowing through without causing it completely here in South Korea?

[02:38:48]

DR. YOUNGMEE JEE: So as you know, we have never completely closed the border. We introduced patient entry procedures. So that I think introduced from—For China, it was just from the beginning. For many, for other countries, I think early April, we have introduced special entry procedures. So all the people need to be tested at entry. Actually, right after entry, or within three days, while they are quarantined. And then, for releasing, at the beginning, we have done another testing. But we changed the policy, actually, later. So, unless they develop symptoms, we have not tested. But we realized, actually, it would be better to test again up to 14 days. So I think recently, also, added again the testing after two weeks.

LAURA BICKER: Yeah, I've been through it twice. [laughter] I feel like I've been tested quite a lot. But compared to my colleagues in China, it's nothing. But yeah. I mean the procedure is still quite strict. And now you've had to step it up, because of the possibility of variants. How concerned are you by kind of people coming in with this variant? Do you think the quarantine measures this kind of 14 days in quarantine and the testing measures will manage to keep variants at bay?

[02:40:25]

DR. YOUNGMEE JEE: Well, I know the procedure for the sequencing, for all incoming travelers. But all incoming travelers, once they come from, we go to sequencing procedure. We cannot really do sequencing for all compound [?] cases, but we make sure that we do sequencing for all positive cases, from internal travelers. And also, when we have outbreak, we select some initial samples of sequencing.

But we cannot say 100 percent, of course. But, because recently, we have discovered internal—the cases that was not from incoming travelers, we also detected the variant from the people without travelers. So we do know that the variant can spread. But we are doing our best, because we have introduced, as you probably know, the testing of the people without symptom, if they wanted to be tested, they can be tested any time, anywhere.

[02:41:43]
So with that, possibly we can minimize the spread, spread of the virus. But the vaccination is the key, of course. The vaccination will start, start at the end of February. So once we have that vaccination roll-out, hopefully we can keep our level of the instance low, because the [audio breakup] [02:42:20] is going down, now. So hopefully that won't go up again. But we just have to cross our fingers.

LAURA BICKER: So let's talk about the vaccination. So I asked, and many people just said I was being a bit facetious I asked President Moon at the press conference if he regretted not buying up the—procuring the vaccines earlier, and rolling out the vaccine earlier here in South Korea. Now the reason I asked this question is because, having seen the start of this pandemic, and as you mentioned, how quickly things were done here, I mean one scientist there at the KDCA said, it's a "*bali bali*" gene in South Korea. Everything is "*bali bali*," which means, for those of you who don't know, very quickly, quick, quick.

[02:43:10]
But it seems that, when it comes to the vaccine, it's "*cheoncheonhi, cheoncheonhi*." It's slowly, slowly. Is there a reason why, certainly in South Korea, there would—you know, you're rolling out the vaccine a little bit more conservatively than, perhaps, the west? I realize that the west has a reason to get the vaccine out quickly. But are you—is there a reason why, scientifically, you're thinking, "Let's take it a little more slowly"?

[02:43:40]

DR. YOUNGMEE JEE: So there are the advisory committee for the government, for the vaccine. So I think during the year, until August and September, we were doing relatively okay with it. At that time, we had the second wave. But there was advice from the expertise that we have to really see the safety and efficacy of the vaccine first. So we—I think government wanted to wait a little bit until the vaccines are really used in other countries, and see how it goes. But still, there was, I think, a negotiation with those vaccines companies in addition to COVAX mechanism.

[02:44:30]
But there was a certain stage that many advisors started to argue with the speed of the vaccine procurement. So certainly, government tried to do it quickly, *bali bali.* So now, I think that we have secured the amount of vaccines that will be enough to cover the whole population, even more than the population now. So we are, I think, doing okay, considering—considering we have started quite late. So we just hope that we can start at the end of February, I think is 24th of February.

But first—first vaccination we thought was with Pfizer, very small amount only, 60,000. But after that, we will be using AstraZeneca. But a lot of the policies in other countries, including Europe, regarding the use of AstraZeneca in old age group, we are still discussing. We have not really decided what we have to do with the AstraZeneca vaccine for old age group. That, I think, will be decided very, very soon. So once we have the redesign, we can all start—we can start vaccinating for the old age group. But that will be decided probably a few days later.

[02:46:19]
LAURA BICKER: Yeah, fascinating how now, it looks as if that the aim is to get herd immunity by November. Is that correct?

DR. YOUNGMEE JEE: Yes, yes. [simultaneous conversation]

LAURA BICKER: Let's keep our fingers crossed. As someone whose mother has been vaccinated, can I tell you, it is a wonderful feeling to know that your relatives are protected, especially at—My mom's in the UK. And in terms—Actually, we just had a question on vaccination, actually, while I've got you here. Is there evidence of anti-vaccination sentiment among Koreans? Says Alicia Nelson. So you're well placed to answer that right now.

[02:47:00]

DR. YOUNGMEE JEE: Well, I think generally, the anti-vaccination movement is not that strong in Korea. But we have heard that different efficacy of the vaccines among different vaccines. So some people think that we have to—we can choose. We hope that we can choose vaccines, which vaccine we will be vaccinated. But that's not going to be possible. We just have to be vaccinated using that designated—the brand of vaccines.

So some people are concerned about which vaccine we will be using for vaccinating them. So the problem is if they don't want that vaccine, they have to wait for a long time. So experts, including myself, actually, we think they'll still able to be better, even though they don't want that specific vaccine, it will be better to be vaccinated as early as possible, even though it has a little less efficacy.

[02:48:13]

LAURA BICKER: Because the flu vaccine [?] usually, and other vaccines usually have quite a good uptake in South Korea. But at the end, I think to explain, Alicia, there was a bit of a mishap at the end of 2020, where some flu vaccine was left out, and there was worry about the kind of batch contamination. And that's kind of increased a little bit of what we call anti-vax sentiment. But ordinarily, South Koreans are not—don't have that kind of anti-vaccination sentiment. Am I right?

DR. YOUNGMEE JEE: Yeah, that's correct, yeah.

[02:48:51]

LAURA BICKER: It's not the same in my country, the UK, and in the US. There are many websites which have kind of anti-vax sentiment. There's not the same here in South Korea. All fingers crossed that that goes well. And I think we're all trying to figure out what's going on in North Korea, Kee Park, when it comes to—when it comes to the vaccine. Do they have enough vaccine procured? Or do we know—what do we know about what they've got so far?

[02:49:18]
DR. KEE PARK: Right. So do you want to talk about whether they can develop their own vaccines now or later?

LAURA BICKER: Let's do that now, because—So I've read the reports. I've have anonymous sources telling me that they've developed their own vaccine Is that possibility or not?

[02:49:36]
DR. KEE PARK: So, yeah, yeah, it is possible. They do have the technical know-how to splice genes, and also to insert it into, let's say, bacteria for mass-produced hormones. I know that they have [02:49:48] that kind of capability. And then, you know, the genetic sequence for the entire SARS-CoV-2 virus is open source. So you can, you know, theoretically put it together and figure out which ones will spike protein and design it.

So they can probably do it. And they might even be able to inject it in some subjects, and even test the immune response by measuring the antibodies. But what they won't be able to do is to do a large-scale efficacy testing, right, because they don't have any, you know, regular infections happening. So when you want to test a vaccine, you got to put it out into the public, where there's actually a decent rate of COVID happening, like US, right, or South Africa. So that's the main issue for North Korea. They won't be able to do the study.

[02:50:40]
So now, let's talk about why the North Korea really needs the vaccine. You know, we talked a little bit earlier—and John referred to it—the economic implications of the border closure. You

know, they went into a bubble, right. So trade with China has almost completely come to a standstill. There are a massive backlog of containers at the ports of entry, humanitarian aid has come to almost a complete stop. There's no rotation of international staff. The country is in a complete lock-down

[02:51:11]
And there are implications to that. So when you have—you will have degradation of healthcare system, increasing poverty, decreasing health-seeking behavior, loss of humanitarian assistance, all these things actually cause significant human costs, right. Not COVID directly, but in a secondary results of these measures. They need a path to reopen, that's for sure. And you know, they see this as a threat to national security. And they really have to have almost—you know, they call it security guarantees, right. What would make them feel secure? It's the vaccine. So they're very keen on it.

There are a couple of ways for them to acquire it. We talked about making their own. But the other one is to get it from the outside. So let's just talk about the COVAX facility, because we know that they have—they went ahead and applied for the allotment. And it's the COVAX AMC, the Advanced Market Commitment. This is the group of about 90 countries that are low-income. They're eligible for free vaccines through donors. And they've just been notified, actually, of allotment of two million doses that will probably come towards the end of this month, actually, right.

[02:52:23]
But there are a lot of caveats. For instance, the AstraZeneca vaccine, which is the one they—you know, they will likely get, they have indicated that they will get, has not been approved by WHO yet. You know, it's under review right now. It probably will be. But, you know, what are the conditions? Especially, what Youngmee talked about, the old age group, and that kind of stuff.

And then also, in terms of vaccine choices, countries like North Korea are limited. And so we can say, we want Pfizer. Great. You know, when I say “we,” South Korea can have Pfizer

because they have ultra cold temperature storage facilities and transportation facilities. Most developing countries don't have this kind of network of ultra cold freezers to be able to safely transport without damaging the vaccine, if you will, with things like Pfizer, maybe even Moderna.

[02:53:12]
So AstraZeneca requires just a standard refrigeration type of temperatures, two to eight degrees Celsius. And they have extensive experience with this type of vaccine, you know, the vaccines I talked about before for children, those are all protected in that cold temperature ranges. So that AstraZeneca makes perfect sense to them for many reasons. And so they have applied for it. And now they have to get their deployment and vaccination plan approved by the WHO. And once it's approved, and it's also the AstraZeneca vaccine is approved by the WHO, as for emergency use listing, then they can start getting their first allotment, which is about two million doses, about three to four percent of their population.

LAURA BICKER: I mean will people have to go into the country for this vaccination program? Or can they do it themselves? Because obviously, I know that a number of NGOs have had to leave the country. Very few workers are left. A lot of the foreign diplomats have also left. So in terms of getting kind of people in to help with this vaccination program, is that going to be a possibility? Or even monitor the vaccination program? Is that something that you're concerned about or will be watching for?

[02:54:30]
DR. KEE PARK: No, this is actually a crucial point that you make, Laura. Everybody is concerned that international staff, humanitarian staff are not able to go back in. And what would be sort of the turning point, the tipping point, where North Korea will say, “You know what? We will actually consider bringing international staff.” And I think it's in the vaccines. So, you know, the vaccine program, the COVAX AMC program is donor-supported. It's not money that's in the bank account somewhere. Donor countries put in money, including South Korea. And there's a

pot of money. And they purchase these vaccines at a discounted rate, and then distribute it in an equitable fashion, which I think is wonderful. I think we need to do more of this.

[02:55:12]
But donors have certain expectations, right. Transparency and accountability. They want to make sure that the money that they have donated goes to do the job that it was intended to do. And every recipient country knows this. This is not just unique to North Korea. Every country knows that there has to be a monetary and evaluation component to their deployment plan.

[02:55:33]
So I think this is an opportunity to really nudge North Korean officials to say, "Can we start talk about how to get safely, right, keeping our population safe, but still, at the same time, bring in international staff?"

LAURA BICKER: Well fingers crossed that people do start to get it. And I think there's genuine concern amongst the diplomat side, and how foreigners will be received. Because certainly, I think there was a little bit of—tension is the wrong word, but certainly made you feel unwelcome as time went on. So perhaps maybe you think aid workers will be able to go back in and be well received? Or do you think North Korean authorities might continue to look at them with caution?

[02:56:20]
DR. KEE PARK: You know, this is not something they will open—you know, with open arms, and say, "Please come." Well, it's not because they don't want to be monitored, I think that's maybe one part of it. But the other one is they are just really afraid of having international staff come in. Foreigners are seen as, you know, a way to bring in virus, you know, letters that go in, packages, you know, for them, it's like it's contaminated.

Snow, they talked about snow. And anything that washes up on a beach. So any foreign element, for them, is a threat and a way of introducing virus into the country. So really, we have to figure out a way to make them feel safe, whatever it takes. And I think we can do that.

[02:57:01]

LAURA BICKER: Okay. And one of the things I wanted to talk about, with regards to—and perhaps, I've been told this is a cultural thing. But I'm not sure that it is. Mask-wearing. It was never an issue in this part of the world. I arrived back into South Korea, and I've been on holiday. Remember when we could have holidays? I've been on holiday with my family. I arrived back in South Korea in January, 2020. It seems like a lifetime ago. And everybody was already wearing masks, right back at that point. Why do you think mask-wearing has become quite easy to do here, and yet not completely a problem? Even in North Korea we've seen them wearing masks, although the latest party Congress, there was no mask. Why do you think mask-wearing is such an issue? Well not an issue here, and an issue elsewhere? Dr. Youngmee, if you can answer that one.

[02:58:03]

DR. YOUNGMEE JEE: Yes, mask-wearing has been very common practice in South Korea, because of fine dust problem during the last few years. And when we first heard the news of this new coronavirus, government actually advised the public to wear the mask, because it is one easy way of protecting people from respiratory diseases in general. So people followed that guideline without big issues.

But at the beginning, actually, we thought that some experts were saying, “Do we really need these?” And at that time, WHO was not really advising to wear mask. And that advice came quite late. But we are doing this just because government advised. And this is some are protecting respiratory disease anyway. So I think that just came natural. [laughter] Having the habit of wearing the mask last two and a half years, because of some other reason, the fine dust, from China, half—maybe half from South Korea as well. But later, actually, we realized that was

very effective way to feel very lucky, actually. We were doing this from the beginning. So we are doing right practice.

[02:59:33]

LAURA BICKER: Yeah. So when I was in Daegu, where for those who don't know, that was kind of the initial center of the virus in South Korea, which was part of an outbreak amongst the Shincheonji Church of Jesus, which is a kind of sect. And it spread throughout the country. So we were in Daegu. And outside of Daegu were these massive queues of people. I said, "What are they queuing for?" They were queuing for masks.

[02:59:59]

But in the UK or the US, they were queuing for toilet paper. So, you know, these-- [laughter] The difference in life. But even within the BBC, for instance, we put out—because we do a lot of kind of public service broadcasting, we put out a broadcast where the doctor was saying, you know, "It may help. But we need to make sure that masks are saved for those who need them," et cetera. Did South Korea have enough masks for people? And remind us how they managed to make sure that people had the masks that they needed.

[03:00:33]

DR. YOUNGMEE JEE: So we actually can produce masks. But at the beginning, it was not like now. So because of people really trying to buy a lot of masks, so it was not enough at the beginning. That's why we had to make such a big long queue, so government also had to introduce mask app to wear the masks as sold in drug stores. So we had the certain period that the mask was not really, not enough. But I think we asked those small producers to produce masks immediately. Then, after certain period, there was no problem. We now have no issue at all. But at the beginning, at the beginning, we had [audio breakup] [03:01:31]. But I think still, mostly we have probably enough masks for the medical people. [simultaneous conversation]

LAURA BICKER: And one of the other points that really astonished people initially was, I did a report from Seoul National University ICU where the nurses were in full PPE. And it looked

like a space suit. Now we've got used to seeing this on our screens. But at the time, you know, I don't think many people had seen anything like it. And I was inundated with messages. We had—I had UK newspapers phoning me up, going, "What is this?" And they put it all over their center pages. But here, you did have enough PPE for staff. Why did you have that kind of amount of PPE? Was it just good planning?

[03:02:24]

DR. YOUNGMEE JEE: Yes, of course. Yeah. That came after the MERS outbreak. So we had to make that preparation, that was first thing you have to do. So PPE is the first step. So after MERS, we were prepared for those PPE and the ICU. But still, I think ICU, we did not really have enough number. So government is actually planning to have more ICUs. Even PPE, we want to have more, I think. But compared with other countries, I think we were relatively prepared because of MERS outbreak. We had prepared at least for certain level level.

[03:03:13]

LAURA BICKER: At Nokia [?] I talked to someone, diplomatic sources, who had left North Korea last year in the summer. And they said that there was PPE held up at the border. And they weren't sure how North Koreans managed to get masks. What do you know about the mask supply there? And were people kind of quite happy to wear masks in North Korea also?

[03:03:38]

DR. KEE PARK: My understanding is that they're able to actually manufacture their own masks. They're not very difficult to make. So I think that's one. And I think the Chinese have been sending in a lot of supplies that's maybe not getting reported official records. But, as talking about the behavior part, you look at Asian—and I don't want to generalize, because there's some exceptions—But people typically like to conform. They don't want to stand out, you know. And so if this is sort of a social norm, of everybody wearing masks, they're going to wear it, you know.

And then, on top of that, when you have a strong governance, you know. So I lived in Cambodia for a few years. And I remember in Vietnam, when they passed mandatory helmet laws, right, for people who were riding motorcycles. Overnight, everybody was wearing helmets. This is in Vietnam. So Cambodia, a few years later, did the same thing, and it just wasn't the same. [laughter] The helmet wear usage rate is like 20-30 percent. There was a little uptick, it went back down again.

[03:04:37]
Now it just speaks to the relationship between the government and the people, as far as governance, the authority to impose certain things. And, of course, I think you know in North Korea, that whole system is very strong. And for those reasons, I think they have a very high mask-wearing rate.

[03:04:55]
I want to mention one more thing about masks. In North Korea, it's so predictable that the mask-wearing is expected, that when they are not wearing a mask, I think it's noteworthy. And I'll give you an example So they're in the last party Congress, eighth party Congress. You know, it was notable that the people inside were not wearing masks. This was like six-seven thousand people indoors, with you know, their leadership sitting right in front. That is not a propaganda piece. To me, that's, you know--

So I think this is an indication of the level of confidence that the government has enabled to control the virus from coming in through its borders. And that you can see that by saying, “Hey, we're not going to wear masks today.”

[03:05:39]
LAURA BICKER: In terms of the kind of efficacy of mask-wearing in North Korea, do you think that will continue? Is that a way of perhaps protecting the country while bringing in foreigners, trying to say, “Well, you can keep your mask on. You can keep social distancing.” Because we talked earlier about allowing foreigners into the country, and how nervous they'll be

about that. Is it perhaps a way of educating the mask-wearing, social distancing, will enable them to stay safe, even if the foreigner poses no threat, but it's a way of kind of continuing that?

[03:06:13]

DR. KEE PARK: I think they'll be very, very cautious on rolling back any one of these measures, right. They are very risk-averse when it comes to the virus. So I think the mask-wearing will continue, even when the country is vaccinated, let's say 70, 80, 90 percent herd immunity, remember the AstraZeneca vaccine, which is the one they're going to go with, may not be effective on the South African variant, you know, especially for the mild to moderate disease. So there are these variants coming through.

[03:06:43]

So I think it's a tool. So it's a key pillar in fighting against this COVID pandemic. But it's not a silver bullet. And North Korea will be very measured and calibrate their responses very carefully. And they'll err on the side of being overly cautious.

LAURA BICKER: Youngmee, if I can ask you, in terms—and I'll ask you both this. In terms of the kind of lingering effect of COVID-19 on the Peninsula, I mean we've talked about how they've both—both North and South Korea have managed to kind of battle the effects of COVID. But we are far from out of this pandemic. It could be many months, if not perhaps years to come, where we're battling different variants of COVID-19. In terms of South Korea, what are the preparations underway for the long-term and lingering effects of COVID-19? And how do you think South Korea will cope with that?

[03:07:41]

DR. YOUNGMEE JEE: So many people think that COVID-19 pandemic changed the international order of countries. That South Korea was the first country outside China with a big outbreak of COVID-19 during February to March. But with the prompt response, as I mentioned, based on MERS experience, we were considered as one of the countries with a relatively successful [?] responded to COVID-19.

But I think, in terms of [03:08:15] infectious disease research and development, I think South Korea is not yet well prepared. And we still need the long vision and strategy and better global engagement. So here I want to actually emphasize the role of close partnership with global infectious disease are in the network. And this network include WHO [03:08:39] developing team, which played a key coordinator role, and also Global Health [?] Gates Foundation, Wellcome Trust, and US NIH and many other partners and scientists, they all really facilitate COVID-19 research during the early phase with this crisis.

[03:09:00]
And now, this R&D network is also preparing for next pandemic caused by disease X, which is unknown yet. And I think Korea need to also participate in this kind of global engagement better. So R&D, we have been putting a lot of money. But I think we need to be more engaged with global community. And need more long-term, long-term planning and strategy, because the vaccine development in Korea is not really like COVID-19 response.

So we are still—we have several candidate in development. But they are not yet like Phase III, only in Phase I. So we hope that we can have better strategy for the R&D, and also hope that those countries with the technology can transfer the technology to low and middle income countries, of course Korea. But maybe to other countries, like India and some other countries with a vaccine development capacity. If technology can be transferred quickly, that that, I think, it really needed for the global, global R&D network. And yeah.

[03:10:46]
LAURA BICKER: Let me put you on the spot here, and I'm going to put you on the spot here. And you can always feel free—I'm used to people telling me, “I can't answer that one.” But how long do you think we are going to be dealing with COVID-19? Are we looking months or years? Do you think it all depends on the vaccines? I mean how long do you think here in South Korea, and elsewhere, we're going to be kind of battling the coronavirus?

[03:11:14]

DR. YOUNGMEE JEE: So I think there will be acute phase, acute phase we want to finish as soon as possible So once we have herd immunity, then I think we could probably finish acute phase. Hopefully that can happen by the end of this year, before winter season start. But still, we will have this COVID-19 together with us for quite some time. Maybe for a long time. Because, as we know, we have variant. And it will probably come back, maybe it can be like endemic diseases like other coronavirus. So maybe we need vaccination, like a flu vaccination, and as many people say.

[03:12:04]

So our target is, I think, at least we can finish this acute phase as early as possible. But for that, we of course need the vaccination for global community. So those mechanisms for the vaccine distribution, the equity that people always say that. But that can probably happen like at least beyond 2022, not this year. This year is not possible. But somehow, I think that the COVAX is targeting 2021. But that's only maybe 20 percent of the whole population. So for the herd immunity for the global population, that it will take time. Probably only time will be '22, maybe beyond. [laughter] So even--

[03:13:06]

LAURA BICKER: Okay, I'm trying not to get too depressed here. [laughter] At least we have a vaccine, right? I mean as someone who lives in different parts of the world from our family and our loved ones, it's always that kind of—And I know millions of others around the world are the same. I think most of us are just hoping one day to see our families, which will be nice. But yeah, I see we're going to be dealing with it for some time to come. And Kee, when it comes to the lingering effects of COVID-19 in North Korea, it's less of the effects of the virus and more the effects of the blockades. Am I right in saying that?

[03:13:44]

DR. KEE PARK: Yeah. So in some ways, it's ironic, the sanctions that they have been subject to for years, I think may have actually given them an edge in a way, by going into a bubble. For

them, it's not a big deal, you know. It doesn't seem to be as big deal as we thought it was going to be. They seem to be like not in a hurry to reopen, for instance. And I think they won't reopen fully until the global pandemic has subsided. And I mean, Youngmee is *the* expert on this. I'm a surgeon. But I will only add to her prediction.

You know, these low and middle-income countries, we all had to be vaccinated. For the global pandemic to sort of come down, we really have to vaccinate everyone. And so it's in everyone's interest, the high-income countries, to make sure that, you know, as quickly as possible, to vaccinate everyone. Yeah. And that includes North Korea.

[03:14:44]

LAURA BICKER: And I realize, in your past as a surgeon, and kind of medical expert. But in terms of the blockade in North Korea, I think many of us are worried about how that's affecting supplies getting in, not just medical supplies. I mean you were there in November before the pandemic, and we're here over a year on. Are you concerned about the lack of supplies that have been getting into the country over that time, and what effect, as someone who knows the country, what effect do you think that could have on North Korea, long-term?

[03:15:19]

DR. KEE PARK: So, from a medical standpoint, you know, I remember in November, some of the medical equipment required parts, replacement parts. And they couldn't get it, because of the sanctions, right. There's no mechanism for a North Korea hospital to order parts from a company in Germany. At least they can't transfer funds, and the companies won't sell because of the sanctions, all kinds of issues. So they have to go through some of the gray market.

Anyway, the medical equipment was already in a very questionable situation then. And now, with the blockade, I can't imagine that they will be able to resurrect any one of these machines. What they're doing, instead though, is trying to develop domestic—you know, engineer and manufacture their own machines within, you know. It's just their [03:16:04] philosophy. And I've

seen them do that with ultrasound machines. They've developed their own CT scanner. So they're doing the best they can with what they have.

[03:16:12]
But I am worried. You know, the health system is going to really suffer. The delivery of essential health services will suffer. Tuberculosis, you know, that's a big, big, big burden in North Korea. How will we get all the test, the testing, and the medications, and continue to deliver the drugs that they need, these life-saving drugs that they need? They're going to run out in a very short time now.

LAURA BICKER: Is there a way that the international community can help, would be allowed to help, North Korea would allow them to help?

[03:16:42]
DR. KEE PARK: So once again, you have to balance their concern about introducing viruses through the international staff. And I think the test case is going to be this vaccine in a couple of months, really. Would they allow a team in and say, "Listen, there was no ill effect of bringing in 25 people. And they're here, and there are no cases that you can detect. Can we bring another group of people in?" I think that would be the way to go.

LAURA BICKER: So I think one of the biggest surprises to someone who is sitting in the Korean Peninsula reporting daily about how South Korea was managing to flatten the curve, when it came to coronavirus, was how western countries, for instance, was not doing anything similar to what was happening in East Asia. Now Youngmee, if I can ask you—Again, I do feel like I'm putting you on the spot. South Korea produced a handbook for countries on how to fight the pandemic. What was your experience with other countries taking that advice? And also, were you surprised by how few in the west followed South Korea's example?

[03:17:55]

DR. YOUNGMEE JEE: Well, I want to say one example wearing mask. And we had one good example of the impact of wearing mask. There was the outbreak of COVID-19 in one of Starbucks Cafe in Seoul. And so all the staff of the cafe were wearing the mask while their guests were not wearing masks, because they have to drink coffee. So a lot of people, a lot of guests were infected. And also, there was secondary and tertiary transmission from those cases.

But no one, no one in the cafe, no staff in the cafe were infected. So that clearly shows the big impact of the wearing mask. And there are many other occasions like that. So hope that other countries could really introduce their wearing mask, as a mandatory requirement for the public. And also, in Korea, we had all the guideline for wearing mask in the public transport. So that kind of policy could be very useful if it was introduced early, maybe also in US and some other countries.

[03:19:23]
But I think some, some country, like Asian countries, may mean we were wearing masks from the beginning, like Hong Kong, and Singapore, Taiwan, those countries were implementing those countries very early. So no problem. For western countries, their kind of policy was quite difficult to introduce, was not really accepted widely on public. So that, I feel—I'm sorry for those. Those, the wearing mask is very, very easy, easy thing to do, in my mind. But I just want to give that easy example, that could be very easily introduced in many countries.

But somehow, with the WHO, I'm member of WHO Emergency Committee. So during the committee meeting, I really wanted to emphasize that easy policy could be introduced in many countries, if WHO give strong advice. But I think my opinion was rather minor. [laughter]

[03:20:38]
LAURA BICKER: Well, we now know—we now know that your opinion is well worth listening to. In terms of test, track, and trace—So I remember March the 11th, I put out a whole kind of TV and radio extravaganza on how South Korea was testing, tracking, and tracing. And it was two weeks before the UK went on lockdown. Did anyone kind of in the west, for instance,

get in touch to ask about how South Korea was testing, tracking, and tracing so quickly? Because at that point, we'd had the peak by about the end of February. And already, its numbers were beginning to come down. So in terms of test, track, and trace, did you find the other countries were kind of willing to learn?

[03:21:22]

DR. YOUNGMEE JEE: Yes, yes. Actually, we had a lot of occasions for doing the experience sharing webinars. Many countries, including US, US, we had a lot of webinars with US, mainly academic institutions. And also, some countries from Europe, like Sweden I think, France, some other countries. But I think maybe not UK. But Asian countries, including Malaysia, Indonesia, Taiwan—Taiwan and Singapore, we wanted to have some discussion of treble [?] bubble. But among European countries, I think there were a few countries that would ask us to share the experience of those three T, four T strategies.

[03:22:17]

LAURA BICKER: Wow. It was put into place quite effectively. We're all, apart from the gather ban, for those who don't know, in South Korea right now, we are not allowed to gather in groups of more than four people. But it works fine, because four people is the perfect number for dinner. [laughter] And more than that, you have to cook too much. Kee Park, obviously, when it comes to North Korea, very few followed their extreme example of closing down the borders. But in hindsight, do you think perhaps, even though it's going to affect them long-term, do you think it's been the most effective strategy for the country?

[03:22:57]

DR. KEE PARK: Yeah, without a doubt. This is a very smart way to go, to prevent the virus from coming in, in the first place. You know, they considered it a matter of national security. And they've done this before, where they've asked a country to sort of sacrifice, in name of national security, for instance, their weapons development. And same thing. I think people are willing to do that, to protect, so that nobody—no North Korean loses their life against this threat.

LAURA BICKER: When do you hope to get back in? Are you hoping at some point you will get back in?

[03:23:28]

DR. KEE PARK: We don't know. We're actually exploring ways to engage with our counterparts virtually. It hasn't been as easy as I thought it was going to be, because I thought it would be a very simple matter to do. But you know, pretty much across the board, DPRK missions around the world, including the ones here in the US and New York, they have sort of went to their own little bubble, you know. And so communication has been somewhat limited. And we know this is going to take a lot more time. So figuring out how to engage with them, share information, and support them virtually. It's been a challenge, but we're exploring it.

LAURA BICKER: So just to—So you're actually kind of chatting [?] to North Korea's representatives virtually about the situation in the country currently?

[03:24:16]

DR. KEE PARK: No, we tried to make that happen. So the best way to do it, I think, would be through a multilateral platform that they already trust and work with. So WHO would be a perfect platform to set up that kind of knowledge-sharing platform. You know, but where they approach the threats, I'll give you an example, is the quarantine period. They have gone as long as 40 days, 30 to 40 days. And, if you look at any other countries, in South Korea, maybe 14 days. And it's based on the level of evidence that you have.

But they don't look at it from—I think it's strictly from a medical evidence, a health evidence standpoint, where they say, “If there's a possibility that the virus can be still infectious after 30 or 40 days, then we're going to go the extra time.” So they see one example, one paper that describes this one anomaly, that's it. That's their cutoff point. So this is the way they think.

[03:25:17]

You might remember when they had the gentleman who tried to swim across to the North Korea border? And they shot him and burned him. And it wasn't because of—you know, he was a defector, but it was because they saw him as a carrier of potentially the virus. Same thing with the leaflets, you know. So for them, it's an attack. That's how they see it.

LAURA BICKER: Now, just to remind people watching, that you're able now to put in questions for our panelists. We've got one from Barbara who said, what lessons should we learn from dealing with COVID-19, so that we can be agile to respond to future pandemics? And how do we avoid repeating the war against COVID-19? Youngmee, you mentioned earlier that this will not be the last pandemic, which sent shivers down my spine, as well as the fact that we're going to be dealing with this for some time to come. So how should we—what lessons should we learn from dealing with COVID-19?

[03:26:20]

DR. YOUNGMEE JEE: That's, I think, as I may have mentioned, most countries—most Asian countries, mainly Asian countries, with some previous experience, were able to deal with this COVID-19 much better than Europe or US. But those countries, 100 years ago, the Spanish flu was the last big pandemic. And so after this, I think it will change everything for all countries now.

So we have to really see the demand for the health infrastructure that that can be really like a COVID-19, we never expected it can be like this surge of the medical need. But for the preparation for the after MERS, we were preparing like MERS, because MERS was mainly related to hospitals in Korea. So the number we prepared was not really enough. So we really have to prepare like, really, a search for the medical need, hospitals need, that kind of preparation need to be really done, in terms of infrastructure.

[03:27:44]

But for the low and middle-income countries, that's not going to be easy. So we will really have to see the long-term strategy for that. We need a lot of support for those countries, from WHO

and many other health partners. And once again, I want to emphasize the R&D network's role in responding to the future of pandemics. So I think we are lucky to have some coordination role by WHO. WHO and developing team did, I think, a great job during this crisis. And so we really learned how the power of the solidarity, and working together.

So with this, we were able to, of course, produce and even vaccinate the vaccine, newly developed vaccine within one-year time-frame So we really have to work together. And we have to prepare for the infrastructure for the surge. And the other part is actually training, training of human resources that is really critical. So even though we have infrastructure, if we don't have trained people, then we really don't know how to do it.

[03:29:03]
So the peacetime preparation, so I think the simulation exercise is very important. So there are actually four components in monitoring and evaluating framework for the international health regulation. So one is a simulation exercise. And the other is joint external evaluation, JEE so-called. We have done— Korea have done that join external evaluation. I think US did, UK did, many countries participated, more than 100 countries participated in join external evaluation. So I think this kind of exercise is very important. And, as I mentioned, simulation exercise, peacetime preparation, is going to be very, very important.

LAURA BICKER: How important is it to find the source of the virus [03:29:54] you've got colleagues within WHO in China as we speak. How important is it that we find the true source of the virus, and know where it came from?

[03:30:05]
DR. YOUNGMEE JEE: There was a lot of discussion on that from the beginning, during the emergency community. And I know there is a mission in China, I think that's maybe a quite long mission, because I think they have to be—as you said, they have to be quarantined for quite a long time, I think at least two weeks. And they will have to see the—meet with the experts in China, and basic [?] different places.

So with that, that mission, I hope that we can have some clue. But we may not really have definite clue, because that was the case with MERS and SARS. But still, this kind of efforts will help. Hope that we can have some better news from the mission.

LAURA BICKER: And Kee Park, when it comes to lessons being learned from COVID-19, do you think North Korea will have learned a lot of lessons from its handling of the virus?

[03:31:16]
DR. KEE PARK: So the North Korea, you know, it was interesting when you asked Youngmee in the beginning, how was South Korea prepared. So was North Korea. They had dealt with Ebola, MERS, SARS, and they have experience with this. And you know, so from their point of view, it's working. And I want to go back a little bit to the last question from, I think it was from Barbara. You know, what have we learned, right, from COVID-19?

[03:31:41]
You know, within a few days of the new inauguration, the Biden administration published a National Security Directive One, which has to do with a plan to retake leadership role in the global COVID response. It's a great read, by the way, if you want to read hundreds of pages. [laughter] But, what it does is, you know, remember, we were threatening to pull out of WHO, which is absurd. I mean. So it's about going back into WHO, actually becoming a member of COVAX facility and a donor for the AMC, and [03:32:15] in the tune of about $4 billion dollars, which is a massive amount.

And there's a clause in there about reexamining, the reviewing the current sanctions regime, as it relates to the country's ability to respond to the pandemic. This is really refreshing. And I bring this up, because, you know, we talk about what lessons have we learned. There are some things which are off limits to politics, okay. One is humanitarian aid, impartiality, neutrality. It's based on need, need only. Who cares about what the government is like? Or who cares about what our national interests are like. It's the needs of the people that are vulnerable. That's off limits.

[03:32:51]
Second thing is, global health security, there are no adversary countries. We're all in it together, right. No one is safe until we're all safe. A threat in North Korea is a threat in Washington, D.C. We've got to work together. And those things should be protected and, you know, off limits, period, right. And the last thing is, I agree with Youngmee, we've got to fully fund the WHO. It's still underfunded. You know, they still have to go out and beg for money to do all their programming.

[03:33:20]
And then, one more thing while I'm on this money thing. You know, US spends, what, $700 billion dollars a year on their military budget. And this whole conference is about, you know, the Harvard-Korean Security Summit. But we devoted Panel 2 on nontraditional threats. So if we just devoted, let's say, this is one out of six panels, one-sixth of the amount of money we spend on military to global health security, I'd be very happy about that. Because, you know, all the weapons that we have cannot kill a single virus.

[03:33:56]
LAURA BICKER: I think that one of the most sobering moments for me during this pandemic was when I interviewed Foreign Minister Kang here in South Korea. And it was way back in March. And she went viral across the BBC platforms, because she talked about the South Korean response. And I think everybody in the UK went, “Well, look what they're doing.” And she said, at the time, “One of the things that we need to be prepared for in this country is pandemics. And that's why we were prepared. And in the future, we need to be prepared.”

And that has stuck with me for a year, now. Because I think in terms of pandemics, it wasn't even something that was on my radar as a reporter, or as a correspondent around the world And here we are, now it's probably one of the biggest stories that any of us will ever cover. And in terms of preparedness, et cetera, so what would you like to see? You've talked about making sure that humanitarian aid is free, free from kind of any restrictions. And what would you like to see,

moving forward, in terms of world collaboration, considering your experience in perhaps developing worlds, and to try to help them be more prepared for pandemics?

[03:35:04]

DR. KEE PARK: So increased funding, number one, right. Let's spend less money on traditional weapons. And let's spend on building up health systems, especially in developing countries. And number two, take the politics out of it. I'll give you very specific examples. When North Korea, it was their turn to host the Regional Committee Meeting for the Southeast Asia Regional Office, that each members, they host their regional committee meeting once a year, it's their health assembly, US blocked it. US said, "No, we don't want you to have it in North Korea, because it's going to involve computers going into North Korea." It made no sense to me. So number one, politics out of it.

[03:35:40]

And I'll just bring the other example, is, you know, when Global Fund, which is a $4 billion dollar a year funder of HIV/AIDS, TB, and Malaria, threatened to pull out of North Korea in 2018, it was the height of the maximum pressures of campaign by the US. And they did. They pulled out, you know. And now they went in, ultimately. But North Korea actually still remembers these things It's fresh in their mind. They just have to be assured that they won't – US or any other country who are rich or have political power, they don't use health as a way to get their ultimate—achieve their ultimate national objectives. They just need to be assured of it. That's what they want to hear.

[03:36:24]

LAURA BICKER: As someone advising, do you think the governments, in terms of US and others, on this basis, you've read the document. You've heard the—As someone now advising the Biden administration and others, that this is now a way to go forward, in terms of where the money should go, and how it should be allocated?

[03:36:46]

DR. KEE PARK: Well, I'm always an optimist. And then, so I know that this is not going to—it's not a perfect world. And we know that, you know. We know that. And even the North Koreans politicize it. So everybody is guilty of it, let's face it. We all should be striving towards the perfect, the perfect ideal. And I think the Biden administration, by putting out this directive, has showed that's their intent at least. And I'm very encouraged by that.

DR. YOUNGMEE JEE: Laura, can I just mention one thing about North and South Korea?

LAURA BICKER: Please do.

[03:37:22]

DR. YOUNGMEE JEE: So I get some information about North Korea's COVID-19 situation from Dr. Kee Park. It is only information I can have. This very—I feel very, very sorry, and as a PT, that there is no information sharing for COVID-19 and other infectious diseases, and many other, between North and South Korea. So only some people know that North Korea belongs to WHO Southeast Asian Region of WHO. And South Korea belongs to Western Pacific Region of WHO.

So, because of political reason, so if North and South Korea can belong to the same region of WHO, there will be many opportunities, advantages, in terms of information sharing, and possible collaborations in health. So when I first joined WHO Western Pacific Region 2014, I really thought this could be a good move forward between North and South Korea. So I do hope—I always hope that North and South Korea can belong to the same region of WHO, so we can talk to each other, at least during the meetings, and workshops. And they can lead some other collaboration. I really hope that can happen within a few years. [laughter]

[03:38:47]

LAURA BICKER: Well, I mean, it looks like you two could make it happen, right? [laughter] In terms of—And you say you're hearing information about North Korea from Kee Park there. How frustrating is it, as someone who is sitting, you know, potentially we're only 100 miles,

really, from Pyongyang. I mean how frustrating is it, as an expert in the field, knowing that you can't help your neighbors?

[03:39:14]

DR. YOUNGMEE JEE: Yeah, that's really frustrating. So I actually talked to the Minister—Minister Kang, and with the other people in the Ministry of Foreign Affairs. I mentioned this a few times. But I know this is not going to be easy, but at least we can approach, I think we can try. That can open really a lot of opportunities.

LAURA BICKER: I mean Kee Park, this is an opportunity for the future?

[03:39:47]

DR. KEE PARK: Yes. There's always opportunities. [laughter] Always.

LAURA BICKER: Well, you are the ultimate optimist. You are the ultimate optimist. [laughter] [simultaneous conversation] Yeah. But is it a way to make this happen? Because it does seem, you've got this expertise sitting here in Seoul, you know, just a few miles. And yet the two can't collaborate. Is there a way that perhaps North and South Korea could collaborate, not just on future COVID-19, but on future pandemics?

[03:40:18]

DR. KEE PARK: Right. So the question is, why doesn't North Korea accept assistance from the South? It's this resource-rich. The problem is the politics, right. So when we try to convene a meeting, and they say, “Is ROK going to be there? We're not going to show up.” Because they see, as soon as ROK is going to be at the table, that something political – or there are political implications of the meeting.

And it has to do with the trust issue, you know. Because if they can just talk about the health aspects, you know, the vaccination aspects, then they're happy. But there are some strings attached. So it will take some time for North Koreans to really believe, and then understand and

know that US and ROK or whoever, their intent is very pure and simple. That's why you have to clearly separate out humanitarian global health security from all the politics, and make a Chinese wall in between. And it will take some time to do that.

[03:41:10]
You know, there is a—The COVAX AMC only provides vaccines, free of charge, to 20 percent of the population. North Korea is going to want the other 80 percent vaccinated somehow. And there are different ways to do that. One is, you know, bilateral arrangements with China, with their vaccines, or even Russia. They have got, you know, 92 percent efficacy rate now, which is outstanding. And they are very easy to work with, from North Korea's perspective, right.

[03:41:35]
But that could be an opportunity, through COVAX AMC, to get the other 80 percent through sort of a pooled funding mechanism, you know. And ROK has a lot of resources, so they can lead that fundraising effort, and pool together and say, "Here. You know, this is—We raised money to help pay for the vaccines for your population." I think that would go a long way, with no strings attached, right. Yeah.

[03:42:06]
LAURA BICKER: That's always the way. It's the strings attached. And Youngmee, do you think that's a possibility? Now I spoke to the Prime Minister during a press conference, I think, just two weeks ago. And he said they were looking at the possibility that, if they have more than enough vaccine, they could offer it to North Korea. Do you think that's going to be a possibility in the future with the current procurement program that South Korea has?

[03:42:31]
DR. YOUNGMEE JEE: Of course I think there is always opportunity. But it really depends on how the North Korea will respond. So I hope that they can accept if we offer. I mean that really depends on the response from North Korea. I think if the Prime Minister mention that that

can really happen, if we have extra, then we obviously are willing to offer. So that really depends on the situation from North side.

LAURA BICKER: Yeah. I mean I think in terms of humanitarian aid, Kee Park, they've always kind of batted it away. Is that because it comes with conditions? I mean we see in state media, quite robust language sometimes, where they appear not to be interested in humanitarian aid. Are they really interested in humanitarian aid, they just don't want it with any kind of preconditions?

[03:43:29]

DR. KEE PARK: Well, let's put the value of humanitarian aid in perspective. We're talking $20-$30 million dollars a year. I mean, you know, this is not a—It's not worth their time to even devote a bureau within the Ministry of Foreign Affairs to deal with it. Because the amount of money that's been going in from the humanitarian aid side has been cut down so much from diplomatic pressure, that it's really meaningless almost, right. The only ones they really take are UNICEF programs, and then WHO some programs through them. And then both of them are implementers for the Global Fund Program. And of course, the vaccination program. Those are the major ones, right.

[03:44:10]

So it's not this—You know, when you talk to some people, they say, “Oh, North Korea, they must depend on external aid for their population.” The truth is, that that's not the case. They can take it or leave it.

LAURA BICKER: And I'm aware that we're into the last few minutes, really, last few minutes. In terms of questions, if anyone has any questions, please feel free to put them to our panelists. But when it comes to the kind of advice that we would offer the world here from the Korean Peninsula, Youngmee you've talked a lot about the lessons learned. If we are to look at ways of learning from one another, is there a lesson that South Korea has learned from other countries? I mean I know South Korea has kind of been looking—put good advice out. There

was even a handbook. But is there a lesson that you've looked at from other countries, in terms of collaboration, that you think is valuable, that South Korea can take onboard?

[03:45:16]

DR. YOUNGMEE JEE: Obviously, we still need to learn a lot from other countries. There are many countries which have done a lot better than South Korea, I think. Although we managed to really flatten the curve now with third wave. But still, we are suffering with many deaths, compared with other countries it's not really that high mortality. But still, we need to learn from each other.

And obviously, it is not yet finished. We really have to look back after everything, at least acute phase of pandemic is finished. So we will have to see what we have done. At that time, I think, it was too early to say we have done successfully. So that's our homework, I think. So if you have some questions, I will stop here. But if you do not have questions yet—Do you have questions?

LAURA BICKER: I have questions. So combining two questions we've received, do we know how North and South Korea will distribute COVID-19 vaccines to their populations? And which groups will be prioritized? And how will those decisions be made? So combining the two, do we know how North and South Korea will distribute COVID-19 vaccines to populations? I think the two of you have covered that. So which groups are going to prioritized? And how will those decisions be made? Youngmee, if you can tell us which groups have been prioritized here?

[03:46:54]

DR. YOUNGMEE JEE: So first group will be front-line medical staff, the hospital staff, medical staff. And it will be the first group. And then, the old age group in the long-term care facility, they will be the next group. And then, we have, depending on the risk, we prioritize each group. So that will, I think, cover until the third quarter or fourth quarter of 2021. Yeah. But the number of each group is, I think, all planned according to the government, the national plan.

LAURA BICKER: And while I have you there, this is a really good question from Nina in New York. There has been a lot of discussion in the US about how comorbidities can affect the health outcomes of people who become infected with COVID-19. So how do the populations of North and South Korea compare to those of the US and other western countries, with respect to those sorts of comorbidities? That's a really good question.

[03:48:11]

DR. YOUNGMEE JEE: I don't really know about North Korea very well. But [simultaneous conversation] Yeah. But for South Korea, we do have quite the morbidity of the chronic disease people, like other western countries. So we do have high population of diabetes and hypertension and other chronic diseases. So they will be prioritized for the vaccination, definitely.

LAURA BICKER: Do you think having--

[03:48:46]

DR. YOUNGMEE JEE: [simultaneous conversation] --the age group. So there will be, the first group, over 65 years old, and then less than 65 years old will come later.

LAURA BICKER: But in terms of—because I think a lot of people, including the Prime Minister of the UK had said that one of the reasons why the death rate was so high in the west, was perhaps a higher rate of obesity, and heart disease, that kind of thing. And that's affected the death rate. What's the situation in South Korea when it comes to that kind of (a) comorbidity, or kind of risk factor, in capturing COVID, and dying from COVID?

[03:49:31]

DR. YOUNGMEE JEE: That can be tracked. So we do have relatively less obesity, compared to some other western countries. That can be actually true. We have relatively less obesity weight than western countries, I think.

LAURA BICKER: And Kee Park, over to you with those two questions.

[03:49:53]

DR. KEE PARK: Yeah, these are really good questions. So the prioritized groups. The way—We have some information on this, because North Korea has submitted an application to the COVAX AMC facility, to their program. And there, you are supposed to list the priority groups. And so my understanding is, that the one percent is front-line healthcare workers, followed by, I think, about 14-15 percent of the elderly population. And a third group is the population with the comorbidities. These are what they're proposing. This is what was accepted.

So then, of course, when it goes to actually, you know, the jabs in the arms, it will have to be monitored some way, to make sure that they stick to this plan. But those are the three groups that they are prioritizing off the bat. And then, as far as the comorbidities, there are some differences between North and South Korea, mainly in the terms of what we call communicable diseases, infectious diseases, is much higher in North Korea, especially younger population. But beyond that, if you look at things like diabetes, cancer rates, and those kind of things, they're more similar than not. That's been my impression.

[03:51:04]

LAURA BICKER: So in terms of the kind of—what about—I mean obviously, levels of obesity will be a lot lower in the likes of North Korea, as well as South Korea. That affects your—So far, we know your ability to fight the virus seems to be in underlying conditions. So there are fewer of those in North Korea. Is that right?

[03:51:24]

DR. KEE PARK: Well, yeah. So obesity, I think for sure. But things like diabetes, their rates are approaching almost 10 percent, which is—and in South Korea maybe slightly higher than that. So yeah, that's—that's a good indication of in the population, you know, the type of chronic disease that they carry.

LAURA BICKER: And in terms of how North Korea, in terms of health services, I know they're building this big hospital in Pyongyang, which they hope. Do you think that will go some way to helping them prepare for the likes of future pandemics, or any kind of health issues within North Korea? Is that hospital a big deal to you?

[03:52:01]

DR. KEE PARK: No. That's one hospital. You know, really, what they need, is a nationwide plan to strengthen the critical care capacity, ventilators, oxygen, generators, those kinds of things. And that's in their plan. And they submitted it to the WHO, a nationwide strategic plan for COVID response last July. And those things are actually all in there. So the Pyongyang Hospital, which we heard about, Pyongyang General Hospital, because of the news, and because Chairman Kim was there. But that's just one lip. It needs a nationwide plan.

LAURA BICKER: Youngmee, if I can ask you, in terms of hospital expansion, you mentioned there were going to be more ICUs, et cetera. You've learned lessons in that way. So how will you expand Seoul's and South Korea's capacity to respond to pandemics, in terms of hospitals and institutions?

[03:53:01]

DR. YOUNGMEE JEE: Seoul government is planning to have more public hospitals. But I think obviously, we also need to work with the private hospitals. I think in collaboration with private hospital, we can secure some bed ICU for preparedness for the pandemic. So that kind of planning will actually be decided after this, even during this crisis, it is happening. But those preparation.

So one is preparing more public sector, but also the definite clear cooperation plan with private hospital to secure more infrastructure for dealing with the pandemic preparedness, that that is coming, I think.

LAURA BICKER: Dr. Jee, while I have you, it would be lovely—We're finishing now. And I realize you guys have talked for a very long time. And it's been really interesting. Just if I could have your final thoughts before we go today, in terms of the COVID-19 and response from you? I mean your final thoughts and final, perhaps, words of advice, lessons learned, et cetera. What would be your final thoughts when it comes to COVID-19?

[03:54:23]
DR. YOUNGMEE JEE: It was really, really—I'm sorry.

DR. KEE PARK: Please. Please, Youngmee, you first.

DR. YOUNGMEE JEE: No, I think it was you. I thought it was--

LAURA BICKER: No, no, no. Let's have Youngmee first. And then we'll have Dr. Kee Park take charge.

DR. KEE PARK: The Scottish accent is really hard on me, too, Youngmee.

LAURA BICKER: Right. Right, then, laddies and lasses. Right. Dr. Jee, if I could have you first.

[03:54:50]
DR. YOUNGMEE JEE: So I was really happy to talk to Laura and Dr. Kee Park. Because that that was the only opportunity for me to know about North Korean situation. I really enjoyed session. And I just want to mention one thing about the US situation. So during the—I had the chance to participate in [03:55:16] last month. And I mentioned the return of US as a public global health leader. And I was very happy to see the change with this new Biden government, and very much welcome that US is back. And we all know these days, time for the global solidarity. And we have to work together. So all of us can only actually, from this pandemic, through the global solidarity. So hope that we can work, continue to work together, and hope

there is another opportunity for us to talk to each other, especially to learn about the North Korean situation. Thank you.

LAURA BICKER: And Dr. Kee Park?

[03:56:00]

DR. KEE PARK: Yeah. So Youngmee and I are both in public health, right. So normally, when we're talking in a panel, it's like an echo chamber. We're all sort of like, "Yeah, yeah, yeah." And it's really refreshing that, you know, John and the team at the Belfer Center has put this panel within this global—you know, the overall security summit. And the audience is different. I know this, because this is the Kennedy School audience, not public health audience.

And the message I want them to know is that global health security is different than traditional security issues. And it offers a whole new way to think about approaching, you know, cooperation, and diplomatic opportunities. And let's not—hope we don't waste it.

[03:56:48]

LAURA BICKER: Well, on that note, thank you both very much for joining us today. And it's been a fascinating discussion for me, especially someone who's followed this pandemic so closely. And to hear from both of you, especially as I cover both North and South Korea. So thank you so much for giving us your thoughts. And I hope, hopefully, keep your fingers crossed, that we're over the acute phases, as Dr. Jee keeps telling us, and that things get better from here on in. So with that [03:57:17].

DR. KEE PARK: [03:57:19] Laura. [laughter]

DR. YOUNGMEE JEE: [03:57:22]

[03:57:26]

DR. JOHN PARK: Well, thank you so much, Laura. That was an exceptional job in moderating a vibrant public discussion, public health discussion on a vital topic. Our thanks to Dr. Jee and Dr. Park for the critical public health work and sharing their insights about COVID-19. Thank you. We now move to our wrap-up session. Today's panels highlighted the fast-moving, nontraditional security issues from the Korean Peninsula. As an oracle of global trends, Korea provides an important perspective of how such issues play out in the global community.

During day two of our Summit tomorrow, we'll be exploring traditional security issues. Titled "Reading Kim Jong Un," Panel 1 will feature a unique collection of authors who researched and wrote path-breaking books about the young North Korean leader. Robin Wright of *The New Yorker* will be moderating the panel, with the intrepid [?] Anna Fifield, author of *The Great Successor*, the visionary Dr. Van Jackson, author of *On the Brink*, and the electric guitar-playing dynamo Ankit Panda, author of *King Jong Un and the Bomb.*

Titled "Negotiating with a Nuclear North Korea—What's Old? What's New?" Panel 2 will feature former US negotiators with North Korea and foreign policy experts. Our very own Dr. Francesca Giovannini, Executive Director of Managing the Atom Project, will be moderating an all-star panel, with Professor David Kang, Director of the Korean Studies Institute at USC, Andrew Kim, Fellow, with Belfer's Korea Project, and former head of the CIA's Korea Mission Center, Dr. Jina Kim research Fellow at the Korea Institute for Defense Analyses, Dr. Samore, Director of the Crown Center at the Brandeis University, and former White House coordinator for weapons of mass destruction, and Susan Thornton, senior Fellow at the Paul Tsai China Center at Yale Law School, and former acting Assistant Secretary for East Asian and Pacific Affairs.

[03:59:31]
As we close today, I'd like to add a personal note of gratitude in honor of Professor Ezra Vogel. Ezra passed away in December at the age of 90. He was our very first speaker at the inaugural Harvard Korean Security Summit, and a strong supporter of our early efforts to launch the Korea

Project. As a natural institution builder, his advice was golden. Ezra continues to inspire our community-building and mentoring activities at Harvard.

Thanks very much for joining today. And we look forward to seeing you for day two.

END