Center for Strategic and International Studies Holds Webinar on Countering Chinese Espionage

CQ Transcriptions

August 12, 2020 Wednesday

Body

Center For Strategic And International Studies Holds Webinar On Countering Chinese Espionage

August 12, 2020 03:00 P.M.

SPEAKERS:

JUSTICE DEPARTMENT NATIONAL SECURITY DIVISION ASSISTANT ATTORNEY GENERAL JOHN DEMERS

CSIS TECHNOLOGY POLICY PROGRAM DIRECTOR JAMES ANDREW LEWIS

[*]LEWIS: Thank you. Hello and ni hao to everyone. Thanks for joining us. We're going to be talking today to John Demers who's the assistant attorney general for national security--a job he's held for more than two years.

He leads DOJ's efforts to combat national security-related cybercrime, terrorism, espionage and (INAUDIBLE) controls, oversea FISA and conduct national security reviews under CSIS and the DOJ.

He was selected about two years ago--almost two years ago--to lead the China initiative at DOJ to counter the Chinese persistent and aggressive economic--economic espionage. And that's a lot of what we'll be talking about today.

Prior to his service as the assistant attorney general, John was the vice president and assistant general counsel at Boeing. And prior to that, he was also at the--you were in the first generation, right? Of the NSD initiation?

DEMERS: Yes, that's right. Yeah.

LEWIS: Yeah. So, NSD's relatively new and you were there starting in 2006.

DEMERS: Right.

LEWIS: Right, so long career, distinguished and thank you for doing this.

What we're going to do today is John will talk for a few minutes. I'll ask him some questions. We'll have a conversation.

And then, we'll turn to the audience. So, get your questions ready. We will screen them, so. But we'll be happy to entertain anything you want to ask.

John, over to you.

DEMERS: Great! Well, thanks very much, Jim. And thanks for having me and--and proposing that--that we do this on this topic. I know, you know, that National Security Division's done a number of events with CSIS including our 10-year anniversary event in 2016.

And, you know, more recently on this topic like just earlier this year we were kind of looking at the one year--a little bit more than one year mark on this topic. But this is a topic obviously, that continues to develop over time. So, thank you for having me again.

So, just for a little background then on the--what the China initiative is here at the Department, you know. It really was an organic outgrowth of the intelligence briefing that the prior Attorney General and I were receiving on, you know, a--a daily/every other day basis.

And we were just seeing in those briefings how much theft of intellectual property was emanating from China and directed by the Chinese government. And began talking about what could we do to, you know, step up our efforts to combat this.

Obviously, this falls squarely in NSD's portfolio. And for years, NSD has been working on this issue. But the question was what more can we do.

And so, we came up with this China initiative which as you said, was to focus on theft of intellectual property by the Chinese government mainly on the theft side. Just, you know, to give some statistics, 80 percent of our economic espionage cases at the department reigns, so that means theft of intellectual property on behalf of a state---on behalf of the government itself--or for the benefit of the government involved China--the Chinese government.

Sixty percent of our trade secret cases involve China, so that trade secret denominator is much bigger. That includes any theft of intellectual property by anyone anywhere, not necessarily government oriented or--or for the benefit of the government.

So, significant numbers and that was before the initiative. So, that's--that's the kind of thing we were looking at when we were deciding to put this together.

And we put this together for a couple of purposes. One, to make sure that we here obviously at Main Justice were focused on this issue and prioritizing the input.

A lot of it was to message the United States attorneys--94 U.S. attorneys around the country who are doing the bulk of the investigations and prosecutions together with the FBI. And these cases are difficult. They're not cases where you're going to have high numbers every year.

And so, we wanted the U.S. attorneys to understand though that they were a priority of the AGs. And he was going to understand, you know, if you had one economic espionage case in a year that's actually a good year in a given district. Two is fantastic and zero is, you know, not a shocker.

So, these are not going to be cases where you've got 30, 50, 100, 150 cases a year. Wanted to focus on them.

The second thing we wanted to do was empower the U.S. attorneys around the country to develop relationships with the private sector, and with academic, and research institutions.

So, a lot of what we see when we see it on the Intelligence side--those of us who sort of live in this space--what becomes difficult is when you go out and you talk about it. And you can get paralyzed because you think, "Well, I learned a lot of this in a classified environment. What can I say? What's classified? What's not classified?"

So, we--but we need those U.S. attorneys around the country to develop locally the relationships with the companies and academic institutions in this--in their area. So, we empower them and in terms of the materials, and

trainings that we get, etc. on, you know, what it is that they could say to the companies to sensitize them to this risk and to try to develop the relationships. We need the private sector in this working with us to help us defend them.

And--and then, the third goal really is to look also at our other tools like you mentioned, Jim, the Committee on Foreign Investment in the U.S. that looks at foreign acquisitions here in the U.S. mainly of technology, but increasingly of data. We can talk a little bit about that as well within China, and--and--and work that process, and make sure that we were adequately focused on the National Security risks.

So, you know, we ticked that off about two falls ago--two autumns ago. Look, we were building as I said, on a series of cases that began in about 2014 with the first indictment of People's Liberation Army officers for cyber intrusions into a variety of--of companies and institutions.

That was really a--a seminal moment. So, I always like to start there because, you know, as you start to think about it, you realize that many of these cases are traditional law enforcement actions. But ones with significant foreign policy ramifications.

So, back then--that was back in the Obama administration--getting, you know, the entire sort of interagency on board with the idea that the Justice Department was going to charge members of another country's military with cyber intrusions is--was a big lift, you know.

LEWIS: Yeah.

DEMERS: But we get it. We went ahead and that has--is a precedent that we've been able to build on and, you know, we had a cyber indictment just a couple of weeks ago. Again, that one involving the Ministry of State Security to Chinese Intelligence Services.

So, we were building on that and what we were trying to combat in this is, you know, what I've called a rob, replicate and replace approach to economic development that we were seeing from the People's Republic of China. And that is, you know, stealing American intellectual property, replicating that product, and then replacing the U.S. company first on the Chinese market and if all went well, on the global market.

And we saw this being done as I mentioned, through cyber cases. But if you look at our more recent cases, what most of the cases we charge are actually insider cases.

So, there's individuals at companies or academic institutions here in the U.S. who are stealing and bringing the technology to China. Now there's--even within that, there's a couple of different kinds.

There's one set which I think of as sort of the state directed cases. What we saw since 2014 was an expansion of responsibilities within the Chinese government from pure People's Liberation Army hacking--cyber intrusions--to the use of MSS or the Chinse Intelligence Services to take intellectual property.

As a consequence I think of that shift in who's working on this issue on the Chinese side, you have a shift in tactics because when you bring in the Intelligence Services, what they're really good at is developing relationships to get information. That's their trade, right?

Since the beginning of civilization for all of us. And what we're seeing in China is then using that same trade craft and those same approaches to develop relationships with individuals in companies here--

LEWIS: Yeah.

DEMERS: --in order to coop them to give information there. And that's what they do on the traditional espionage side and--and have done for a long time.

So, that means that a lot of our cases aren't just the cyber intrusion cases. Although the MSS does that too. They're these insider cases.

And--an, you know, an example of that would be the MSS officer who we extradited from Belgium two years ago who had coopted an individual at a U.S. aerospace company in order to steal commercial jet engine technology and bring it to China.

The--the second category in this--these individuals--these insiders--are people who have been induced by Chinese programs like the Thousand Talents Program to take intellectual property from their employer--whether it's a company or it's a university--and take that to China one way or another by entering into these Thousand Talents contracts and get paid either for doing work there or really, ultimately for transferring the intellectual property.

So, the Thousand Talents' just a level set everybody is program that at one level is totally fine. It's about recruiting the best human talent you can from around the world and bringing it to China. Something obviously, a lot of companies do, right?

And a lot of organizations do when they go after the best people. But it has a underbelly and the underbelly is that when you apply for this program--it's a very formal, bureaucratic process to apply for this program--you've got to show that you're going to bring intellectual property there.

And an aspect of this--and if you look at our cases that we brought--a lot of our academic cases involve individuals who were members of this Thousand Talents' Programs. And a hallmark of the ones we've charged is that they're hiding their Thousand Talents' affiliation.

So, this isn't as if, you know, "I worked at one company--"

LEWIS: Yeah.

DEMERS: "--and then, I openly sort of, you know, have a--have a weekend job" or something like that. These are individuals who are hiding from the U.S. government from which they were getting grant money to do the same research hiding from their institutions, their affiliations with Chinese universities or other Chinese entities and they're work there.

And--and so, if you look at our cases, they all kind of sound in, you know, fraud, tax fraud--

LEWIS: Yeah.

DEMERS: --you know, grant fraud, things like that.

So, that's, you know, the way. And that--and that last piece, you know, Jim, has really developed. I--I mean, when we started this initiative, I--we didn't really have that piece in mind. That's developed through the investigations that we have done, you know, together with the Bureau.

So, you know--

LEWIS: So, I was talking--I was just talking to somebody who's on the Board of one of the big Tech universities. And what do you think the reaction is to the universities to this?

I know this is a little off-topic, but they weren't entirely persuaded that all their Board colleagues were understanding of our problem.

DEMERS: Yeah. I mean, look, I think here's the thing. When I go to a company and I say, "You know what the most important thing is that you protect the intellectual property that different--differentiates you from your competitors and people are trying to steal it. You should really protect it." It's, you know, like, "No, duh. This is what I'm supposed to be doing."

If you go to a university with a very different environment which is one that begins--and frankly that the Chinese are taken advantage of--which is an open environment sharing information, you know. The hallmark of being successful at universities is publishing your findings, not keeping them secret to monetize them, right?

LEWIS: Right.

DEMERS: And--and you go there, and you start to talk about theft of intellectual property. It sounds very different.

So, the--the--what we have been emphasizing for the universities is one, "Here's the risk that you're facing. Here's what's happening. "

We can talk about, you know, the recent actions involving the PLA researchers in this context. And look, what we're saying is we expect you to have clear conflict of interest and conflict of commitment policies, so that your disclosures to the federal government are accurate.

But if you're comfortable that you're professor has this relationship with China and it's all openly disclosed to you, we're not going to tell you not to do it unless, you know, the information is classified or exported whole.

So, we're not telling. So, unless it's government information or exported whole information, we're not going to tell them what to protect. But we are going to push the value of a transparency at those colleges.

And if you look at the cases that we indicted, if you look for instance, at the Harvard case which--

LEWIS: Sure.

DEMERS: --since it's Harvard got, you know, the most notice. Here's an individual who unbeknownst to Harvard, was using Harvard's logo and name in China. I should say these are all allegations. That case is still pending.

Using that name in order, you know, as part of a collaboration with--with a Chinese university. And again--and again, that if he had been doing that openly--at least with respect to the university piece, you know, the university could decide what is inbounds and what's not inbounds.

So, the differing reaction, but we've been working very hard with the universities--the Bureau has.

Coronavirus has, you know, sort of hand--hampered us in our ability to continue our outreach to them, but we're doing what we can, you know.

LEWIS: It's been a busy couple of months for you. So, I think people will be disappointed if we don't talk about TikTok and WeChat, if we don't talk about the Houston Consulate and, you know, then the whole China telecom Huawei clean network thing.

DEMERS: Right.

LEWIS: So, I don't know where you want to start, maybe with Houston?

I mean--

DEMERS: Sure.

LEWIS: --why Houston?

DEMERS: Yeah. So, you know, a couple of things on Houston. One, Houston has long been on the radar screen of the FBI as the source both of a significant intellectual property theft emanating from it including--including recruitment into the--the Talent Program--

LEWIS: Yes.

DEMERS: --spotting and assessing of folks.

And then, on the foreign influence side or the covert foreign influence side which we at least at this point can talk a lot less about, but I hope one day we'll be able to--to talk more about.

So, that's why Houston and, you know, was not chosen at random out of the consulates out there. They were actually at the forefront in both of these hearings. And the closer of the Houston Consulate and the simultaneous actions taken with respect to the PLA folks who were here, but not disclosing their affiliation. If they were here on J1 research visas, they were not disclosing their affiliations with the PLA--were all attempts at disruption of what we had been tracking for quite some time of activity here in this country.

And what you've seen sort of publicly in terms of those disruptions for arrests, you know, I think more than 50 interviews in 30 different cities. Even if that number is still just a tip of what was going on under the surface and what we were trying to disrupt together with the Bureau and together with the State Department, of course, whenever you're talking about a consulate closure.

So, if we recognize that we're not going to just be able to prosecute our way through these issues. There have been years of folks being sent here undercover in a variety of covers. And what we need to take are actions to disrupt that level of activity. And that's really the best way to understand what happened in Houston and also to understand what was happening on the--on the PLA side of things.

LEWIS: Now I'm going to warn you that what you say next could alienate millions of 15-year-olds, but do you want to talk a little bit about TikTok?

DEMERS: Yeah. Well, it alienated me from my daughter as well, so.

(LAUGHTER)

You think, you know, so what are our National Security concerns with TikTok?

TikTok, look, is a very interesting case. Let me just step back and say one of the things we've seen and--and really kind of exploded on the scene with the pack of OPM, right?

LEWIS: Uh-huh.

DEMERS: And Office of Personnel Management Records, but after that with, you know, as recently as the Equifax indictment we brought a few months ago, Anthem, the healthcare company hack and other cases we've seen.

LEWIS: Sure.

DEMERS: It is a Chinese appetite for large volumes of sensitive personal data, right?

LEWIS: Uh-huh.

DEMERS: And we have seen that on the cyber intrusion side as I just talked about. We also see it on the CFIUS side.

So, we see targeted acquisitions or proposed acquisitions of U.S. companies that wouldn't traditionally be thought of as falling within CFIUS because CFIUS was traditionally thought of as protecting technologies, right?

LEWIS: Yeah.

DEMERS: On the data side, you know, that brings into sort of the CFIUS purview health insurance company, financial services companies, all sort of data especially as you think about the fact that more and more smart technologies exist. And those smart technologies are gathering data continually on your life and the way you're living your life. We've had a lot more of those come through the CFIUS process.

So, what's interesting about TikTok is you have one of the first instances in which individuals are signing up for and providing the app with their sense of a personal data. First, when they sign up for it, right?

And there's, you know, information you can give. And some people tell the truth and some people don't, right?

(LAUGHTER)

And then, there's the data that the app collects about you while it's on your phone. And like a lot of other apps, that app is collecting geo-location data. If you enable it, it's connecting your contact list. It's--it--it is following your use of the phone and other apps on the phone.

Part, you know, certainly on the surface to provide you with a better TikTok user experience, right?

LEWIS: Sure.

DEMERS: But can also be used--abused really by--by the--the State. So, once is the sense of the personal data piece.

The second is, you know, what we saw a lot of allegations on TikTok when it comes to censorship of certain policy views. So, you know, Uyghurs, Hong Kong protests, Tibet, Taiwan, all those issues, you know. There are many reports of the content being censored from a--from a foreign influence perspective.

So, those are the National Security risks associated with TikTok. What's interesting about TikTok is you have an instance of, you know, Americans voluntarily signing on to this product as opposed to the Chinese stealing the data or the Chinese buying the data.

And that's what, you know, the--the recent executive order was--was meant to address. And we'll kind of--obviously there's more for that process to play out. But we'll see how it goes.

LEWIS: So, when you look at the actions over the last really year, I mean, you've got Huawei. You've got China Telecom in the U.S. You've got Clean Network. You've got TikTok and Tencents. And maybe we'll come back to that, but what is the goal here for the administration? What is it they're driving for?

DEMERS: Well, certainly, very focused on telecommunications as you point out in--in--in the way you strung together there. There's a--a real I think appreciation that especially as we move to 5G technologies, you know, as I think any of us who'd think about it for a little while realize is just so much of your life is running over telecommunications network right now. And never more so than during Covid, right?

(LAUGHTER)

As we're doing right here. Your professional life, your banking life, your personal life, you know, your social life, on and on. And with the internet of things, of course, more and more things are going to be connected through 5G cards, you know.

Your--I just bought a new oven. Your oven is connected to your phone if you want it to be, your refrigerator, you know, all of those things. All of which can be used to paint a very interesting picture of your life to someone who wants to learn more about you.

So, one is that an understanding that the security therefore, of the networks over which all that data is running is really paramount to National Security in this century. And so, what you're seeing with the focus on the telecommunications licenses, the use of Huawei and the resistance of the use of Huawei and 5G networks is a desire to ensure that we have trusted vendors from trusted countries. And that is countries that share our same political values that are running these telecommunications networks over which our entire lives are already running and only will run more so in the future.

LEWIS: Huawei brings up the issue of cooperation with other countries and we're not the only one to experience Chinese espionage. And, you know, I--the Canadians, of course, now have people being taken hostage in China. What's it like working? Where do you--how do you assess cooperation not just Five Eyes, but NATO, others--Japan, Australia? What's the effort to cooperate with these in these cases?

DEMERS: There's--on the 5G, you know, there's been a tremendous effort to--to cooperate with these other countries starting with the Five Eyes, but then growing out from there in Europe and in Asia.

And it's been a--a difficult road, but it has. It's also born successes. Obviously, the U.K. just changed its position on the use of Huawei in--in 5G networks.

That is, you know, the result of I think a lot of discussions with--with these countries and trying to illustrate to them the risk. But we're--the main thing that we're up against in these discussions is not a failure to appreciate what the risk is. It's a worry about the economic impact that angering a country like China can have.

China remains a tremendous market for a number of these countries, investment opportunities both sort of foreign direct investment into them, and then investment by their companies, and the Chinese market for their companies.

So, that's always a--and we've seen numerous reports of this. But that is very openly an economic stick that's, you know, held over the heads of these countries as they're making a decision on--on the 5G front. And that's been something that we have had to--to work through.

I think in this regard actually, China's behavior during the Coronavirus has actually, you know, helped move some folks into our camp especially in Europe by illustrating some of--some of the risks.

LEWIS: Yeah. It just is a footnote. We have a separate project with my colleague Heather Conley interviewing Scandinavian countries. And one thing that surprised me about Chinese investment and one thing about surprised me is how many of them brought up Hong Kong as--

DEMERS: --Yeah--

LEWIS: --Something that--that created, you know, unhappiness and--

DEMERS: --Right--

LEWIS: --Bad feeling in the relationships. So--

DEMERS: --Yeah--

LEWIS: --I don't know if the Chinese always get that far. Chinese viewers, no offense, you know.

DEMERS: Yeah. I mean, I think you're right, Jim. Hong Kong and the Uyghurs have been two of the biggest issues especially in my discussions with the Europeans.

LEWIS: Yeah.

DEMERS: Those are the two issues that have really, you know, sort of brought to life I think some of the risks we're talking about and also solidified the importance of sort of--look, we have a lot of our disagreements with the Europeans and about different things.

(LAUGHTER)

But the truth is at the end of the day, we do share the same political values. And that is very helpful when we're having these discussions.

And I think, you know, what happened in Hong Kong with the--the breaking of the promises--

LEWIS: --Yeah--

DEMERS: --Obviously that they made in '97 was happening with the Uyghurs has--has really helped us.

LEWIS: Well, I want to come back to the economic issues. But since you brought it up, one of the things that I admired kind of in the executive order was it looked like it was very skillfully written in a way to try and catch apps.

So, apps are a new problem. You've got--

DEMERS: --Yep--

LEWIS: --A foreign service located outside the U.S. made by another country.

So, what were you guys thinking when you wrote the app language which, you know, the Europeans share that problem. They like to catch apps. Not just Chinese apps, but what are you thinking in terms of extraterritorial, sovereignty? What's the story on apps?

DEMERS: I mean, apps are, you know, really raise the problem that I think TikTok illustrates best and that is, you know, you have there available in your app store. And you have U.S. users who are choosing to download those.

But once you do that, you really have no idea where any of that data is going. I think all of us even use the most ubiquitous apps that we use. We--we don't really appreciate everything our phone is collecting on us in our lives.

(LAUGHTER)

And we tolerate that risk. Maybe if we think that the worst thing that's going to happen is I'm going to get strange solicitations for something that I didn't realize anyone ever knew that I was interested in.

(LAUGHTER)

But I was talking while Siri was on and Siri picked that up. And suddenly--

LEWIS: --Yeah--

DEMERS: --Sent me an ad on my Washington Post app for the very thing that I was talking to my wife about.

(LAUGHTER)

So, you know, we--we sort of tolerate that because it provides us I think with benefits. But once you start looking at that from a National Security perspective, and--and thinking about the data that--that the phone and the apps are collecting on you, it's a very different matter if a country with very different values from a--a--and without the same rule of law, and separation of powers that we have, and impacted court system is collecting all that data.

And what--what we see or in terms of what--what are the Chinese doing with this data? Which is the other question that often comes up. And--and we see two different things. One, huge quantities of data are needed to perfect artificial intelligence tools/algorithms.

So, one of them is, you know, that. The second is more from a counterintelligence perspective--99 percent of that data they will not be interested in from a counterintelligence perspective.

But once they're interested in somebody if it's as a potential compete [sic], or somebody who has just gotten an important government job, or something like that, if they can mine those existing data sources to find out what that person's financial like--life is like, what their health life is like, what their, you know, married life is like, you know.

If you're a married person and you have a dating app on your phone, that's a little strange and of great interest to an intelligence officer, right?

And they can use all that to paint a very effective picture of you and to think about where your vulnerabilities might be or even how best to approach you. If the purpose is cooptation, how to--how to approach you for that purpose.

LEWIS: Yes.

DEMERS: So, you know, that's what we think they're doing with these--with the information. Then, of course, geolocation is very important for--for targeting someone if in fact, that's what you're doing. I don't mean targeting like killing. I mean, targeting just by following around.

LEWIS: Sure, yeah.

DEMERS: In fact, for instance, that my phone doesn't move throughout the workday would tell you--if you didn't already know--that I work in a secure facility, right?

LEWIS: Uh-huh.

DEMERS: Because your phone probably moves during the workday, right?

It's--it's--it's in your pocket. It's in, you know. And so, if I'm--let's say I'm undercover and I'm pretending that I have one job, but in fact, you see my phone behaving in a way that suggests I have another job, that tells you a lot about me too.

LEWIS: So, the other company that the executive orders went after was Tencent and WeChat. And Tencent's a great company. If they were located anywhere else, they would be giving American companies a real run for their money.

But the EO is crafted in a way that--that it goes after WeChat, very popular app. Not a lot of users in the U.S., but it didn't seem to go after the game side of Tencent. Is--was that intentional? Was it an oversight?

I don't want to tag you guys on--I don't want to ruin Tencent's business here. They'll probably be mad at me.

(LAUGHTER)

You know--

DEMERS: --Yeah--

LEWIS: --That's where they make most of their money in the U.S. is on gaming and they have some really good games. So--

(LAUGHTER)

Is that your chance to alienate even more teenagers?

DEMERS: Exactly.

(LAUGHER)

No, look, the--the--the--the--there--there was not an oversight in the grafting of that EO there on--on the WeChat part. It's--it's a little different, right?

It's a communications app. Fundamentally. It--it does collect a lot of the same information about the users that we were talking about before.

LEWIS: Yeah.

DEMERS: Back to TikTok, there's that piece of it. In addition, WeChat is used here in the U.S. as a method by the Chinese Communist Party to communicate with Chinese individuals here in the U.S.

For instance, I'll give you an example from the university setting where the Chinese students at a university--students who are visiting here from China--all have WeChat. And they will be in a group chat with the other students at the university. And the Chinese will use the WeChat to message what they want to the Chinese students.

So, for instance, the State Department has some great examples of messaging by the--here's the goal of the Chinese government. Send the Chinese student here to reap all the benefits of the U.S. technical education, but not allow them to get polluted by ideas like liberal democracy or religious freedom, right? How do you do that?

You need to control the space around them both electronically and you need to encourage what already happens with foreign exchange students just like, you know, they like to hang out with people who speak the same language and of the same cultural references as them.

You look at U.S. students in Rome, for instance, all like, "Are you really learning Italian here? You just keep hanging out with each other."

(LAUGHTER)

So, the--they--they try to encourage that by creating these bubbles around the Chinese students. And by messaging, for instance, America's very violent. Look what's happening. Look at this picture. The--the--the Global Engagement Center estate has great examples of this.

Look at this picture of this Chinese guy who was beaten by the police. I have no idea whether the picture is true or not. But they message the--how, you know, dangerous America is. "Don't go out there." Don't--you know, basically get to know the country.

So, WeChat has a kind of foreign influence. And in this case, it's a little even less foreign influence and more controlling aspect to it which, you know, obviously an app like TikTok doesn't have.

So, it's a slightly different risk profile, but still one that's been on our radar screen as a used--because of the Chinese government's use of it here in the U.S.

LEWIS: We have a boatload of questions. So, I'm just going to start going down the list.

DEMERS: Yeah.

LEWIS: One of--one of the first was that the recent indictments have highlighted the efforts to steal vaccine and anti-viral activity.

DEMERS: Yeah.

LEWIS: You--you know, are there other hacking teams? What's the situation going on there? How much is China focused on stealing vaccine data?

DEMERS: Yeah. So, look, first of all, you have to sort of see that in context. We know from our prior cases that the Chinese have long been interested in biomedical research of all kinds, right?

LEWIS: Uh-huh.

DEMERS: So, just recently we stopped someone in Boston who had vials of biomedical material in--in her--on herself--on themselves as they were trying to, you know, go back to China. They'd been a researcher here in the U.S.

We--we've seen it in--in other cases that we've indicted. It's on the Made in China 2025 plan, right? So that--

LEWIS: --Uh-huh--

DEMERS: --Gives you a sense of where the focus of Chinese efforts are. So, in that context, it would be surprising if they were not trying to steal the most valuable biomedical research that's going on right now. Valuable from a financial point of view and invaluable from a geopolitical point of view to be the first--maybe the Russians have them beat now. I don't know--to develop a coronavirus vaccine or treatments.

So, what you saw charged in that one case was just one of multiple that was an attempted intrusion--intrusion of attempted intrusions that we have seen around the country. And, you know, obviously we haven't charged all of those for--for a variety of reasons.

But it--that isn't sort of the exclusive piece of it. It--it's part of a--of a greater effort to see, you know, to try to collect whatever research there is to try to get ahead of this.

LEWIS: I can combine a couple because they overlap. People ask, "How do we avoid the appearance of racism?"

And then, among Chinese students and researchers of Chinese consent, there's a concern that this might lead to a Red scare and racial profiling. So--

DEMERS: --Yeah--

LEWIS: --The Red scare one is a legitimate one. Racial profiling? I know. What are you thinking on that? How do we avoid that impression?

DEMERS: Yeah. So, look, this is something that we are very focused on--have sort of flagged as an issue from the beginning.

LEWIS: Wow.

DEMERS: We launched this. I mean, one, if you look at our cases you'll see that although many do involve individuals of Chinese descent, others do not.

The Libre case, the Harvard case in Massachusetts--

LEWIS: --Right--

DEMERS: --Is not a--a--a Chinese American person. To the extent that they do, it's because we--what we've seen is that the Chinese government itself focuses on--and when they're trying to coop, they focus on individuals of Chinse ethnicity.

The more recent the immigration, the better because--

LEWIS: Yeah.

DEMERS: --Part of the--the focus could be coercive. So, if you have family back in China that you feel like is at risk or--or are planning on going back to China and want to make sure you have a job, then you're going to be more willing to help the Chinse government.

But the--what we always say on the--to the businesses we talk to, obviously to the--the agents we work with, and to the schools, you need to focus on behaviors. Ethnicity is not a risk factor. Don't focus on ethnicity.

Then the upside of focusing on behavior as well as being of course, consistent with, you know, the values that we hold dear is that you're going to catch people who are misbehaving regardless of their motivation.

So, you're going to find that person who's trying to take intellectual property of your company, and is stealing it, and wants to send it to the Chinese. But you're also going to find the guy who is just unhappy with the company and looking to get revenge.

You're going to find the guy who wants to sell it to another U.S. competitor or who wants to go out on his own and set up a competing enterprise.

So, it's really to your benefit not to focus on--on this security risk as a Chinese intellectual property theft risk, but as an intellectual property risk. And then, you'll find people, you know, as I said, regardless of motivations.

But where we are very sensitive to this, we like to talk about it in terms of what the Chinese Communist Party is doing, what the PRC government is doing because it really is a concerted top-down authoritarian plan here. It's not about, you know, people of a certain ethnicity, you know, doing this kind of activity on their own.

LEWIS: So, related question that I got from a couple of people is a concern that screening Chinese students or Chinese researchers when they leave the U.S.--screening them at the airport is going to become a new norm. Is that a realistic concern? Is that what, you know, what's the attitude on that?

DEMERS: I think, you know, what we're trying to do is really write with a fine pointed pencil as opposed to a big magic marker.

So, if you're, you know, that means, you know, folks may get screened on the way out. But that's not going to be everybody. That's going to--may depend on what institution they're coming from in China if we have reason to believe that that institution's been involved in intellectual property theft in the past, what fields they were studying in here.

A guy who's a younger graduate studying Mesopotamian architecture is probably not going to get screened at the airport. But--

LEWIS: --Oh--

DEMERS: --The--

LEWIS: --Go ahead, you know.

DEMERS: But someone who's here as a visiting researcher who's a professor in, you know, in an advanced field and comes from a university that's been affiliated with the PLA, and, you know, who we know folks have come and gone from there in the past, they may get screened.

So, you know, I think, you know, there has been some--for sure some significant screening at the airports as people leave. But it--it's not, you know, it--it's more targeted than it may first appear.

LEWIS: Someone asked if you see a connection--a strategic connection--between the soft power and cultural propaganda activities in the U.S. that we talked about with TikTok and WeChat. And the data theft--the data I.P theft--the acquisition of stolen I.P. Is there a connection between these two that you see? Is it--or are they two separate programs run by the Chinese? That's a hard one.

DEMERS: At first blush, I would say that they are separate. Certainly, you can use the data as I said, to create targeting practice for individuals who you might want to--to influence. But for the most part, I would say that these are two separate efforts, but some overlap on the part of the government. But I'd have to think about that a bit more.

LEWIS: Okay. We're getting a ton of questions, so we'll try and get through as many as we can. I appreciate it.

DEMERS: Yeah.

LEWIS: They're really good too. We got one. Someone was actually listening to what you said and they noted that you said, "China's behavior during the coronavirus has actually helped move some folks into our camp--"

DEMERS: --Yeah--

LEWIS: "--Especially in Europe." Could you talk about specific behaviors that prompted this move?

DEMERS: Yeah. I think the somewhat ham-handed attempts, for instance, to dole out assistance--personal protective gear, et cetera, while requiring countries to thank them publicly for the great assistance they receive--

(LAUGHER)

From the wonderful country of China. Now you can do this subtly.

(LAUGHTER)

But when you do it really obviously--

LEWIS: --Yeah--

DEMERS: --It comes off the wrong way, right?

And it looks like you're conditioning humanitarian assistance on deep expressions of gratitude. And I think folks don't appreciate that and they see through your ostensibly charitable intentions.

So, that is a--a piece of it. I do think that there's been, you know, continued questions about not necessarily the--although it's still open questions for the origins of the virus, but, you know, did--how did the Chinese government respond initially in terms of their suppression of knowledge about the virus and even their--their retaliatory acts they took against or the pressure they put on countries that were starting to for instance, restrict flights to certain parts of China.

That was very offensive to the Chinese government when those things were happening. In hindsight, you might say, "Gosh, I wish we had all done that sooner." But while it was happening, the Chinese government reacted to those actions by certain European countries like it was a--a--a--an--a--an offensive to them and pushed them--including through, you know, economic means--to reverse their decisions.

So, all of those things I think sort of illustrated to individuals and coming on top of what you mentioned, Jim, which was the backdrop of the Hong Kong and the Uyghurs that, you know, maybe this isn't a country that we share the same values with.

LEWIS: So, one of the questions--this is actually a question I was going to ask too. They said, "How do you differentiate what the Chinese are doing both in trade craft and in objectives from what other countries do when they spy on us?"

And I was going to ask specifically about Russia, how we would compare Russia--

DEMERS: --Yeah--

LEWIS: --To China. Questions from the floor are raised about other countries who I shall not name.

(LAUGHTER)

But how does Chinese--how does Chinese espionage compare?

DEMERS: Yeah. So, if you look at--let's start with economic espionage--

LEWIS: --Yeah--

DEMERS: --If you look at that--because that's where we've been focused today--

LEWIS: --Yeah--

DEMERS: --We definitely see Russians attempts to steal military technology and export control technology. We don't see the same effort to steal commercial technology for the purpose of developing Russian competitors to American companies or to European companies.

So, the breadth of that Made in China 2025 plan inclusion on that plan of technologies that run the gamut from agriculture to, you know, engines that could be used in fighter planes is not something that we see not just in Russia, but honestly we don't see it in any other country.

LEWIS: Instead of--

DEMERS: --Although we do see and we've charged a number of cases that involve--

LEWIS: --Right--

DEMERS: --As from Russia, they're--they tend to be more focused on the--the military controlled technology aspects of it.

LEWIS: Maybe a related question is people ask--and it's reasonable--as the--the U.S. and China go into a more tense relationship, as we move down the path of decoupling, have you seen a more urgent set of Chinese efforts or expanded Chinese efforts? Has--has decoupling effected the--the level of Chinese espionage?

DEMERS: I don't think it's affected the espionage that I've seen so far. I think that, you know, clearly the talk on both sides--including on the Chinese side--is stronger, you know, including out of, you know, folks who tend to use diplomatic ways of speaking.

LEWIS: Yeah.

DEMERS: So, there's been an increase in--in rhetoric. But I don't see an increase in economic right now as a result of this, you know.

We have seen this espionage for many, many years. I think it has gotten more persistent, more sophisticated and more well-resourced over time, but that's kind of a longer time trend.

And a lot of these programs take quite some time to develop. And programs like the undisclosed PLA individuals are things that we're trying to undo now. But they've actually, you know, been going for quite some time.

LEWIS: Someone asked related to that is most of the--and you said this in your remarks. Most apps collect this kind of data. So--

DEMERS: --Yeah--

LEWIS: --What's to stop the Chinese from simply turning around and purchasing it or hacking it and stealing it? What? And this is--this is on some ways a privacy question is that--

DEMERS: --Okay--

LEWIS: --Do the relative porousness of our privacy rules give China other avenues even if you show off their apps?

DEMERS: Yeah. Look, probably the biggest avenue that that gives them is purchasing both data on the open market. There are data of (INAUDIBLE), you know, who will sell--who will collect data and then sell it either for commercial purposes or they're happy enough to sell it to--to nation states as well.

The--so, what's to stop them from like stealing, you know, some other, you know, U.S. apps--data? I mean, not, you know, that country's information security protocol. And it's just another avenue.

So, if we're talking about purchases of data, some of which when it comes to a purchase of the companies we can regulate through the investment review process. We are trying to combat the theft of data--and that's in our cyber intrusion cases--and, you know, our work with the private sector.

And then, the app is just sort of a third way to get data from--from users and--and who are voluntarily providing the data whether it's knowingly or unknowingly.

LEWIS: So, we did get one question that started off by saying, "WeChat is so critical to business and social life in China. I have WeChat. I have WeChat on my China phone. It's currently in a drawer with the battery out, but that's a different story.

Is the EO designed to really speed decoupling to going beyond simply WeChat and TikTok? Is it--is it a measure to really decouple the U.S. and China?"

DEMERS: Well, I--I certainly didn't read it that way or think of it that way. The, you know, and look, there's a lot to be left now with the Commerce Department to work on their--the--the regulations and how this is actually going to work.

So, I think there's a lot that needs to be worked out there. But I didn't see it as a greater effort to--to--to decouple or to accommodate.

LEWIS: Related to that, someone asked, "What sort of things do you think the Commerce Department will ban or could ban for TikTok under the EO?"

And one of the things I've been saying is IEPA gives the president a lot of authorities. There is perhaps some First Amendment issues, but where do you see the--how do you see the ban playing out? What do you think Commerce should do when they--when they implement this?

DEMERS: They shouldn't ban people embarrassing themselves on WeChat.

(LAUGHTER)

No, that would raise serious First Amendment concerns, so.

LEWIS: Yeah.

DEMERS: Now--

LEWIS: --No, sorry. That's permitted.

DEMERS: Exactly. You can always make a fool out of yourself.

LEWIS: That's right.

DEMERS: I think that look, I don't want to get ahead of where Commerce is with this. This is going to be--

LEWIS: --Yeah--

DEMERS: --A pretty quick process. We'll know the answers in September, but I--I don't want to get ahead of that process.

LEWIS: Okay. Someone came--that makes sense. Someone asked, "Can you give an example of TikTok collecting data for analytical purposes?"

Does--in--in the--the--I shouldn't be asking this one. I should've read it before I asked it. They said, "Is this what you think TikTok can do or do you have evidence that it's being done?"

I can answer that one for you if you want, but you should take it.

(LAUGHTER)

DEMERS: Look, it's certainly what TikTok can do.

(LAUGHTER)

It's not TikTok itself that we're worried about obviously. It's the Chinese government's access to the TikTok data under their National Security laws that we worry about.

And, you know, beyond that to what we know, then I--I just--I'm not going to get into that piece of it.

LEWIS: Yeah. Someone asked, "Given the scope of the problem, how much additional hiring has the U.S. achieved?"

I know when I go up to the Hill I always say more FBI agents in California. But are we expanding our efforts or are we expanding our personnel? What are we doing?

DEMERS: You know, I think we have. I mean, I--I can speak for the department. At Main Justice, we have certainly increased the number of prosecutors who work generally on that counterintelligence side of the house.

So, for many, many years, we have, you know, ramped up the counterterrorism prosecution side and had--

LEWIS: --Yeah--

DEMERS: --Less growth on the nation's state--countering nations' state right side. Over the last few years, as the terrorism threat, you know, let's all knock on wood that it sticks--has receded somewhat and the nation's state threat has amped up. Those are the two big differences. By the way, Jim, you know, when I was here from 2006-2009 when NST got started--

LEWIS: --Sure--

DEMERS: --It was a counterterrorism--

LEWIS: --Yeah--

DEMERS: --Organization. And coming back to it nine years later--

LEWIS: --Yeah--

DEMERS: --You know, seeing how much I've grown on the National Security side, the cyber work. So, we have definitely increased resources on that side. In the U.S. Attorney's offices, I think it's been more about a redeployment of resources than an increase in resources.

The Bureau has increased resources on the nation's state side. So, there has been an increase. Obviously, you know, Director Wray gave some pretty startling numbers about the number of Chinese investigative--counterintelligence investigations that are opening up each day.

So, there's--there has been an increase in resourcing this problem generally.

LEWIS: We have a few more questions. And so, if we can slide a little bit over on the time, I think we can hit--

DEMERS: --Yeah--

LEWIS: --Almost all of them. I'll stop taking questions now. But one of them is, "With the focus on Chinese," this is a good one, "focus on Chinese students and academics, do you see the Chinese coopting people from other countries--country--foreign students in academics of other nationalities who might be under less scrutiny?" Classic intelligence technique.

DEMERS: Yeah, it is. But it's also a lot harder to pull off--

LEWIS: --Yeah--

DEMERS: --Because if that foreign student isn't looking to get a job in China, and doesn't have a family in China, and has no ties to China, it's just that much less likely that they're going to be willing to be coopted.

It doesn't mean that they won't, you know, that it can't happen. People obviously susceptible to all sorts of inducements, right?

Usually financial. But it's that much harder. And look, we know, you know, a lot of what we're doing here every step of the way, you know, these are not silver bullets to end the problem. But we're trying to make the job a lot harder, right? So, when we extradited--

LEWIS: --Sure--

DEMERS: --That Intelligence officer from China, what was the significance of that? Obviously, we disrupted that one instance of intellectual property pathway. But the broader significance was that Europe was a place that Chinese Intelligence officers liked to meet Americans because they both felt safe there, right?

LEWIS: Right.

DEMERS: Chinese Intelligence officers don't want to come here. A lot of Americans who are being coopeted especially at the beginning felt nervous going to China. But you can meet in Europe. If the Chinese Intelligence officers don't feel safe doing that kind of activity in Europe following that extradition from Belgium, that's a broader disruption than that. Now that doesn't mean they can't do it, but it just makes their job that much harder.

LEWIS: So, we had a couple of questions on the Thousand Talents' Program. One of them is, "To how--what extent do you see the people recruited by the program? Is this according to the Chinese military or are the cases mainly commercial?"

DEMERS: Mainly it's been commercial, but I'd have to--I haven't sort of gone through the cases. But that's sort of at first blush, that's my impression has been mainly commercial. It's easier to do on the commercial side, but, you know, there's obviously a lot more controls on the military, technology and information.

But I wouldn't exclude it from the risks. But as I think about it, most of our cases have been on the commercial side.

LEWIS: What about other countries--particularly small countries that might have a strong high-tech industry in D.C. and not a Chinese (INAUDIBLE)?

I have a funny story to tell you about the Middle East after the call.

(LAUGHTER)

LEWIS: But what do you see on--what do you see outside the U.S. when it comes to Thousand Talents? Are we the primary target? Are they going after other high-tech sectors? What are the Chinese up to?

DEMERS: They're, no. Well, we're probably the primary target because that's where the bulk of that high-end technology is that they're interested in. But certainly, Europe is also a--a target.

And, you know, again, you--you---you step back and you look at that Made in China 2025 plan. If you go through those areas of technology, you know, you could figure out which countries have either companies, or professors, or institutions that are at the cutting edge of all of these different technologies. And there's definitely going to be, you know, a--a--any number of Europeans and European countries that fit into that--Japan, South Korea, etc.

So, it's not exclusive to the U.S. It is a means of developing China in part by taking technology from outside China.

LEWIS: So, we're--we're almost done. We just have a couple more questions if you'll bear with me.

I'll give you a break. Someone asked, "Is there any evidence of data surveillance being used to suppress ethnic and religious minorities such as the Uyghurs?" Yes.

Okay. The next question is--

(LAUGHTER)

You've got to be kidding me. This one's a little outside your bailiwick, but it touches on things that you--you pay attention to. "How do you think the administration is thinking about balancing the needs of the semiconductor industry that continue to sell commodity items to China with the need to close off maybe the high end?"

And so, when you think about Intel, Qualcomm, Micron, and the other guys, how can we--how can we find a balance in permitting safe sales to go?

I will say I was talking to someone from DOD who said there are no safe sales to China. A little extreme, but where do you think we're going to go with balancing controls and continued sales?

DEMERS: I mean, on that topic, I can say that that is a topic of discussion, you know, in the interagency. And I think, you know, I--I don't want to say--

LEWIS: --Yeah--

DEMERS: --Where I think they are headed in the future. I think, you know, it has been an issue that we have considered while we've had these policy discussions. And, you know, when I talk about sort of write--writing with a fine pencil, those are the kinds of distinctions I think that we could make and--but, you know. There are a lot of players in this.

LEWIS: So, two quick questions at the end. One is, "Can we expect more indictments for Chinese hacking this year?" That's a yes or no question. Now you can go a little further if you--

DEMERS: --Yes--

LEWIS: --Want. Okay.

DEMERS: Yes.

LEWIS: Good. So, yes.

(LAUGHTER)

Any predictions on when? No.

(LAUGHTER)

DEMERS: If I say it, it wouldn't be a prediction.

(LAUGHTER)

LEWIS: Yeah, that's right. That's right. So--so, what are the--and this will be the final question. What are the next steps you think for the Chinese initiatives? What? Where do you think? How's the momentum going? How's this expansion going? What are the things you're going to target on? Will they be additional things? What are the next steps for the China counterespionage initiatives?

DEMERS: I think look, this has been an initiative that sort of as I said, it was born kind of organically and it's developed organically from what we've seen in the cases and as we talked about, the academic side of things. I think we're going to continue to work with the universities. I think our work has been somewhat interrupted by coronavirus and our inability to do the same level of outreach and thinking we were in, you know, in--in the spring--as recently as the spring.

I think, but we're going to, you know. What I've appreciated is I think we've all--and this event proves that Jim is--we're starting to shift from the, "Well, let's delay that and, you know, see if we can do it in person later" to the "Let's just do it."

LEWIS: Yeah.

DEMERS: "And do it perfectly now."

LEWIS: Yeah.

DEMERS: Right?

LEWIS: I know.

DEMERS: And as we do that, our activity has sort of ramped up. And I appreciate getting back into that both on the private sector side, but especially on the academic side.

I, you know, I think, you know, that--that we continue with the cyber investigations and we continue on the traditional espionage side. I don't see any big new initiatives. But that's not really the way this has grown. It's just kind of--

LEWIS: --Yeah--

DEMERS: --Follow our investigative leads and--and let those leads take us to wherever we end up.

(LAUGHTER)

LEWIS: And that's kept you kind of busy.

DEMERS: Yeah.

LEWIS: It's--

DEMERS: --The ground is fertile, Jim.

(LAUGHTER)

LEWIS: Any final thoughts or words you'd like to leave the audience with?

My request is help me figure out how to persuade people that this is a major--perhaps the major national security problem for the U.S. What are your final thoughts on this?

DEMERS: Well, my final thought on that is think about the many, many, Jim, bipartisan issues that we are taking on at this time in the United States. You'll come up with a very short list, but China will be at the top of it.

So, that's how serious this issue is. That's, you know, how much the facts underpin, you know, everything I think that--that we've been saying and looking at.

And it's not that over time folks can't take different approaches to the problem. But I think there's a real appreciation that the problem is real and it needs to be addressed. And there is more, you know, just from my perspective, more sort of coalescing in the interagency process around this issue that I've seen.

And then, I saw the first time I was in government, you know, on--on--on--on these sets of issues, so. But I--look, thank you for all the attention that you're paying and thanks for putting on this event. It's always great to talk about these issues and, you know, I really appreciate you doing this despite all the--the technical issues that go along with this.

LEWIS: No, it's one of my favorite issues and I really appreciate you coming on. This has been very helpful.

I would--at this point, I would normally say please thank John Demers--John Demers--

(LAUGHTER)

--And wait for applause. But--

DEMERS: --Right--

LEWIS: --You'll just have to--you'll have to take my word for it that people are applauding.

(LAUGHTER)

Thank you for doing this.

DEMERS: Okay. Thanks a lot.

LEWIS: Okay, John. Thanks.

DEMERS: Appreciate it.

LEWIS: Yeah, talk to you later.

Load-Date: August 19, 2020
