The Honorable John C. Demers
Assistant U.S. Attorney General for National Security
Confronting Nation State Hackers and Cyberspies

Cyber Media Forum
Project for Media and National Security
George Washington School of Media and Public Affairs
Howard Baker Forum

28 April 2021

Moderator: Let me welcome all of the journalists and others who are on the call with us today. I'm David Ensor, Director of the Project for Media and National Security at the George Washington University. This is a session of something we're calling the Cyber Media Forum. The Project also runs something called the Defense Writers Group which has existed for 40 years and what we try to do is bring journalists together with knowledgeable officials and experts. Basically these are sort of beat reporter discussions with journalists who actually focus in on an area. This obviously we're focusing on cyber and cybersecurity and we're honored today to have the Assistant Attorney General for National Security of the United States Mr. John Demers as our guest. I'm going to chat with him for the first portion of this session and then we're going to open it to and I will recognize one by one journalists who are on the call to ask questions and you'll get a chance to ask a question and maybe a short follow-up.

Let me start, Mr. Demers, if I may by just asking you simply to describe to us what is the division. I know you were there at the creation of the division and then you went away and you came back and now you're running it. How would you describe its work and what are your front-burner issues?

Mr. Demers: Thanks very much, David. Thanks for organizing this. Thanks for having me on and thanks to all of you who I can't see right now but I know have joined and I look forward to your questions.

First on the National Security Division, and I'll focus obviously on the cyber component of it. Actually when we got started in 2006 as an outgrowth of the government's reorganization after the attacks of September 11th, this division was very much focused on counterterrorism. And that was the case throughout really the

time that I was here then. There were some areas we worked on on the cyber end including terrorist use of the internet but cyber issues were much less prevalent generally and certainly within the work of the division between 2006 and 2009.

Coming back to it, if you fast forward to 2018, obviously a lot has changed, both just generally in the world and in terms of everything that folks do on the internet these days but also on what criminal actors and what nation state actors will do to exploit the internet itself in a variety of ways which we can talk about.

So the division itself had reorganized in the meantime to reflect the changing nature of the threat and had created a section within it that focuses on nation states, cyber issues, and then some of the counterintelligence issues more broadly.

The real change though between 2006 and 2018 is that how much of my work in the last three and a half years or so has focused on the nation state threat and I think everyone knows that at the Department when we talk about the nation state threat we're primarily talking about China, Russia, Iran and North Korea. Then as a piece of that threat and as a way in which each of those actors has used its cyber capabilities to project its power, we have to work on the cyber activities, the maligned cyber activities of those four countries.

So the way we're organized for anyone who is less familiar with the way the Department's organized, the National Security Division on the cyber side deals with the nation state cyber threat; the Criminal Division deals with the more purely criminal actor cyber threat. So you'll see for instance that Ransomware, at least until recently, has been predominantly a criminal issue and therefore a Criminal Division issue, less so on the nation state cyber side. Although that is changing.

And of course we have to work closely together because oftentimes when we're first notified of a breach we don't know who the actors are, so we worked obviously closely and always with our partners in the Bureau. And again, the Bureau is organized slightly differently. They have a Cyber Division that covers both sides of the threat and they also have a National Security Branch and a Criminal Division, that those two have to coordinate with the Cyber Division because again, the threats are coming up

on both sides of it.

But this has been a big part, cyber's been a big part of our work here in the last three and a half years and before then and I think will continue to be a significant priority of the Department. We now have the Deputy Attorney General and the Principal Associate Deputy Attorney General, two former alums of this office, of this job. Specifically both of whom have spent much of their career both in the government and outside the government focused on cybersecurity and are very familiar with this area, and of course we've just had a spate of cyber intrusion all of which means that cyber will be at the forefront of the Department's agenda going forward over the next few years.

Moderator: Let me ask you first in terms of topics. The coverage of the U.S. response to SolarWinds focused on the attribution and the sanctions imposed by Treasury under the new executive order. But your piece of it didn't get too much attention. But it seems to me, if I'm reading it right, that it could be quite consequential. If I'm right, you're basically doing a sort of risk assessment on the entire Russian IT and telecommunications sector and companies that you refer to the Commerce Department because the pose an unacceptable risk in your view could be subject to what some would call a corporate death sentence by being put on the entities list.

Talk about that. How important is that? And tell us what it is precisely you're doing.

Mr. Demers: Sure. On that piece specifically, what we're seeing, and the SolarWinds hack is an excellent illustration of this, are what we call supply chain hacks. That's increasingly a method in which hackers are getting into the systems of companies and of the government.

So you have let's say the direct intrusions which are spearfishing campaigns, some way of getting the credentials of individuals who are in organizations and then entering that organization's IT system. Then you have the possibility, as you saw in SolarWinds, of hacking into a supplier of the ultimate customer or the ultimate target really, in order to introduce some kind of vulnerability often into software which then can be exploited once that software is downloaded onto the customer's network, whether it's the company or on the government side.

So we're seeing that increasingly. Some of the cases before then had also seen what I call a close cousin to this which is sort of the managed service provider hack which is you get into a company that's actually managing the IT services for a number of different companies so again, you're getting, in that case we analogize it to getting the keys from the superintendent of the building and then you can get into all the various apartments. The same thing on the supply chain side.

So as we look at the supply chain vulnerabilities we are undertaking an assessment under an executive order that was signed about a year and a half or two years ago to address supply chain vulnerabilities in the private sector procurement.

At the time it was signed I think everyone understood the focus to be on China and in fact some of the early investigations that the Commerce Department is engaged in do involve Chinese telecommunications companies. But it's not exclusively about China by any means.

So what we're looking at is whether there are vulnerabilities in the supply chain of U.S. companies that emanate from Russian companies. Or U.S. companies that have a significant back office presence in Russia, maybe doing software. And where a vulnerability could be introduced into the software because of where they are.

The important thing to keep in mind here is that these are not punitive sanctions in the same way that we think of the Treasury Department sanctions. This is meant to be protective. That is we're looking at the technology, we're looking at the vulnerabilities that may be introduced into that technology, we're looking at the significance of where those vulnerabilities will be introduced. And then we'll see whether we need to take, and the first step would be a referral to the Commerce Department based on our investigation, we'll see whether we need to take steps to mitigate those vulnerabilities. So it could be everything like you said, David. It could result in the company not being able to do business with a U.S. company or a company here in the United States. But there are also other mitigation measures that we could take and those will have to play out.

So think of it maybe as a hybrid between some of the sanctions regimes we have and the CFIUS regime where the answer isn't always oh, you've lost the acquisition, but maybe there are

mitigation measures to put in place. That could be licensing regimes. We'll just have to see when we get there. We are at basically our investigative stage that we're doing together with the FBI and pulling in the intelligence community at this stage. Then we would be making a referral to the Commerce Department which ultimately owns the authorities under this executive order.

But it is very much, to come back to the beginning, a response to the supply chain vulnerabilities that we see being exploited by nation state actors.

Moderator: There was reporting actually by Dustin Volz who I think is on the line with us now and maybe he'll come up with a question about this. I don't know. But that the DOJ is establishing a task force to combat Ransomware. You mentioned Ransomware earlier. Is this another area where you need to get creative and go after the middleman and the facilitators, try to take down the infrastructure and the financing? What new strategies are you going to employ and where will your division be involved in this?

Mr. Demers: We've seen, just as background, a very significant increase in Ransomware attacks. As I said, mainly on the criminal side because of the nature of the threat. Right? At the end of the day most of the time what the hacker wants is money. But we see Ransomware also being used on the nation state side to some extent now where maybe they don't just want money but they're trying to disrupt some activity of a government entity or maybe even a private company.

The Department has set up this Ransomware Task Force to take a look at this issue. It's going to be basically the Criminal Division, the National Security Division, the U.S. Attorneys Offices that are involved in this area, but it's also going to be training folks up so even if they're not currently involved as much on the cyber side, but making sure they have the expertise and the support to do these kinds of investigations in cases. And of course always our partners at the FBI to look at these strategies, to look at them holistically to see how to combat this Ransomware, working with international partners, working with our interagency partners and taking a look at the whole suite of activities that we have.

One of the things you'll have seen recently is, I mean I think what gets the most notice always in terms of the Department's

actions is the big indictments that we do. We've done several of those over the last few years. Again, covering all four of those nation state actors and covering non-nation state actors as well, from the Criminal Division. But there's a lot of work that the Department is doing to try to investigate, remediate and help the private sector protect against these threats. That is a little less visible, but you'll have seen it sort of in our use of the Rule 41 Criminal Search Warrant Authorities to take out the Hafnium web shells. You'll have seen it in sinkholes we've created for some Botnets. We've also used search warrant authority to try to map the victims of the Botnets so that they can be notified. We of course use our subpoena authority. Especially relevant when it comes to these third party hacks, so service providers or supply chain hacks. Again, always enabling the investigation of the hacks, the identification of the victims so that then the Bureau and DHS can work with those victims to root out the infiltration and to if need be to remediate what's happened.

So there's a lot of pieces and all of those will be part of this Ransomware Task Force and we'll see where it goes. But the idea is we all have a problem. It's a problem that's been getting worse which is Ransomware. There's been a lot of very visible examples of this including in some pretty high profile states and municipalities, and we need to be working as a department and then as an interagency on this issue.

Moderator: You mentioned web shells. Earlier this month of course the Justice Department got a court order in the Southern District of Texas that empowered it to essentially invade the code, the computer networks of some U.S. companies and to delete this one kind of malware.

There are dozens of such things out there. Can you tell us why you picked this one? Was it especially threatening in some way? And is this a tool that we're going to see used more frequently now?

Mr. Demers: I think it is a tool that we could see used more frequently. It's one that we'll use judiciously. If you look even in this case, there was a passage of time between the original identification of the malware and when we took our action and in that time many, many, many of the victims of the malware took the actions themselves to take these web shells out and to protect themselves.

But you get to a place where that's not happening for whatever reason with sort of the remaining in this case few hundred servers. And we have a decision to make which is are we going to go ahead and do that action ourselves or are we just going to leave that malware there sort of unremediated?

In this case, in part because we knew that although malware might have been put on there by one group, it was also being exploited by a number of different hackers that we should go ahead and take the web shells out and down.

We'll have to think through these very much on a case by case basis, but we have I think now, using the proper legal authority and being as transparent about it as we could and sort of putting out a press release that very day that described everything that we'd done and continuing to try to notify individual companies who might have been affected by our activity. So we're trying to do this openly, but this is a tool now that I think we have shown can be effective at least to some extent. None of these tools are silver bullets but we don't want to exclude the use of any tools in the appropriate circumstances because we need all of these together to try to combat the issues that we have right now with cyber intrusions.

Moderator: Let me quickly as you about the North Korean indictment in February. What's interesting seemed to be that associated indictments and plea agreements related to facilitators like [Caleb Al-Umari] and [lesser] facilitators like Ramon [Ualrunwa] Abbas, aka Ray Hushpuppi, who were accused of helping the North Korean hackers turn their ill-gotten crypto currency profits into cold currency through ATM cash-outs. Can you talk about the role these facilitators in global cybercrime and crime by a nation state, after all, and what plans do you have to go after them? Are they a weak point for the DPRK's efforts that you can profitably go after?

Mr. Demers: There's always a question when you in indict these nation states. Our first nation state indictment was back in 2014 and it was focused on a number of officers of the Peoples Liberation Army of China for theft of intellectual property. Sort of non-traditional espionage or military activity. And the question always comes up what effect do these indictments have? Why are you doing these nation state indictments when you can't arrest the hacker because the hacker belongs to another foreign

government?

I think part of the answer is illustrated in the case that you mentioned which is this latest North Korea case which is, some of these hacks and this is probably especially true in the North Korea example. The North Korea case illustrates sort of one, North Korea is and has been for a long time starved of hard currency so they use their cyber capabilities which are quite sophisticated and an asymmetrical tool obviously of nation state conflict. They use those in large part to get money. But when you get the money, you have to find a way to get it back to North Korea in sone usable form. So you need to be working with money launderers basically, in order to do that. Or the folks who were involved in this cash-out scheme which was literally going to ATM machines and pulling out cash. Right? Those people are often, as this case shows, not going to be in North Korea. Because you can't be in North Korea and do the ATM cash-out scheme, for instance, as an example. So they may be in countries where we can reach someone, where they are extraditable.

So in those cases I think it's a very useful form of disruption to be able to go after those facilitators, as you call them, of this scheme who are sort of necessary to the scheme itself, especially in the North Korean context.

Then more generally I think all our indictments over the course of the last now seven years have really helped to illustrate the problem, illustrate it to industry, illustrate it to our foreign partners, illustrate it to the American public at large and bring heightened awareness of these issues and to do attribution, which if you listen to some of the nation state responses they'll tell you I've been told by the Chinese, for example, wow, attribution is so hard. Of course you can never figure this out. Why do you even bother? It may sometimes be hard but we can figure it out and as you know, we attribute not to the nation state, we don't attribute to the military organization, we attribute down to the individual officer or contractor who's doing this work.

So I do think that some of these recent indictments show that we can also get some of these high figures. There's another indictment which we've extradited two folks from Malaysia. Again, there are countries where if folks are operating out of those countries we have better relationships than we do obviously in terms of extradition than we currently do with North Korea, China, Russia and Iran.

Moderator: I'm going to ask one more question and then I'm going to turn to folks who are on the line and try to recognize as many of you as we have time for, so think about what your question will be.

Let me ask you about China, Mr. Demers. Critics that I've heard from see two problems with DOJ's counterintelligence work on China. First, is there a danger - some think there might be - that counterintelligence concerns start to chill research by Chinese-Americans and start to spill over into ethnic witch hunts. People will remember the name Wen Ho Lee. Then there's the issue of trying to disentangle our critical supply chains from Chinese manufacturing. And really the question is how realistic it is to be able to do that and what the costs might be. Talk to us about those issues.

Mr. Demers: On both of those which I don't think are exclusive Justice Department issues, but sort of broader interagency issues to deal with. But to take them in order.

We are very sensitive to the possibility that our prosecutions of individuals who oftentimes will be either from China itself or perhaps be Chinese-American can lead folks to draw the wrong conclusion and we've tried to be very clear. Let's say with respect to students. We recognize there are about 360,000 Chinese students studying in the United States. We have never said that we shouldn't have Chinese students study in the United States. We think we should. We should remain open to Chinese students and researchers coming to the United States. We should really focus on those who are conducting illegal activity.

The good news is that when you focus on the activity and not, as you really can't do for a host of constitutional, even moral reasons on ethnicity, you capture people who are doing something wrong regardless of their motivation. So a company, for instance, that's focused on the insider threat, generally focused on where people may be physically on their campuses or digitally on their networks, is going to capture yes, perhaps, the person who's doing it for a nation state like China, but is also going to capture the person who's doing it for their own greed or for some competitor.

So it's really the practical and smart way to do this as well as the right way to approach this and that's what we have tried to

approach.

So if you look at our university cases, we're very focused on integrity and on individuals who have repeatedly not told the truth about the extent of their involvement with the Chinese government. The money that they've received from the Chinese government or Chinese universities, positions they hold in China, activities they've done here on behalf of those positions and the furtherance of those contracts.

So we're focused really on the folks who are hiding what they're doing.

We are not telling any university or any university professor don't do that, don't collaborate with China. You certainly can. What we're saying is when you do it, be open about it with the federal government funding agencies and be open about it with your university.

So I certainly understand the risk. And look, if you look through our cases you will find a lot of defendants who are not Chinese-Americans but are still acting on behalf of China. The Chinese are very ecumenical when it comes to who they will get to help them do their work and so you see that reflected in our cases as well. But there's a real problem out there and I think it is sophisticated, programmatic and persistent in nature when it comes out of China and that's really what we've been focused on without of course ignoring some of the other issues.

Moderator: Thank you.

Let me turn now to the journalists who are on the line and give them an opportunity to ask you questions. And I neglected to mention at the top and especially thank the Howard Baker Forum which is co-sponsoring this event and helping to make it possible. At the end of this I'll tell you about another session we're going to be having next month which I hope you'll all be interested in.

First, I'm just going to go to the list of people here and see which of you would like to ask questions.

Eric Geller of Politico. You're at the top of the list here. I see you're on; and then [Elisa Savenyes] will be next. Eric, do you have a question?

Journalist: Yes. Thanks so much. I appreciate it.

Last year, what seems like forever ago at RSA, I asked you a question about whether it's still reasonable to expect companies to self-attest to security conditions that they're meeting. I remember I said at what point do we decide look, the government's job in protecting Americans is easier and they're going to have fewer cases to investigate if tech companies have to meet the same kinds of safety standards that food and medicine companies do. And I looked at my notes and you said it may make sense at some point to become more actively engaged in making sure that these companies are complying.

We've obviously seen several major attacks since then which demonstrate that these companies that we rely on are not doing their due diligence.

Is it time now, particularly with the new administration that might be a bit more interested in this kind of thing, to look at applying the same logic to the tech industry? Particularly the software industry, that we apply to other critical industries in terms of regulation?

Mr. Demers: I think the new administration is taking a very holistic look at this issue and obviously came in just on the heels of the SolarWinds hack and then we've had others since then. And they're very focused on how we need to respond as a government and how we can work with our international partners on this response.

One of the areas, look it's still true that most of the time we find out about these intrusions from the private sector. Sometimes from the companies that have been intruded upon, other times through some of these private security companies, but the private sector remains a very valuable source of information and partner for us.

One of the issues that I think everyone is taking a look at is, are we going to have cyber breach legislation? What sort of legislative regime do we need to set up to provide the right environment for better self-reporting of these issues, which maybe is a slightly different issue than the specific one that you raised but it's related to it. I think on the one you raised, it will be a part of all of these discussions.

I think right now the thinking is very open about what the best way to handle these threats are, and we just get week after week illustrations of how much more we need to do about this issue.

At the end of the day I'd probably respond the same was as I did to you last time. You remembered that better than I did. But there is very much a moment right now when everyone's looking at what all the different approaches are and you've already seen sort of a closer partnership and a desire for closer partnership with the private sector in terms of the response and the remediation and the investigation. I think you will see other changes going forward.

Moderator: [Elisa Savenyes] of Bloomberg News, do you have a question?

Journalist: Yes, thank you so much for joining us.

So today we've talked about at least three kinds of attacks. There were the SolarWinds attacks, the Microsoft exchange attacks and Ransomware. I'm curious about your thoughts on differences in the legal strategy for deterring the hackers and people responsible for each of those different kinds of attacks.

Mr. Demers: With the supply chain compromises I think our legal strategy has to include what David and I were talking about in terms of looking at where the supply chain vulnerabilities are. That's more of a sort of ex-ante issue of addressing security of the supply chain up front.

In terms of how we then respond, there are slight differences in how we need to approach this. Obviously if it's a supply chain attack or a service provider attack. You have sort of a third entity. You have the ultimate victim, you have the sort of intermediate victim and then you have of course us who are all trying to work together to remediate this. We do have to take a slightly different sort of legal approach to that.

But again, in terms of deterring, deterring is ultimately about changing the motivation and raising the cost of somebody's act. One way of doing that, again, is through the supply chain review. You're basically telling a country if you prove yourself to be untrustworthy in cyberspace then we cannot trust your company when it comes to their work in cyberspace. So that is a way of

raising cost ultimately on the country. Of course a lot of the actions that the administration took to respond to the SolarWinds hack and other Russian maligned activity are also meant to raise the cost on a country. But they also have a second sort of salutary effect which is if there's any other country thinking about getting in this game, look at the cost that could be imposed on you because if countries start to think that hey, I actually could benefit from some of this myself then they may be willing to engage in this behavior and it may spread from those countries.

On the criminal side, it's sometimes easier because these criminal cyber hackers aren't just in these four countries but they're in countries around the world where we can effectively arrest and extradite those individuals, so you have a more traditional sort of law enforcement deterrent approach to those cases. And again as we talked about, on the nation state side very often if they're officers in the military, if they're intelligence officers, it's going to be very difficult to get them but we can try to go after some of the folks who are facilitating what they're doing outside the country.

At the end of the day on the criminal side what we have to do is how do you stop people from making money off what they're doing? The nation state is actually much more complicated because you have North Korea that's trying to make money but it also has other political objectives. The Chinese have other objectives whether it's developing their own industry, whether it's retaliating against something [like here], that's certainly true of the Russians. Whether it's just general political and military espionage.

Some of those objectives are very difficult to deter and that's just the world in which we live now. And then one worrisome thing we haven't talked about yet is those countries acting as safe harbors for cyber criminals in exchange for the cyber criminals doing work on their behalf as long as they don't target their own Chinese or Russian citizens.

On the legal side I think you'll see that our approach is very consistent but when it comes to deterrence the nation state problem I think is [inaudible] difficult because of the very mixed motivations.

Moderator: Let me turn next to Dustin Volz of the Wall Street

Journal and then after that will be Maggie Miller of The Hill. Dustin, do you have a question?

Journalist: Yes. Thanks. I do want to ask you about Ransomware and this is something I discussed a little bit with John Carlin as well. I think there's growing dialogue around the issue of whether or not some of these payments should be made illegal by Congress given, especially what you're talking about here with increasing awareness of nation state activity and nation state actions on some of these attacks.

I was just wondering if you have a view on that issue. Obviously the Justice Department has said for a long time its top priorities are helping victims and making sure they come forward so they can work with you. But this has been sort of considered somewhat analogous to terrorism payments. Obviously the victims in many cases are wildly different than what you might see in that area and that's something that [inaudible].

Mr. Demers: I certainly don't want to get ahead of all the review and thinking that's going to go on about Ransomware now. To some extent you can analogize them to the hostage payment that folks sometimes make. On the other hand if you look at sort of the Department's history of prosecutions, you won't see us having prosecuted many folks for making hostage or ransom payments.

I don't know about that one. We'll see how the thinking on that evolves. It could have the effect as you said, Dustin, of putting us in a more adversarial posture vis-à-vis the victims which is not where we want to be for other work in this space.

Moderator: Maggie Miller, The Hill. Then Joe Uchill will be next.

Journalist: Hi, thanks so much for holding this today.

I know that the newly announced Ransomware Task Force is going to be addressing some of the escalating Ransomware attacks on places such as hospitals, schools, other critical organizations. Can you detail a little bit more anything else the Justice Department may be doing to try to address specifically kind of this tide or wave of Ransomware attacks against the hospitals and schools that I feel like has just been building in the past year and has become such a critical problem.

Mr. Demers: Again, this is what the Ransomware Task Force will be looking at. So we need to have of course the same partnership with hospitals schools and other vulnerable sort of non-profits that we do with the private sector and the commercial sector.

A lot of times they're subject to the same sort of supply chain vulnerabilities but they're also subject to direct intrusions against them using more traditional methods like fishing or something like that. Some of them may not have the money or sophistication to have the cyber defenses that maybe some private sector entities do. Some certainly do and are as sophisticated as the most sophisticated private sector entity, but it varies certainly among them.

For the Bureau in the first instance to work with these entities, but at the end of the day it's often the same criminals who are targeting both one kind of entity and another kind of entity and so if we're focused on - we can work on the defensive protection side and certainly on the investigation and remediation side with schools and hospitals, but on the sort of investigations, sort or prosecution, deterrence side, if we're focused on the cyber criminals and their tools, their infrastructure, on the internet, I think we'll probably both the private sector victims and the public victims.

But it's a real worry, and especially thinking about hospitals. Then it's not just a money problem for them, that they have to pay these kind of ransoms, but if you've actually been able to lock up patient records or other capabilities staying in the hospital then it becomes actually a physical health problem for folks. That's something that I'm sure we'll be looking very carefully at as part of this task force.

Moderator: Joe Uchill of SC Media. Then after that the Washington Post.

Journalist: Thanks.

You mentioned that with Rule 41, you waited until, essentially you gave everyone a chance to correct the problem on their own, but this was such an overwhelming issue that you needed to go ahead with sort of a formal, a more aggressive measure.

I'm wondering in general are there formal criterial for these kinds of things, about what scenarios that would need to be met

to take this kind of aggressive action? Are there procedural standards beyond just getting a warrant that need to be met? What are they? And do you expect organizations like Europol who will take actions that affect the United States, companies, servers, to meet those same standards? Thank you.

Mr. Demers: I would say that is something we're still working through. It's not the first time we used a search warrant in a cyber operation. We've used them to map Botnets but we used them for something very similar to this activity in the past. But this is one of the very first times and this was something that was sort of discussed at the Bureau and here at the Department very thoroughly, but we don't yet have sort of worked out what our criteria are going to be going forward. Now that we've had this experience, that's the kind of discussion that we're having now internally. Again, I don't see this as a tool - it's not a tool of first resort that we're going to be using a couple of times a week as different intrusions come up. It does require working with the private sector in arriving at a solution. It does require testing to be sure that you're not going to otherwise disrupt someone's computer system.

Part of the reason obviously for the delay is just that. It takes a while to decide to do these and it takes a while to, on the technical side to make sure that you're doing it right, you're doing it very carefully and judiciously. So I see us going forward to sort of developing more formally a framework for when we would use these operations and what thresholds would have to be met, but that's what's happening now, sort of an after-action to what we did.

Moderator: We've got with us two Washington Post reporters, Tanya Riley and Erin Schaefer. So I don't know which one of you would like to ask a question or whether you both want to come on, but go ahead if you have a question please.

Journalist: Thanks so much.

I was going to ask about the cyber intelligence gap which we've heard a lot about from the leadership at the NSA and others. Is DOJ looking for expanded authorities to try to get more insight into U.S. networks? How are you trying to combat this and get more insight into these networks?

Mr. Demers: I think on the cyber intelligence gap, there are

different ways to try to fill the gap. One is for the government to have more authority to do this directly. That is to be sort of scanning at least aspects of these networks. Then the second is to encourage the private sector to be doing that and then making sure you have the right sort of legal environment for the private sector to come forward, whether it's intrusions they've detected or intrusions that they've in fact detected on their own networks to come forward to us so that we can then start working together on the investigation and the remediation piece of this.

I think that's the policy discussion that's going on right now which is what's the best way to fill this gap consistent with what we want the role of government to be, consistent with what we want the role of the private sector to be, and then how do we remove the sort of legal or liability disincentives to the private sector doing this work or sharing information with the government? How do we look at whether those have to be adjusted to some extent?

So we're involved in that broader conversation. I don't think is' settled yet anywhere specifically, but it's something, as you said, that folks are looking at carefully and not just sort of one part of the government, but the government as a whole.

Moderator: Eric Tucker of Associated Press. I see you're on. Do you have a question?

Journalist: Thank you so much for doing this. I appreciate it.

If I could return to the Rule 41 operation for a quick moment. I was wondering to what extent the Department or the Bureau had received any pushback from the civil liberties community and to what extent if you've had to mitigate any concerns that they might have raised. And if you have received concerns, what those concerns might be looking like.

Mr. Demers: I think you've seen some of those concerns expressed just in the press, in discussions of this operation and there are folks out there who are worried that the government without the permission of the entities that own the servers went ahead and did this remediation. Although of course we had court authorization so we weren't just able to do this on our own. We did have to go to a judge who authorized this activity.

And I get that. I don't think that's a silly question or issue

to raise at all. The problem is, the situation we were in where after several weeks you still had unremediated web shells ,that continued to be access points for hackers of all stripes into those systems. So the choice that the government had was just continue to leave those open or take the court-authorized action that we did and ultimately we decided to move ahead. But to the extent possible before then we had been notifying every victim that we could identify of the intrusion. We'd been working with the private sector side to patch all those vulnerabilities. So we did what we could, I think, with any identifiable victim before we took the action that we did.

So I understand the concern. On the other hand, the answer can't be well, you just have to keep watch as people - that continues to be a vulnerability on some of the systems.

Moderator: Mark Hosenball of Reuters, I see you're on. Do you have a question?

Journalist: What is the priority within the Justice Department of chasing down the intrusion cases and are you actually going to be seeking new legislation from Congress to pursue this stuff given the controversies about conducting investigations based on secret court decisions by the FISA court?

Mr. Demers: I don't know that we have conducted any cyber intrusion investigation based on a FISA court decision, and the FISA court matters are in my world, so I'm not sure what you're referring to there. The Rule 41 search warrant we used was a criminal authority, not a Foreign Intelligence Surveillance Authority.

I don't know that we see a need right now for new legislation when it comes to our investigations. As I talked about, there are discussions going on about whether more on the notification side of things from the private sector. But in terms of our investigative authorities, I think by and large we have what we need and we'll be able to continue to do these investigations. And as I mentioned, I see them continuing to be both on the criminal side and on the national security side, a priority of the current leadership.

Moderator: Del Wilbur of the Los Angeles Times. I see you're on. Do you have a question?

Okay, Ryan Lucas of NPR. Ryan, do you have a question?

Journalist: I wanted to ask you about the China Initiative which was obviously a big part of the Trump administration's Justice Department and your work. And we're now a little over three months in 100 days in I guess would be the best way to put it in the new administration. I'm wondering what changes you see or expect to see on that initiative going forward.

Also you've talked about this and we've talked about it, you've been very mindful about making clear to the public or attempting to make clear to the public that this is not about Chinese-Americans or Chinese people, but at the same point in time we have seen a rise in API hate incidents, something that's been very, a bit topic for Congress. They've taken action on it. And whether that factors in at all into adjustments that DOJ wants to make to the China Initiative.

Mr. Demers: Look, we continue to investigate and to bring cases, I've seen cases just in the recent weeks involving Chinese maligned activity in the U.S. including at universities and at companies. Just last week we had a guilty verdict in a China Initiative case involving the theft of some can lining technology and we charged some other cases at universities. So that work continues. It continues, as mindful as we were, and as you know, based on our other conversations that I've tried to be from the beginning on this about the risk of feeding into any narrative that would be harmful to Chinese-Americans or to innocent Chinese folks for sure. Focusing very much on the maligned activity of the government.

And if you look back at some of our China Initiative cases, you'll see at least two in the last six months where these cases have been ones where we have been trying to protect Chinese dissidents and others from the predatory activities of the Chinese government. So if you look at our case involving Operation Fox Hunt, that's about the Chinese government sending operatives here to try to pressure dissidents and others to return home to China to go to jail. So we're protecting the folks who are here. If you look at our case involving one of the big telecommunications platforms you'll see that we were charging an activity that was basically disrupting discussions with dissidents in the United States about Tiananmen Square, about Hong Kong and other topics about which the Chinese are very sensitive.

So that's an area, when you look at the future and where we could be working, that's an area where we are very interested in focusing as we continue to do sort of the economic espionage cases and the political/military espionage cases that we've been doing, is to focus on Chinese activity that is repressive of its own people here. And we see that among Chinese students at American universities. We see that surveillance that the Chinese government conducts of them. We've seen in this country reprisals when the student goes back to China based on things that Chinese students said, or cartoons that were drawn here in the U.S. at U.S. universities. We've seen U.S. universities respond to that by trying to make class participation on-line more anonymous in order to protect their students.

So that's an issue that we are focused on and we have talked to the FBI about how we can continue to develop that piece of the case. As I said, we're going to continue to prosecute these other cases as well that we've been prosecuting.

That's I think where we are in a nutshell. Obviously we'll be constantly reevaluating and responding to the threat. And of course on this issue of sort of hate crimes and violence against the API community, that's something that the department is taking very seriously and in particular the folks in the civil rights division are very focused on and will be working on.

I think that these two things can coexist and we have to keep our focus as we have been on the Chinese communist government itself.

Moderator: Ryan Lovelace of the Washington Times. I see you're on, do you have a question?

Hearing none, I'd like to ask one final question if I may. It's about encryption. I'm wondering whether it may not be – I'll be a little arch here just to make it more interesting.

Mr. Demers: Is this your Columbo moment, David?

Moderator: Yeah. [Laughter].

Isn't it time the Justice Department abandoned its Quixotic quest for a law enforcement back door? The Department had several years in the Obama administration. Even the President made it a priority and you weren't able to come up with a policy proposal

that could work because the bottom line is there can't be a back door for law enforcement that doesn't also work for hackers and spies. So isn't it time just to admit that far from going dark, we actually live in the golden age of surveillance. There's other ways to get information. Why not make yourself a hero and just declare that there's not going to be any back door?

Is that sufficiently Columboesque for you?

Mr. Demers: I don't know. He was a little more subtle, David. [Laughter].

This has been a very constant issue for all of us here certainly on the government side. We'll see where it goes from here.

I can only say look, from my perspective, and I understand all the different debates having been engaged in them to some extent. I can certainly see what encryption blinds us to on the investigative side. I see that in our national security cases. We're seeing that in our domestic violent extremist cases. So I certainly see the cost here, and whether we can work on a solution and work with Congress on a solution. I do think there was some movement on the Hill over the last year on this issue. We'll see if there's a workable solution here or not going forward. The new obviously leadership here, the new administration overall will have to decide what its position is going to be. As you said in the past both in the Obama administration and in the Trump administration folks on the government side tried to deal with this issue. Certainly no one discovered any great solution to this. But we'll see where it goes.

Moderator: Thank you very much, Mr. Demers, for being with us today. It's been a really interesting hour and I'm grateful to you. I hope we can do it again in the future.

And to those on the call, as I mentioned the Howard Baker Forum and we have another session planned. It's actually with Brandon Wales, the Acting Director of the Cyber Security and Infrastructure Security Agency at DHS. It will be on the 13th of May at 10 o'clock. At least that's the schedule. IT could change, but we will send all the people who are on this call an invitation and others and hope you will join us at that time.

Again, thank you very much, Mr. Demers, for a very interesting

hour.

Mr. Demers: Thank you.

Moderator: If you have any closing things you want to say, please fire away.

Mr. Demers: No. I think we've covered a lot. There's always a ton to cover but I'm very happy to have been here and very happy for all the questions. Feel free to reach out with other questions as well. Thanks very much, David. Thanks for putting this together.

Moderator: Thanks everybody.

# # # #