Press Releases: On the Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace

Special Briefing
John J. Sullivan

Deputy Secretary of State
Robert Palladino

Deputy Spokesperson

Robert L. Strayer, Deputy Assistant Secretary for Cyber and International Communications and Information Policy
Lotte New York Palace Hotel
New York, NY
September 28, 2018

MR PALLADINO: Thank you, again – all of you – for coming. Welcome today's roundtable discussion. We are privileged to have with us the Deputy Secretary of State John Sullivan. Deputy Secretary Sullivan will speak about this morning's ministerial meeting that he attended on advancing responsible state behavior in cyberspace. He has a few opening remarks and then he would be happy to take some questions. We are also joined by Deputy Assistant Secretary for Cyber and International Communications and Information Policy Robert Strayer. DAS Strayer will also be available for questions.

Today's briefing is on the record and off camera and embargoed until its completion. Thank you all for coming, and Deputy Secretary Sullivan.

DEPUTY SECRETARY SULLIVAN: Thanks, Robert. Hello, everyone. Happy to be here. This morning I hosted a meeting with like-minded countries on advancing responsible state behavior in cyberspace. Our goal is to deter malicious activity in cyberspace. The U.S.-led international effort seeks to promote and maintain an open, interoperable, reliable, and secure cyberspace.

During the meeting this morning we discussed strategies to confront cyber threats while maintaining the many benefits that free people and free nations have come to enjoy from the internet. The U.S.-promoted framework launched by President Trump last week for international cyber stability has three

components. First, responsible states must comply with their obligations under international law. Second, nonbinding norms of responsible behavior during peacetime provides important guidance to states, and we're looking to develop those. And third, implementation of political confidence-building measures can help bring stability to cyberspace.

Having said that, there must be consequences for states that act contrary to this framework. Today I called on like-minded partners to join the United States to work together to hold states accountable for their malicious cyber activity.

So with that short summary, I'm happy to turn it over to you and to take your questions. I don't know, Rob, if you have anything further you want to add.

MR STRAYER: Nothing more to add.

DEPUTY SECRETARY SULLIVAN: Great.

MR PALLADINO: Let's just start with Nirmal, please, from *The Straits Times*.

QUESTION: Yeah, *Straits Times*, yeah. Just – can I just ask your opinion on states that intervene actively in issues of cyber security and cyberspace, internet, internet social media platforms like Facebook, WhatsApp, et cetera – go in and actively regulate and intervene, which in some quarters is seen as contrary to the openness of those platforms on the internet? So what would – quite the opposite of the U.S. What would be your thoughts on that?

DEPUTY SECRETARY SULLIVAN: Well, the internet is – the cyber domain is an open system. The United States Government participates, the Department of State participates on Twitter, Instagram, Facebook, you name it. What we're talking about is action by nation-states that are contrary to the norms that have developed over time on appropriate use of cyberspace, which we saw in interference in the U.S. election in 2016, in cyber attacks that have been attributed over the last year and a half or so – WannaCry and Petya.

One of the things we talked about today at the ministerial was the work we need to define those – further define those norms and define those boundaries that states can't cross, and if they do cross, that there would be consequences and costly consequences for crossing those boundaries.

QUESTION: When you talk about consequences of those states that don't comply, could you talk about what kind of consequences? And in this case, since you mentioned it, what kind of consequences is Russia facing for meddling with the 2016 –

DEPUTY SECRETARY SULLIVAN: Well, we've already seen, both by statute and regulation, consequences that have been imposed on state actors that have engaged in inappropriate cyber activity. We announced recently our national cyber strategy, but while that strategy was being developed, it didn't mean that we were not actively protecting our cyber domain and imposing costs and consequences that – on those who have violated cyber norms. So we've attributed cyber attacks, we've imposed penalties on those responsible for those cyber attacks.

Our national cyber strategy, which we have adopted – it's the first one in 15 years that the United States has adopted. It really needed a – we really did need to update and embed our cyber strategy into our larger national security strategy. So it's an ongoing effort by the United States along with its allies and partners and like-minded countries to develop norms of behavior for states and others to use the cyber domain, and for those who breach those norms to have consequences imposed for that breach.

MR PALLADINO: Question.

DEPUTY SECRETARY SULLIVAN: Yes, sir.

QUESTION: Yeah. Did you discuss at all – there's – a lot of cyber attack is kind of like a grey zone attack, so did you discuss at all any kind of threshold of what would be considered, like, act of war through cyber?

DEPUTY SECRETARY SULLIVAN: Well, there – there's – what we spent – what we focused on today was, for the most part, cyber activities short of what we would characterize as a use of force, as an act of war. There are potential cyber activities that would be catastrophic and cause enormous loss of life and property damage, which would be the equivalent of an – be the – an act of war.

We're focused – we have means to respond to that, the President has, the United States has. What we focused most of our discussion on today was malign cyber activity that's short of a use of force, that's short of what everyone would consider an act of war. And that's where we're focused on defining norms of behavior, and through the UN with the GGE, the Group of Government Experts, which we hope to reconvene, to define norms of behavior that states will abide by and, if they don't, to impose consequences.

MR PALLADINO: Let's go to Bloomberg and Reuters.

QUESTION: Mr. Deputy Secretary, Nick Wadhams from Bloomberg. Just two questions. One is: Have you noticed any attacks or phishing attempts, or whatever it may be, ahead of the midterm elections? Is that – whether it's Russia or other adversaries, have you seen a spike in attacks or any concerns related to the midterms?

And just following on the President's comments on China, there was some confusion about whether he was just referring to these inserts in newspapers in Iowa when he was referring to Chinese meddling. Is there any evidence of Chinese cyber meddling ahead of the elections?

DEPUTY SECRETARY SULLIVAN: Well, I guess a couple of thoughts. First, I would say that we've been directed by the President, the entire Executive Branch, the U.S. Government, to be vigilant to protect our – both our election infrastructure and more generally our cyber domain not only for purposes of defending ourselves in anticipation of the midterm elections but in general protecting our cyber domain. We are – the United States is constantly, daily, almost minute by minute subject to attacks not necessarily by state actors, but non-state actors as well. So we are vigilant. I can't comment now on any

particular intelligence-related observations concerning attacks that would be directed at our midterm elections, but what I can say is that we have been directed by the President and everyone in the Executive Branch, and the U.S. Government is leaning far forward to protect the United States, to protect our election infrastructure, our cyber domain against all attacks, and in particular those that would be focused on the midterm elections.

QUESTION: But just to be clear, you can't say whether you have evidence of cyber attacks –

DEPUTY SECRETARY SULLIVAN: I would not discuss that in this context.

QUESTION: Okay.

MR PALLADINO: Lesley?

QUESTION: But in terms of the – sorry to interrupt – the second question, was Mr. Trump referring specifically to those newspaper inserts in Iowa?

DEPUTY SECRETARY SULLIVAN: You'd have to ask the White House for a clarification of the President's –

MR PALLADINO: The President at his press conference just two nights ago did say that more information would be coming out, so okay. Lesley?

QUESTION: Yes, Lesley Wroughton from Reuters. During this meeting, I mean, are you also going to be – are you – did you – was there any specific mention of very specific countries or actors that were part of this malign behavior?

DEPUTY SECRETARY SULLIVAN: Well, this meeting was focused on developing norms, systems, working through the UN and multilaterally on cyber infrastructure and protecting cyber infrastructure, making it resilient, imposing consequences for those who violate the norms that likeminded countries have adopted. This wasn't a discussion of particular cyber incidents or mal actors in the cyber domain. That wouldn't be something that would be discussed in this type of forum. It –

QUESTION: Okay. And what about actions against such players? Are you – is there agreement on what one does?

DEPUTY SECRETARY SULLIVAN: So we discussed today the concept of deterrence, which is embedded in our National Security Strategy and in particular our National Cyber Strategy, to impose costs and consequences on those state actors and non-state actors who seek to attack the United States, our allies and partners, our cyber infrastructure.

QUESTION: Now would that be sanctions?

DEPUTY SECRETARY SULLIVAN: It could be any number of tools that are available to the President, whether it's sanctions, diplomatic activity, offensive cyber activities by the United States. There's no – there's really a wide variety of tools that the President could employ depending on the nature of the attack that was made on the United States.

MR PALLADINO: Nikkei, Ken.

QUESTION: Yes, Ken Moriyasu from Nikkei. China has always been known for stealing corporate secrets through cyber hacks. Has the U.S. Government detected China's activity spreading into new areas, not necessarily elections, but do you feel that China's cyber activity is expanding? And is that the reason why the U.S. is looking for common norms, because it's not just Russia but all state players expanding?

DEPUTY SECRETARY SULLIVAN: Yeah, it's not just Russia, it's not just China; it's other countries as well, North Korea, Iran. We – it wasn't the focus of our discussion today, but it's certainly mentioned in our National Security Strategy and National Cyber Strategy that there are state actors that have targeted the United States. And that's been – that's discussed in the strategy documents, and we are – we're working hard to make our cyber domain more secure, more resilient, but also to deter that type of behavior by the range of responses that I mentioned, which would also include offensive cyber operations by the United States.

MR PALLADINO: Last one. We'll go back to you.

QUESTION: I work with W Radio Colombia, and Colombia was part of this meeting. Did you ask something of these allies more than just getting together to form some norms? Is there a back-and-forth, so you ask something of them and they ask something of you?

DEPUTY SECRETARY SULLIVAN: Well, there was an ask, and that is – and it's a substantial ask, that we work cooperatively with them in developing these norms. It's not – the United States is not declaring norms. We have our own ideas. We want to persuade others to see the – to value the internet that we do, the open, resilient internet that we're all hoping for, and we want to work with others multilaterally to develop those norms so that there is agreement across that wide range of countries from around the world that was in the meeting today about the importance of an open and resilient internet that is protected against state actors that don't necessarily share our values or our understanding of appropriate norms for cyber activity.

QUESTION: Can I just ask quickly where you're at with that?

MR PALLADINO: Last one.

QUESTION: I mean, where you're at with this discussion about norms?

DEPUTY SECRETARY SULLIVAN: Sure.

QUESTION: Is it the beginning, the middle, the end?

DEPUTY SECRETARY SULLIVAN: It's the middle, I would say. We have – we have had discussions with these – with many of the countries that were present in the meeting today. Those discussions continued with this meeting today and will continue going forward, including with the UN, who was represented at – the under secretary-general was there, and the UN has a role to play.

MR PALLADINO: Great. Deputy Secretary Sullivan, Deputy Assistant Secretary Strayer, thank you both so much for participating today. Thank you, all.

DEPUTY SECRETARY SULLIVAN: Thank you.