RESPONSES OF
JOHN C. DEMERS
ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

TO QUESTIONS FOR THE RECORD
ARISING FROM A HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ENTITLED
"CHINA'S NON-TRADITIONAL ESPIONAGE AGAINST THE UNITED STATES:
THE THREAT AND POTENTIAL POLICY RESPONSES"

DECEMBER 12, 2018

Questions from Senator Grassley:

1. I have taken a serious interest in how DOJ enforces the Foreign Agents Registration Act. In July 2017, I held a hearing on that very topic and later introduced legislation, the Disclosing Foreign Influence Act, to beef up DOJ's enforcement authorities. Recently, I wrote to the Department about China's Confucius Institutes. These Institutes are an arm of the Chinese government and are a propaganda outlet for them. Chinese officials have even admitted the point of the Institutes is pro-China propaganda and to project China's "soft power" overseas. FARA is not limited to lobbying work. It extends to propaganda. Since the Confucius Institutes are the Chinese government and are designed to spread pro-China propaganda in the United States, should they and their employees register under FARA? Please explain.

The Department is committed to enforcing the Foreign Agents Registration Act ("FARA") to the fullest extent of the law and is enhancing FARA enforcement, including by educating prosecutors and agents nationwide about the importance of the statute and how to investigate violations of it, and by increasing public awareness of FARA through additional outreach and making public our advisory opinions. In 2018 alone, the Department brought five criminal cases involving violations of FARA. And the number of new registrants and new foreign principals has almost doubled since 2015. To improve FARA enforcement, the Department has designated a deputy chief in the National Security Division to oversee both FARA registration administration and any criminal and civil investigations and litigation that arise from FARA enforcement.

Although I cannot comment here on the registration obligations of any particular entity, the Department is concerned about the potential threats to academic freedom and open discourse

from influence efforts on behalf of foreign governments at colleges and universities. The Department is aware of reports that student groups funded by the Chinese government have served as a vehicle for China to monitor Chinese students and visiting scholars while in the United States. Such groups could also serve as a means for the Chinese Communist Party to exert political influence and shape public opinion on campus. As part of the Department's China Initiative, the Department is educating higher education institutions about these threats and will apply FARA to unregistered entities seeking to advance China's political agenda.

2. Do you consider the Confucius Institutes to be a national security threat? Please explain what steps the Department has taken to monitor Confucius Institutes for foreign agent activity.

Consistent with longstanding Department of Justice policy, I cannot confirm or deny that there is investigative activity with respect to the Confucius Institutes, nor can I comment on the use of particular investigative techniques. But I can confirm that the Department is paying close attention to this issue and has urged colleges and universities to carefully examine their agreements regarding the operation of a Confucius Institute and to know the content of courses for students and the materials used. Over the last year, a number of campuses have chosen to close the Confucius Institutes.

3. I have requested the Department's FARA Lobbying Disclosure Assessment for many months. My staff have been told it exists but that they have to travel to the Justice Department to review it. It's not classified and thus I see no legitimate basis why you cannot send it to the Committee. Will you commit to sending it to the Committee?

The Department will work through our Office of Legislative Affairs to provide the FARA Lobbying Disclosure Assessment directly to your staff.

4. It has been reported that the Russians hacked and accessed DNC emails. Are you aware of whether the Chinese ever accessed any emails of the DNC, Hillary Clinton, her campaign, or her associates at any time?

The Department cannot comment on this in an unclassified response. The FBI will provide a separate, classified response.

5. In October of this year, I wrote a letter to the National Institutes of Health asking about the steps they have taken to ensure the integrity of taxpayer funded research. As you know, foreign governments, like China, have embedded their citizens in our research to steal our work product and take it back to their home country. Taxpayers deserve to know what you are doing to stop this from happening.

a. Have you found that China is a serious threat to the integrity of this country's publicly funded research?

The FBI will provide a separate answer addressing threats posed by China to publicly funded research.

As part of the China Initiative, the Department will educate institutions about the potential threats posed by Talent Recruits and the implications of participating in such a program.

b. Is the FBI interfacing with NIH and the Office of Security and Strategic Information at HHS to help stop foreign threats to the integrity of our research? If so, please describe the level of cooperation. If not, why not?

The FBI will provide a separate answer describing its ongoing partnership with NIH and HHS.

c. I understand that NIH depends substantially on research institutes to vet the researchers that are hired for publicly funded projects. Since taxpayer money is supporting these researchers, some of which are from foreign countries, what is the FBI doing to help research institutes vet foreign researchers?

The FBI will provide a separate answer describing its efforts to assist research institutes.

Questions from Senator Whitehouse:

(1) Please explain the structure and status of the Department of Justice operation designed to obtain judicial permission to take down botnets. Please include in your response where the operation is located within DOJ, how it is staffed and tasked, and the nature of this operation's interactions with relevant sections at the Department. What is your assessment of the operation's role and do you believe it has the authorities it needs to be effective?

The Department of Justice uses technical means, combined with the appropriate legal process, to combat botnets. Like other actions taken by law enforcement to disrupt ongoing, online criminal activity, actions to take down or otherwise disrupt botnets primarily occur as part of an ongoing criminal investigation. Operations targeting botnets are initiated in a variety of Department components. NSD, for example, would work with a partner United States Attorney's Office ("USAO") to obtain a search warrant or other court order necessary to disrupt a botnet operated by foreign military or intelligence services, or those acting at their behest. Alternatively, the Criminal Division will often act in the same role for botnets operated by criminal groups.

The warrants and orders allow the Federal Bureau of Investigation to, for example, collect the identifying and technical information needed to build a map of the botnet's infected computers and notify victims, or seize the botnet's command and control infrastructure from the

malicious actors. The Department can, in some cases, use the information collected to locate, apprehend, and charge suspects responsible for the botnet and for violating federal criminal law.

The Department's botnet takedown operations have been extremely successful and include dismantling Coreflood, Gameover Zeus, and Avalanche. Most recently, the Department announced an extensive effort to map and further disrupt the VPNFilter and Joanap botnets – global networks of infected computers under the control of Russia's military intelligence agency ("GRU") and North Korean hackers, respectively.

The Department's authority to take down botnets was enhanced by changes to the Federal Rules of Criminal Procedure that provided clear venue for a judge to issue warrants in connection with botnet investigations. The Department has also has worked with Congress on legislation to enhance federal law enforcement authorities to combat botnets. Specifically, the Department has supported two legislative proposals that would improve the Department's ability to counter the scale and sophistication of the threat posed by botnets.

First, the Department believes it should be illegal to sell or transfer surreptitious control over the botnet's infected computers to another person. This would allow the Department to investigate and prosecute not only those who create and use botnets to commit crimes, but also those who make money by selling access to the infected computers to other criminals.

Second, the Department supports expanding the reach of the civil injunction process. This powerful tool gives federal courts the authority to issue injunctions to stop the ongoing commission of certain crimes, such as fraud and illegal wiretapping. The Department used the process to help disrupt the Coreflood and Gameover Zeus botnets, which were being used to commit fraud against banks and bank customers. *See* U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE 69-71 (2018) (discussing the Department's efforts to disrupt botnets using civil authorities). Yet – depending on the facts of any given case – botnets can be used to engage in other illegal activity (such as stealing sensitive corporate information or hacking other computers) that may not constitute fraud or illegal wiretapping. Expanding the list of offenses eligible for injunctive relief to include operating a botnet would allow the Department to prevent the substantial harm caused by botnets, regardless of the category of crime being committed.

Questions from Senator Coons:

1. **I am concerned that we are not doing enough to combat persistent cyber intrusions from our adversaries, including China. There are many laws, such as the Computer Fraud and Abuse Act, that would allow law enforcement to identify, charge, and prosecute cyber criminals. Although it may be difficult to successfully extradite and prosecute individuals located in countries like China, there have been a number of cases where the U.S. has had success in arresting and extraditing cyber attackers from foreign countries.**

a. Do you agree that we should be more aggressive in using existing laws against cyber criminals located abroad, such as in China?

Since bringing criminal charges against five members of China's People's Liberation Army ("PLA") in 2014, the Department has been aggressively investigating and prosecuting state-sponsored criminal cyber activity. In the past calendar year, the Department has brought as many national security cyber cases against criminals acting on behalf of our major adversaries as in the prior five years combined; many of these cases have been brought against Chinese actors located abroad. The Department also continues its important work to hold foreign cyber criminals accountable, including those operating from within China.

Most recently in its pursuit of state sponsored criminal activity, on December 20, 2018, the Department unsealed an indictment charging two Chinese nationals with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. The indictment alleges that the defendants, acting in association with the Chinese Ministry of State Security ("MSS"), conducted global campaigns of computer intrusions that targeted, among other data, intellectual property and confidential business and technological information at managed service providers ("MSPs"), which are companies that remotely manage the information technology infrastructure of business and governments around the world. The indictment also accuses the defendants of engaging in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal hundreds of gigabytes of sensitive data and information.

As noted in my Statement for the Record, in October 2018, another Chinese intelligence officer from the MSS's Jiangsu Province Ministry of State Security ("JSSD"), Yanjun Xu, was extradited to the United States and charged with attempting to co-opt an employee of a defense contractor to steal trade secrets related to commercial airplane engines. This extradition was unprecedented and reflected the close cooperation with our foreign law enforcement partners in Belgium.

Shortly thereafter, the Department charged ten defendants, including JSSD intelligence officers and hackers as well as company insiders working at the JSSD's behest, with conspiring to hack U.S. and French defense and aerospace contractors. As with their colleague Xu, their aim was to steal aerospace-related information, specifically technology that could be used to develop a rival Chinese version of a commercial airplane turbofan engine.

Although our goal is always to hold accountable in court those we charge with trade theft or cybercrimes, criminal investigations can also provide critical support for civil and economic tools that deprive criminals located abroad of the benefits of their crimes. For instance, on November 1, 2018, a grand jury in San Francisco returned an indictment alleging that a Chinese state-owned company, a Taiwanese company, and three Taiwanese individuals engaged in a scheme to steal trade secrets from Micron, an Idaho-based semi-conductor company. The defendants are alleged to have used the information for the benefit of a

company controlled by the Chinese government. The Department also filed a civil action to seek an injunction to prevent the Chinese and Taiwanese companies from transferring the stolen technology, or exporting products based on it to the United States. And based in part on our investigation, shortly before the criminal charges were unsealed, the Commerce Department added the Chinese company to the Entity List to prevent it from buying goods and services in the United States.

Our charges also provide a means of rallying like-minded nations to confront an adversary, to reinforce the difference between acceptable state behavior, on the one hand, and that which is inconsistent with voluntary, non-binding norms of responsible state behavior in cyberspace. For example, in relation to the MSP investigation referenced above, the Department's criminal charges were accompanied by supportive, public statements from nearly a dozen like-minded nations condemning cyber-enabled theft of intellectual property.

The Department is also aggressively working to investigate and prosecute cyber criminals operating from within China even in instances where there are no accusations that they were working at the behest of Chinese intelligence services. On May 7, 2019, a federal grand jury returned an indictment charging a Chinese national as part of an extremely sophisticated hacking group operating in China and targeting large businesses in the United States, including through a computer intrusion and data breach of Indianapolis-based health insurer Anthem Inc. (Anthem). The indictment accuses Fujie Wang and other members of the hacking group, including another individual charged as John Doe, of conducting a campaign of intrusions into U.S.-based computer systems. As part of the computer intrusion and data breach of Anthem, the defendants allegedly identified and ultimately stole personally identifiable information and other data concerning approximately 78.8 million persons from Anthem's computer network.

On January 24, 2018, Sinovel Wind Group Co. Ltd., a Chinese manufacturer and exporter of wind turbines, was convicted of conspiracy to commit trade secret theft, theft of trade secrets, and wire fraud for victimizing AMSC, a U.S.-based company formerly known as American Superconductor Inc. As proven at trial, Sinovel stole proprietary wind turbine technology from AMSC in order to produce its own turbines powered by the stolen intellectual property. At the time of the theft, Sinovel owed AMSC more than $100 million for wind turbine parts it had already received and had contracted with AMSC for more than $700 million in products and services to be used for the wind turbines that Sinovel manufactured, sold, and serviced. After stealing AMSC's technology, Sinovel never paid AMSC for the more than $800 million in products and services owed or under contract. Evidence was presented at trial that Sinovel's theft caused AMSC's stock value to decline by more than $1.2 billion, forcing AMSC to lay-off 70% of its workforce. On July 6, 2018, the sentencing court imposed the maximum statutory fine in the amount of $1.5 million on Sinovel, and ordered it to pay a total of over $58 million in restitution to AMSC and other victims.

The Department will continue to aggressively investigate and pursue cyber criminals abroad, and will leverage the Department's China Initiative to help identify priority Chinese trade theft cases.

b. Does law enforcement have sufficient resources to prioritize investigation and prosecution of these cyber-crimes? Where would additional resources have the most impact?

The Department is committed to prioritizing the investigation and prosecution of cybercrimes and related nation-state counterintelligence efforts and, accordingly, has sought further personnel funding. As set forth in the FY 2020 President's Budget Request for the Department of Justice, we have requested $72.5 million to strengthen our cyber capabilities and $24.7 million to further the Department's counterintelligence efforts including cybercrimes and our Foreign Investment Review Section asset protection work. Additionally, the Department's China Initiative will be a key factor in ensuring that such cases are adequately resourced and staffed.

2. What is your assessment of federal law enforcement's ability to attribute specific cyber- crimes to the individual actors who committed the attacks?

The Department's recent and growing number of prosecutions against nation-state actors reflects our increasingly sophisticated ability to attribute criminal conduct to the individuals and states involved. Our ability to do this in court with unclassified evidence is a result of the commitment of law enforcement and our ability to match the adversaries' evolutions in tradecraft and sophistication with our own evolutions in unclassified attribution sources and methods. Our ability to do so, however, will require continued dialogue and partnership with the private sector, which manages the vast majority of the Internet's infrastructure and services, to ensure that investigators have access (supported by legal process as necessary) to threat data in those partners' possession.

3. Your written testimony highlights efforts by foreign governments, like China, to obtain detailed personal information including health and other sensitive electronic information that can be used to target individuals for espionage. It is now publicly reported that a cyberattack on the Marriott hotel chain that collected personal details of roughly 500 million guests was part of a Chinese intelligence-gathering effort. As we continue to consider new privacy legislation, are there reforms that the Department of Justice recommend we consider and include to help keep sensitive personal information out of the hands of foreign governments?

The Department has increasingly recognized that access to personal information can be a national security concern. *See* U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE 26-28 (2018). As we have advised this Committee on prior occasions, the Computer Fraud and Abuse Act ("CFAA") needs to be updated to make sure that

it continues to appropriately deter violations of Americans' privacy and security.[1] Among other things, legislative reform is required to better protect against insider threats, make CFAA and certain Wiretap Act offenses subject to the Racketeer Influenced and Corrupt Organizations Act, expand the availability of civil injunctive relief to cover botnets (which may steal personal information), and punish the sale and rental of criminal botnets. The Department would welcome the opportunity to provide technical assistance on drafts of legislation, or work with Congress to clarify or expand our laws to provide law enforcement with new tools or sharpen existing ones, as appropriate.

Questions from Senator Blumenthal:

1. **Mr. Meng Hongwei mysteriously disappeared in China at the end of September. At the time of his disappearance, Mr. Meng was the President of the International Criminal Police Organization – INTERPOL – and sent only a single knife emoji to his wife, which was their signal for danger, to indicate that he was in trouble. The Chinese government later admitted that Mr. Meng was arrested on "undefined corruption charges," becoming the latest victim in a broader practice of purging political dissidents in China. INTERPOL then accepted a reportedly unsigned letter of resignation from Mr. Meng, and quickly moved on to select a successor.**

    a. **What is the Department of Justice doing to secure the release of Mr. Meng?**

The Department is aware of the reports concerning Meng Hongwei's disappearance, as well as China's broader efforts to purge political dissidents. The Department is particularly concerned with China's coercive efforts to pressure Chinese expatriates to return home. The Department and FBI continue to work with others in the interagency to track, monitor, and thwart Chinese government agents operating secretly in the United States for this and other purposes.

    b. **How does this event factor into U.S. efforts to confront non-traditional Chinese tactics of espionage and destabilization?**

The disappearance of Meng Hongwei may increase China's perceived power in the eyes of Chinese nationals, especially those working in targeted technology sectors of the United States. As a result, these students, scientists, or researchers may be more vulnerable to pressure or recruitment by Chinese intelligence agencies to engage in illicit technology transfer. The Department, including the FBI, will continue to work with the private sector, universities, and foreign partners to assist them in their efforts to protect intellectual property and provide awareness training that will help them recognize and respond to suspicious behavior.

---

[1] *See* Statement of Sujit Raman, Associate Deputy Attorney General, at a Hearing Entitled "Cyber Threats to Our Nation's Critical Infrastructure," Subcommittee on Crime and Terrorism, Committee on the Judiciary, United States Senate (Aug. 21, 2018), available at https://www.judiciary.senate.gov/imo/media/doc/08-21-18%20Raman%20Testimony.PDF.

2. **Following the arrest of Meng Wanzhou, the Chief Financial Officer of Huawei, the president suggested that he would intervene in her case. His suggestion that he would intervene to block action by the Department of Justice either in that extradition proceeding or in the underlying criminal action is extremely disturbing to me and may be to others in the law enforcement community. Acknowledging that you cannot comment on a pending criminal proceeding, I ask:**

   a. **Were you consulted before President Trump said he might intervene in Ms. Meng's case?**

No, I was not consulted. Because this is a pending matter, I am not in a position to comment further.