

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE
8, 2016

Thursday, December

Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues

Joint Summary of Outcomes

Yesterday, Attorney General Loretta E. Lynch and Department of Homeland Security Secretary Jeh Johnson, together with Chinese State Councilor and Minister of the Ministry of Public Security Guo Shengkun, co-chaired the third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues. The dialogue aims to review the timeliness and quality of responses to requests for information and assistance with respect to cybercrime or other malicious cyber activities and to enhance pragmatic bilateral cooperation with regard to cybercrime, network protection and other related issues.

Both sides endorse the establishment of the dialogue mechanism as beneficial to bilateral communication and enhanced cooperation, and believe that further solidifying, developing and maintaining the dialogue mechanism and continuing to strengthen bilateral cooperation in cybersecurity is beneficial to mutual interests.

The outcomes of the third dialogue are listed as below:

1. **Combatting Cybercrime and Cyber-Enabled Crime.** Both sides re-commit to cooperate on the investigation of cyber crimes and malicious cyber activities emanating from China or the United States and to refrain from cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. To that end, both sides:

Plan to continue the mechanism of the “Status Report on U.S./China Cybercrime Cases” to evaluate the effectiveness of case cooperation.

Affirm that both sides intend to focus cooperation on hacking and cyber-enabled fraud cases, share cybercrime-related leads and information with each other in a timely manner, and determine priority cases for continued law enforcement cooperation. Both sides intend to continue cooperation on cases involving online distribution of child pornography. Both sides seek to expand cyber-enabled crime cooperation to counter Darkweb marketplaces’ illicit sale of synthetic drugs and firearms.

Seek to provide concrete and timely updates on cases brought within the ambit of the dialogue.

Exchanged views on existing channels of multilateral cooperation, and intend to continue exchanges regarding this topic.

2. Network Protection. Both sides acknowledged the network protection seminar held in August 2016 in China, and believe that enhancing network protection is beneficial to both sides. Both sides suggest holding regular network protection working-level meetings, either remotely or in-person, the next of which should be planned for 2017. Both sides seek to promote the protection of our respective networks through multiple methods. To that end, both sides:

Plan to enhance network hygiene by promoting the cleaning and patching of malware infections in our respective networks and promoting best network protection practices.

Propose to engage in regular reciprocal sharing of malicious IP addresses, malware samples, analytic products, and other network protection information, and to develop standard operating procedures to guide network protection cooperation.

Seek to assess the effectiveness of information shared and provide substantive feedback to each side regarding the utility of that information.

Plan to provide Principals with regular summaries of network protection cooperation.

Intend to continue discussion on future cooperation concerning cybersecurity of critical infrastructure, and to provide timely assistance on cybersecurity incidents impacting critical infrastructure.

Intend to hold, as early as possible in 2017, a U.S.-China government and technology company roundtable to discuss cybersecurity issues of mutual concern.

3. Misuse of Technology and Communications to Facilitate Violent Terrorist Activities. Both sides acknowledged the seminar on misuse of technology and communications to facilitate violent acts of terrorism held in November 2016 in China, and decided to continue cooperation on information sharing in countering the use of the Internet for terrorist and other criminal purposes. Both sides will consider holding a second seminar in 2017.

4. Hotline Mechanism. Both sides welcomed the launch of the U.S.-China Cybercrime and Related Issues Hotline Mechanism, and decided to continue to use the hotline in accordance with the Work Plan. Both sides will conduct routine review of the use of the hotline.

5. Dialogue Continuity. Both sides recommend that the dialogue continue to be held each year, and that the fourth dialogue occur in 2017.