CRS INSIGHT

U.S.–China Cyber Agreement

October 16, 2015 (IN10376)

Related Author

- John W. Rollins

John W. Rollins, Coordinator, Specialist in Terrorism and National Security (jrollins@crs.loc.gov, 7-5529)
Susan V. Lawrence, Specialist in Asian Affairs (slawrence@crs.loc.gov, 7-2577)
Dianne E. Rennack, Specialist in Foreign Policy Legislation (drennack@crs.loc.gov, 7-7608)
Catherine A. Theohary, Specialist in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844)

U.S.-China Cyber Agreement

During the state visit on September 24-25, 2015, President Xi Jinping of China and President Barack Obama reached a Cyber Agreement. Soon after, the White House released details contained in the agreement. In principle, the United States and China agreed, among other things, to

- provide timely responses to requests for information and assistance concerning malicious cyber activities,
- refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property,
- pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community, and
- establish a high-level joint dialogue mechanism on fighting cybercrime and related issues.

U.S. Claims of Chinese Unauthorized Computer Access

Accusations of China's pursuit of cyber-capabilities directed at U.S. security interests have persisted for decades. Reportedly, many U.S. investigations of Chinese government and suspected quasi-affiliated entities have focused on unauthorized access to both U.S. government and private-sector databases for purposes of economic espionage. On May 19, 2014, the U.S. Department of Justice indicted five Chinese military hackers for computer hacking and economic espionage directed at six American entities in the U.S. nuclear power, metals, and solar products industries. In discussing the details related to this indictment, U.S. Attorney General Eric Holder stated, "This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking."

U.S. and Chinese Statements

President Obama stated on September 16, before the state visit, that his Administration viewed alleged Chinese cyber theft of trade secrets as "an act of aggression that has to stop." He warned, that the U.S. government is "prepared to [impose] some countervailing actions to get their [China's] attention."

The statement contained in the Cyber Agreement that neither government will knowingly support cyber-enabled theft of intellectual property for commercial gain appeared to signal Chinese acceptance, for the first time, of the distinction the U.S. government draws between cyber intrusions for national security purposes and activities pursued for commercial benefit. President Xi lent his personal imprimatur to the pledge not to support commercial cyber espionage by stating that "... both government[s] will not be engaged in or knowingly support online theft of intellectual properties," and by declaring in a speech in Seattle three days earlier that "the Chinese government will not, in whatever form, engage in commercial theft or encourage or support such attempts by anyone." Some observers have noted that a troublesome aspect of the Cyber Agreement, however, is that it may not reflect the intentions of the People's Liberation Army.

In response to a question about whether he was satisfied with China's steps on cybersecurity, President Obama said that the United States has traditional law enforcement tools available to "go after those who are attacking our companies or trying to extract trade secrets and data," and, through an executive order issued in April 2015, also has the ability to impose sanctions.

Sanctions

On April 1, 2015, President Obama signed Executive Order 13694 finding "that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." Declaring that the circumstances constitute a national emergency, the President ordered the Department of the Treasury to block all property and interests in property under U.S. jurisdiction of any person or entity that the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, finds responsible for or complicit in a cyber-enabled activity that compromises any computer or network that serves a U.S. critical infrastructure sector, harms a critical infrastructure sector, disrupts the availability of a computer or network, or causes "a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.... " The President further determined that any designated person will be denied entry into the United States. To date, no persons or entities have been designated and made subject to economic and travel restrictions under this order. Prior to President Xi's state visit, however, media reports suggest "the Chinese arrested a handful of hackers at the urging of the U.S. government" in anticipation of Chinese hacking of U.S. entities related-issues to be discussed with President Obama.

International Cyber Agreements and Norms

The intent of an entity's use of a cyber-capability appears to be a factor in the development of international laws and norms in cyberspace. Discussing the different types and purposes of software code being developed and used by various nations, U.S. State Department Coordinator for Cyber Issues, Chris Painter, stated in October 2015, "I don't know what (a) cyberarm is. A piece of (software code) could be used for malicious, research, or defense purposes."

Many existing international instruments have implications for cybersecurity, including those relating to law enforcement, defense, and security, along with treaties, conventions, and agreements, such as the United Nations Charter and the Geneva Conventions. The Council of Europe Convention on Cybercrime, also known as the *Budapest Convention*, is a law-enforcement treaty that requires signatories to adopt criminal laws against specified types of activities in cyberspace, empower law-enforcement agencies to investigate such activities, and cooperate with other signatories. The *Convention* focuses on identification and punishment of criminals rather than prevention of cybercrime. Consequently, it may act as a deterrent, but it has no remediating effect on the criminal acts that do occur. While widely cited as the most substantive international agreement relating to cybersecurity, some observers regard it as unsuccessful. While the United States has ratified it, China is not a signatory. China and the United States are members of the UN Group of Governmental Experts, which focuses on cooperative cybersecurity and norm development. Likewise, both nations have worked with the Association of Southeast Asian Nations (ASEAN) to strengthen cooperation in combatting cybercrime.