Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China

June 15, 2015

Dirksen Senate Office Building Room 608
Washington, DC 20510

Paul M. Tiao
Partner, Hunton & Williams LLP
Testimony before the U.S. – China Economic and Security Review Commission

Chairman Reinsch, Vice-Chairman Shea, and other Members of the U.S. – China Economic and Security Review Commission, thank you very much for the opportunity to appear today to testify at this important hearing. My name is Paul Tiao. I am a Partner at Hunton & Williams LLP, where I am a member of the firm's Global Privacy and Cybersecurity Practice and Co-Chair of the firm's multi-disciplinary Energy Sector Security Team. I advise energy, healthcare, financial, transportation, communications and other companies on cyber and physical security preparedness, incident response, statutory and regulatory compliance, investigations, law enforcement, litigation, and public policy issues. Prior to joining Hunton & Williams in 2013, I served in the federal government for fifteen years as Senior Counselor for Cybersecurity and Technology to the Director of the Federal Bureau of Investigation, Judiciary Committee Counsel to the Assistant Majority Leader in the U.S. Senate, Assistant U.S. Attorney in the District of Maryland, and Trial Attorney at the Department of Justice. I am an adjunct professor of cybersecurity law and policy at George Washington University, and an instructor at the National Institute for Trial Advocacy. I currently serve on the Virginia Cybersecurity Commission, which was established by Governor Terry McAuliffe last year.

I commend the Commission for focusing on China's commercial cyber espionage threat. This threat presents one of the most significant economic and national security challenges facing the U.S. As discussed below, the nature of this threat has been documented in detail in recent private and government publications, the cost to U.S. industry is significant and growing, and the need for effective deterrent action by the government and the private sector is urgent.

As documented in reports published by leading network security and digital forensic investigative companies, reports issued from the federal government, statements by the President and senior public officials, and indictments announced by the U.S. Department of Justice, the Chinese government has engaged in a systematic program of commercial cyber espionage designed to advance the economic and industrial goals described in its 12th Five-year Plan. Issued in 2011, China's 12th Five-year Plan prioritizes growth in certain industries, including nuclear, wind and solar energy, energy conservation and environmental protection, drugs and medical devices, rare earth and high-end semi-conductors, information technology, aerospace, telecommunications, and clean energy vehicles.[1] According to the U.S. government, "Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical

[1] KPMG, *China's 12th Five-Year Plan: Overview* (Mar. 2011).

advancement, and growth of the renewable energy sector."[2] Consistent with these goals, the Chinese government, through the People's Liberation Army (PLA), has developed an extensive computer network operations program that is systematically stealing vast stores of intellectual property, business sensitive information, and personal information from U.S. companies in these and other economic sectors.[3] Targeting these technologies and business information enables China's domestic companies to rapidly make "leap frog" technical developments and develop from favorable positions in business negotiations, thus expediting their growth into global market leaders.[4] The PLA's cyber command – housed in the PLA General Staff Department (3rd Department) – is estimated to have more than 100,000 personnel divided among 12 bureaus, three research institutes, and 16 regional and functional bureaus.[5] As detailed by Mandiant in a 2013 report featuring just one of those bureaus, a single PLA hacking unit was responsible for the theft of hundreds of terabytes of data from at least 141 organizations (115 of which are based in the U.S.) representing 20 major industries between 2006 and 2013, with the emphasis on industries prioritized in the 12th Five-year Plan.[6]

Commonly described as an Advanced Persistent Threat, the PLA's method of attacking a target company typically includes the following stages: 1) initial reconnaissance for the purpose of collecting information about the target company and its network environment; 2) initial compromise of the target's network, often through the use of spear phishing, strategic web compromises, and other social engineering tactics; 3) establishment of a foothold that ensures control of the target's network from outside of the network; 4) a cycle of privilege escalation that is designed to give the hacker expanded access within the network, internal reconnaissance of the target's network, lateral movement of the hacker within the network, and actions to ensure continued, long-term control over key systems in the network; and 5) completion of the mission through exfiltration of the desired data to the Chinese government via a series of compromised computers ("hop points") in the U.S. and around the world.[7]

The organized nature of the PLA's commercial espionage campaign complicates network defense efforts for U.S. companies, as PLA actors share techniques among different hacking units, and continuously develop, modify and improve on their malware tools.[8] In addition, the social engineering methods used by the PLA to compromise victim networks have become increasingly difficult to stop as hackers have become more sophisticated and corporate executives increasingly reveal details about their personal and professional lives on social media sites. For example, PLA hackers often leverage current or upcoming industry conferences in sending highly-tailored spear-phishing emails regarding specific topics to individuals who will

---

[2] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace* (Oct. 2011).

[3] Northrup Grumman, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage (prepared for the U.S. – China Economic and Security Review Commission)* (Mar. 2012); Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013) (hereinafter, "Mandiant 2013 APT1 Report").

[4] CrowdStrike, *Global Threat Intel Report* (2014).

[5] Mandiant 2013 APT1 Report.

[6] *Id.*

[7] Mandiant 2013 APT1 Report; CrowdStrike, *Global Threat Intel Report* (2014); Verizon, *2015 Data Breach Investigations Report*.

[8] CrowdStrike, *Global Threat Intel Report* (2014).

likely attend the conference, or compromise the website devoted to that conference in order to infect individuals who visit that website with malware.[9] The recent data breaches involving personal information held by two major health insurance companies, as well as the breach of federal employee data held by the U.S. Office of Personnel Management are widely believed to be attributable to Chinese hackers.[10] If in fact that is the case, then the details about each affected individual's healthcare information and the information regarding the background checks, security clearances, job assignments, job performance and training of affected federal employees would provide Chinese actors with a treasure trove of information for use in spear phishing attacks.

The economic costs associated with the Chinese government's commercial cyber espionage campaign takes on a variety of forms, including the:

- Loss of intellectual property to a potential Chinese competitor that may be able to use it to develop and sell a competing product or reduce R&D costs;
- Reduced incentives for technological innovation by targeted companies;
- Loss of confidential business sensitive information that may, for example, be used by a Chinese company to underbid the victim for a lucrative contract or undermine the victim's strategy in business negotiations;
- Opportunity costs in the form of service and employment disruptions, lost sales and revenues, and reduced trust in and use of online commercial activities;
- Costs of securing networks, insurance and recovery from cyber attacks;
- Legal fees associated with breach-related litigation and government enforcement actions; and
- Reputational harm suffered by the victim company and reduced stock prices.[11]

The nature of these costs are illustrated in the ground-breaking indictment announced by the U.S. Department Justice against five PLA hackers in May 2014. The indictment details the ways in which the PLA used hacking methods to engage in commercial espionage for the benefit of Chinese industries and to the detriment of several U.S. companies, including Westinghouse, SolarWorld, U.S. Steel and Allegheny Technologies, Inc.[12]

- In 2010, while Westinghouse was building four power plants in China and negotiating other terms of the construction with a Chinese state-owned enterprise, including technology transfers, a PLA actor hacked into Westinghouse's networks and stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routings within the plant buildings.[13]
- In 2010 and 2011, while Westinghouse was exploring other business ventures with the same Chinese state-owned enterprise, the same PLA hacker stole sensitive, non-public,

[9] CrowdStrike, *Global Threat Report* (2013).

[10] Nicole Perlroth, David E. Sanger & Julie Hirschfield Davis, *Hackers tied to China amass trove of U.S. data; Breaches of government and health care firms expose files of millions*, NY Times (June 6, 2015).

[11] McAfee & Center for Strategic International Studies, *The Economic Impact of Cybercrime and Cyber Espionage* (July 2013).

[12] Indictment, U.S. v. Wang Dong et. al., No. 14-118 (W.D. Pa. May 1, 2014).

[13] *Id.*

and deliberative emails belonging to senior decision-makers responsible for Westinghouse's business relationship with that state-owned enterprise.[14]

- In 2012, at about the time that the U.S. Commerce Department found that Chinese solar products manufacturers had "dumped" products into U.S. markets at prices below fair value, a PLA hacker stole thousands of files including information about SolarWorld's cash flow, manufacturing metrics, production line information, costs, and privileged attorney-client communications relating to ongoing trade litigation. Such information would have enabled a Chinese competitor to target SolarWorld's business operations from a variety of angles.[15]
- In 2010, U.S. Steel was participating in trade litigation against Chinese steel companies, including one particular Chinese state-owned enterprise. Shortly before the scheduled release of a preliminary determination in one such case, a PLA hacker sent spear-phishing emails to U.S. Steel employees, some of whom were in a division associated with the litigation. Some of these emails resulted in the installation of malware on U.S. Steel computers. Three days later, the PLA hacker stole host names and descriptions of U.S. Steel computers , and thereafter took steps to identify and exploit vulnerable U.S. Steel computers.[16]
- In 2012, Allegheny Technologies, Inc., was engaged in a joint venture with a Chinese state-owned enterprise, and was involved in a trade dispute with that enterprise. In April of that year, a PLA hacker gained access to Allegheny's network and stole network credentials for virtually every Allegheny employee.[17]

In my own work representing corporations that are targets of Chinese commercial cyber espionage, I witness firsthand the costs they incur in order to prepare for and respond to cyber-based attacks. For example, prior to an cybersecurity incident taking place, large companies devote extensive financial, staff and consultant resources to keeping information security policies up-to-date, implementing technical network security programs, developing and exercising breach response plans, participating in public-private and private-private cybersecurity information-sharing arrangements, negotiating the information security terms of third party vendor agreements, ensuring that third party vendors maintain adequate information security, purchasing cybersecurity insurance, and training employees.

If a significant cybersecurity incident takes place, then typically the CEO, Chief Operating Officer, Chief Information Officer, Chief Information Security Officer, General Counsel, VP for Communications, VP for Human Resources, and other senior executives work closely on a daily basis with lawyers from Hunton and external digital forensic experts to oversee the response. This would typically include an internal investigation of the breach, restoring the integrity of the network, engaging law enforcement if appropriate, developing and implementing internal and external communications strategies, analyzing the company's legal obligations, complying with state, federal and foreign notification requirements, complying with third party contractual requirements, responding to inquiries from regulators, managing congressional inquiries, and defending against civil litigation and regulatory enforcement actions. These measures are very

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

time-consuming and expensive, and can go on for years. Not surprisingly, the costs associated with data breach response are on the rise.

So, what can we as a country do to deter the Chinese government from engaging in commercial cyber espionage? The indictment of the five PLA hackers in May 2014 could be helpful, as it may introduce the possibility of jail time and restricted international travel into the calculus of future would-be Chinese hackers. However, the indictment has affected diplomatic relations between the U.S. and China, and appears to have led to retaliation in different forms against U.S. companies doing business in China. It remains to be seen how frequently the Justice Department will seek similar indictments in the future.

The President's April 1, 2015 Executive Order on Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities authorizes the government to impose financial sanctions on foreign hackers. In addition, the DOJ indictment of the PLA hackers provides a basis for the U.S. government to impose trade sanctions on the Chinese government or bring an action before the World Trade Organization. However, it is unclear how often or in what way the new authority under the Executive Order will be used, or whether the government will successfully pursue trade sanctions based on the DOJ indictment.

The enactment of cybersecurity information-sharing legislation would assist private companies and the government in strengthening their network security, thereby making it more difficult for PLA hackers to conduct successful computer network operations.

Actions by private companies that are the target of China's commercial cyber espionage may in certain circumstances deter the PLA from attacking a company. Recently, a network security firm announced that its proprietary monitoring technology had been used to identify PLA intrusion activity associated with zero-day vulnerability (a network vulnerability for which no official security patch has been issued). The firm reported this vulnerability to Microsoft, which then released a patch rendering the zero-day useless. Subsequently, the firm observed the same PLA hackers looking for the presence of the security firm's proprietary technology and withdrawing its intrusion efforts upon finding that technology.[18] Technologies with such capabilities are promising, but unfortunately examples of technical deterrence remain rare and not well understood.

For all forms of deterrence, whether they are indictments, trade sanctions, economic sanctions against individuals or technical measures, we need to gain a better understanding of how they may work and whether they are or could be effective. However, currently, little analysis or effort is devoted to these questions. It is my hope that the government and the private sector can work together in the future to examine the effectiveness of different forms of deterrence, and develop models of action that will someday persuade the Chinese government to reduce or end its campaign of commercial cyber espionage.

Thank you for the opportunity to testify today.

[18] http://blog.crowdstrike.com/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/.