Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Committee on Foreign Affairs

Subcommittee on Asia and the Pacific

Reviewing President Xi's State Visit

October 7, 2015

Chairman Salmon, Ranking Member Sherman, distinguished members of the Subcommittee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 3,400 customers in 67 countries, including 250 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions. In 2014, we conducted hundreds of investigations in 13 countries.

Has President Barack Obama secured relief from Chinese hacking? That is the question on the minds of many following the announcement by the US leader and his counterpart, Chinese President Xi Jinping, on September 25, 2015. On balance, the agreement is a step in the right direction. At best I would expect it to result in a decrease in the digital intrusion pressure applied by Chinese military and intelligence forces against American companies. The Chinese would likely continue pursuing their strategic goals by changing tactics at the human level and operations and the merger and acquisition level. At worst I expect the agreement to have no effect whatsoever.

To understand the agreement, one must review the words spoken and written by the two leaders. After looking at the words, I offer four interpretations, and then provide concluding remarks.

The fact sheet released by the White House offers four main points with respect to cybersecurity: investigations, conduct, norms, and dialogue. To assess whether both sides interpret the agreement in the same manner, and what the agreement means, it is important to start with the statements offered by both presidents.

In a joint press conference, each leader summarized the fact sheet in his own words. President Obama stated the following:

"I raised once again our very serious concerns about growing cyber-threats to American companies and American citizens. I indicated that it has to stop. The United States government does not engage in

cyber economic espionage for commercial gain. And today, I can announce that our two countries have reached a common understanding on the way forward. We've agreed that neither the U.S. or [sic] the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. In addition, we'll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace."

President Xi, as translated and published by the White House, offered his interpretation:

"During my visit, competent authorities of both countries have reached important consensus on joint fight against cyber-crimes. Both sides agree to step up crime cases, investigation assistance and information-sharing. And both government will not be engaged in or knowingly support online theft of intellectual properties. And we will explore the formulation of appropriate state, behavior and norms of the cyberspace. And we will establish a high-level joint dialogue mechanism on the fight against cyber-crimes and related issues, and to establish hotline links."

Statements about investigations, norms, and dialogue are less contentious than those concerning conduct in cyberspace. The relevant excerpt from the White House fact sheet states the following:

"The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

What does this mean for victims of Chinese hacking? First, consider President Xi's posture prior to the September 25th press conference. In written answers to questions posed by the Wall Street Journal, President Xi claimed "The Chinese government does not engage in theft of commercial secrets in any form, nor does it encourage or support Chinese companies to engage in such practices in any way."[1] Combining this statement with his later declarations, it is possible President Xi is professing that the Chinese government does not hack, because he does not consider the People's Liberation Army,

[1] http://www.wsj.com/articles/full-transcript-interview-with-chinese-president-xi-jinping-1442894700

Ministry of State Security, or other organizations conducting hacking operations to be part of his definition of "Chinese government." Therefore, PLA units such as 61398, revealed by Mandiant in 2013, will continue to raid American companies, because Xi does not count them as government forces.

A second interpretation could be congruent with both US and Chinese interests. The US targets Chinese organizations, as well as others worldwide, in order to conduct economic espionage. Such economic espionage is designed to better understand foreign financial conditions and uncover bribery and corruption that harms American commercial interests. The US has a long-standing policy of not passing what it learns from these economic spying missions to American companies for competitive gain. It's possible the US administration believes its Chinese counterpart will now act in a reciprocal manner. American companies will still be targeted by Chinese hacking teams, but the Chinese government will claim that it is working to collect economic data and uncover bribery and corruption. Whether the Chinese government passes what it learns to Chinese companies, for economic advantage, remains an open question.

A third interpretation could signal a tactical shift in Chinese commercial data acquisition. China has never been a "one trick pony" when it comes to stealing business information from foreign targets. The Chinese conduct extensive and aggressive cyber operations, but they also employ equally comprehensive human campaigns as well. To educate American businesses, the Federal Bureau of Information produced two independent movies, *Game of Pawns* and *The Company Man,* both available on YouTube.[2] The first tells the true story of Glenn Duffie Shriver, an American student in China recruited by the Chinese Ministry of State Security to infiltrate US government agencies. Shriver was arrested while fleeing to South Korea and spent nearly four years in Federal prison. The second tells another true story while obscuring the identity of the victim company. In *The Company Man*, viewers learn of a plot to steal technical documents from an American company, with Chinese agents falling for a sting operation enacted through a patriotic employee.[3] The February 2013 "Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets" documents many other cases, and more have been prosecuted since its publication. In brief, the Chinese may have decided to simply shift resources toward the physical collection of commercial data, and wind down their cyber operations. This change in tactics

[2] https://www.youtube.com/watch?v=R8xlUNK4JHQ and https://www.youtube.com/watch?v=Gy_6HwujAtU
[3] The surveillance video of the sting operation is posted online at https://www.youtube.com/watch?v=aIzKI2U5UV8.

would still support Chinese strategic goals. This transition from virtual to physical would still be a win for US companies, because it is easier to identify, counter, and apprehend human threats.

A fourth interpretation could signal an operational shift in Chinese commercial data acquisition. Early in his translated remarks, President Xi said the following:

"We have agreed to vigorously push forward the bilateral investment treaty negotiation, speed up the pace of the work so as to achieve a high standard and balanced agreement.

We will expand mutually beneficial cooperation in energy, environmental protection, science and technology, aviation, infrastructure, agriculture, health and other areas. The two governments and relevant agencies have signed many cooperation agreements, and our businesses have signed a series of commercial contact."

These words, combined with President Xi's meeting with American business leaders in Seattle, could mean that he intends to conduct more merger and acquisition activity, and that he expects the Obama administration to permit it. Currently sensitive technology deals, such as the rumored $23 billion bid by China's Tsinghua Unigroup Ltd for chipmaker Micron Technology, are likely to be blocked by the Committee on Foreign Investment in the United States (CFIUS) process.[4] While some deals, such as the 2014 acquisition of IBM's low-end server business by China's Lenovo Group Ltd., have cleared CFIUS approval, others remain problematic. Xi's mention of many of his government's strategic emerging industries indicates these remain a strategic priority.[5] As shown by Baidu's investment in, and joint venture with, American content delivery network company CloudFlare, China will use traditional business methods to acquire intellectual property, market share, and service know-how in order to advance its strategic goals.[6]

A final consideration for this agreement requires considering who is left out. The focus on US and Chinese companies ignores many other targets. These include so-called civil society organizations (CSOs), as well-documented in the recent report by the University of Toronto's Citizen Lab titled

[4] http://www.reuters.com/article/2015/07/21/us-micron-m-a-tsinghua-exclusive-idUSKCN0PU1X120150721
[5] http://www.swissnexchinanews.org/innovation/2013/10/27/chinas-7-strategic-emerging-industries
[6] I have concerns about the CloudFlare-Baidu deal, as noted in "Dark Cloud: Why CloudFlare's Deal with Baidu Could Haunt US Tech Companies": http://motherboard.vice.com/read/cloudflare-baidu-partnership-yunjiasu-china

Communities @ Risk.[7] These CSOs include dissident groups inside and outside China, universities, think tanks, media organizations, lawyers, and human rights watchers. Companies in Europe, Asia, Africa, and elsewhere are not covered by the US-China agreement. Furthermore, the agreement mentioned the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, also known as the UN GGE, but it did not agree to implement its findings concerning critical infrastructure. Therefore, those systems continue to be held at risk, as will the government, military, intelligence, and law enforcement organizations of each country.

I also expect US private sector security companies to bear the brunt of the public verification process. They will be subjected to repeated questions such as "are the Chinese still hacking," while the US administration is likely to remain fairly quiet. Furthermore, I do not expect the US administration to impose sanctions on Chinese entities for the remainder of the President's tenure, consistent with his general foreign policy preferences.

The Xi visit produced more positive statements than I expected. Now we must see if words are followed by decreased malicious activity in cyber space.

I look forward to your questions.

[7] https://targetedthreats.net/