James A. Lewis
Center for Strategic and International Studies
Questions for the Record (QFR) from the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, Hearing of July 9, 2013

QFR – Congressman Murphy

1. How do you protect the designs (or blueprints) for technology developed in the United States through the production phase in China without risking it being stolen?

   Companies have developed a range of strategies to protect heir intellectual property during the manufacturing phase n China, including keeping the most sensitive processes outside of China, not providing the full package of IP used to make the product, ad lmit8ing Chinese employees access to IP.

2. What are some common tactics used by China and the PLA to steal IP or technology?

   The most common tactic used by China to steal IP is "phishing," where a spoofed email is sent to company employees with an attachment (such as a video or spreadsheet) that infects the company network when it is opened. A second technique uses malicious websites, which contain malware that is automatically downloaded when the website is visited. Hackers attract visitor s by using common search terms, such as "Gangnam Style" or popular ring tones to get victims to visit the site.

   a. What is the PLA's assessment of US industries' ability to identify these tactics and protect against them?

      While the PLA assessment of US cybersecurity is not known, their actions indicate that they hold it in low regard, since they often use only the most basic hacking techniques and still succeed against many US companies.

   b. Have tactics changed/evolved in recent years/months?

      Tactics have change in recent years, growing more sophisticated. Attacks come in stages where the hackers first gain entry, then take control, and then exfiltrate information. The most advanced malware now may also use encryption to hide some its features and to make attribution more difficult.

3. What is our biggest leverage against the Chinese for their acts of cyber espionage?

   China does not wish to damage either economic or military relations with the U.S. This means that if they decide the U.S. is serious in its objections to cyber espionage, they will change their behavior.

   a. What role do companies have in protecting themselves?

Companies owe their investors due diligence in protecting their networks. Some companies have not put in place the most basic defensive techniques. This is one reason why China has been so successful.

c. Are other countries raising the issue of cyber espionage with China through diplomatic channels?

Several European countries have raise the cyber espionage issue with China, the most notable being Germany, where Chancellor Merkel has complained to Chinese leaders.

4. What needs to change in China for them to stop their policy of cyber espionage towards our companies?

China will only change if it faces persistent pressure from the US and its allies to stop economic espionage. This includes continued engagement at senior levels and, possible, retaliatory measures against known Chinese actors.

5. States actors in China such as the PLA are primarily interested in profit. In your testimony, you raise a very interesting point about the domestic costs of clamping down on cyber espionage by President Xi. What is the political climate in China that breeds the type of behavior of cyber espionage? How can these costs be reduced, and what can the international community do to raise the international costs of *not* clamping down?

China's transient for Marxism has been difficult in that the rule of law was badly damaged under Mao. Corruption is widespread in China, there is little respect for property rights or intellectual property protecting, and this environment encourages hacking. Chinese hackers also feel that the West owes China for the "Century or Humiliation' and western imperialism. Many Chinese know that returning to rule of law is essential for their countries development. The development of agreed international norms on responsible state behavior in cyberspace would help change Chinese behavior, as would promoting better compliance by china with existing agreements on trade and intellectual property protection.

6. There are currently many government agencies whose jurisdiction includes cyber security issues. Do you believe that the regulatory structure could be streamlined to address persistent cyber security threats more effectively? If so, what are your recommendations for doing so?

The U.S. needs to create a new Agency responsible for all aspects of cyber security (as was recommended in the December 2008 CSIS "Report on the Cybersecurity for the 44th Presidency). This agency could be modeled on USTR or on the National Counterterrorism Center, and existing authorities given the DNI would allow for this Center to be stood up quickly. To quote that report;

> "Twenty years ago, all the federal experts who protected cyber space, gathered together, would have made a rather small club. Today, hundreds of cyber experts of varying ranks are found all over government—a proliferation in numbers that reflects the growth of the Internet itself and our reliance on it. But while

cyberspace operates with a shared set of organizing principles, the human network too often resembles a large fleet of well-meaning bumper cars.

The central problems in the current Federal organization for cybersecurity are lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility. A new administration could put much time and effort into an attempt to revitalize or resuscitate the existing organizational structure, which was the product of a marriage between a decade-long process of accretion and an end-of-term response to crisis. Our view is that this effort would waste time and energy.

The Commission considered many options for how best to organize for cybersecurity. We grew to understand the importance of bridging across the federal agencies in order to leverage their knowledge to provide the best security for our nation. Improving cybersecurity will be difficult, as the problem cuts across agency responsibilities. We also recognized the importance of involving the private sector – the federal government cannot do this alone.

Many of our interviews encouraged us to think of a holistic approach to cybersecurity, one that looked beyond security alone and asked how best to enable and assure essential services in cyberspace. The progression of out thinking led from an improved DHS to an expanded cybersecurity function in the NSC; from an expanded NSC to a new cybersecurity entity; and from a new cybersecurity entity to one that looked broadly at enabling the secure and reliable use of cyberspace for national functions."

7. Many of China's universities offer programs in cyber security. Do you believe that similar programs should be available in the United States? How should these initiatives be developed? Is there more that U.S. universities could be doing?

   The U.S. needs to put more effort into creating a cybersecurity workforce. Currently there is a shortage of individuals with needed skills. Universities could play an important role in this, noting that traditional computer science programs are often not adequate for cybersecurity. Programs at junior colleges could also help meet workforce needs.

QFR – Congressman Gardner

1. In the energy sector, protecting intellectual property is less tangible than other industries, and arguably more difficult to address. Keeping in mind the complexities on legislation in this space, as all industries are different and cyber does not have neat borders, what more could be done apart from the President's recent Executive Order to prevent these types of attacks?

   Seeing a robust Cybersecurity Framework emerge from the February 2013 Executive Order is the most important thing that can be done to make Critical Infrastructure more secure. NIST should be encouraged to draw upon the experience of the Australian government, which has developed a number of mitigation strategies that greatly reduce risks. Another set

of generally principle of minute prescriptive guidance from NIST will not help. In addition, progress in removing impediments to information sharing are also important and the eventual passage of legislation like the House Bill CISPA would improve the situation.

2. Do you believe that allowing private industry to decide how to best secure their system – by allowing them to choose amongst the Executive Order, NIST framework, other standards, or best practices – is a workable system to gather the necessary information to combat cyber threats?

   Prescriptive regulations are unnecessary, but left to their own devices companies may not always choose the best approach. Current industry best practices are, judging from the very high number of successful attacks, inadequate It is important to set a standard for due diligence which critical infrastructure companies must meet. How companies meet these standard should be left them to them to choose.

3. In your opinion, do you believe that various private industries have been adequately working together to address cyber espionage and its threats as opposed to simply relying on the federal government to do it for them?

   Very little has been done to address cyber espionage by anyone. The financial sector has made substantial efforts, but their focus is on cyber crime, not espionage.

4. What role do private industries play in protecting their own property?

   Corporations owe a duty of care to their shareholders to protect their asset, including intellectual property. Increasingly, companies will incur liability risks if they do not put adequate cybersecurity measures in place. We can now definitely state the minimal requirements for cyber security (found in guidance like the Australian Signals Directorate's 35 Mitigation Strategies) and companies will need to take these into account if they are to exercise du diligence.

5. How critical is it in legislation or any other cyber guidelines to address the importance of improving the flow of threats information sharing from all directions (such as company to company, government to company, and company to government)?

   Information sharing is problematic now because of legislative framework governing privacy is outdated, written for dial telephones and cooper wires. Information sharing cannot be improved or make its full potential contribution to cybersecurity without the passage of legislation like CISPA.

QFR – Congressman Tonko

1. Mr. Lewis, you present an interesting conundrum, where China's reliance on cyber espionage has undermined its ability to innovate. Do you believe this trend will continue? Will

China's weak IP protections increase the likelihood that the next generation of technology will be developed and manufactured in the U.S.?

China continues to struggle with creating an innovation economy, because of weak IP protections and political constraints. The 'innovation engine" in the U.S., however, is slowing done due to a combination of funding constraints, political obstacles, and regulatory burdens. This slowing of innovation in the U.S. puts America's technological leadership at risk. Until we change this situation, the U.S. will continue to slow in productivity growth, manufacturing, and innovation.

2. Companies know they risk their IP in China but are willing to accept that risk for the short-term economic benefits. If Chinese companies demonstrate an ability to absorb and recreate U.S. technology at quicker rates, do you foresee the costs of IP loss causing companies to reconsider where they do business?

   Companies appear to be reconsidering the risks of investing in China, in part because of the risk of intellectual property theft. The larger issue is how to get China to follow the "rules" created for international trade so that foreign companies can safely do business in that country.

3. Can you express your views about the ways and means we currently investigate and sanction those that conduct IP theft? How can our methods be improved today? What new authorities can be offered to improve our methods in the future?

   Until recently, the U.S. has not done anything to stop Chinese cyber espionage. Recent initiatives by the administration have begun to change, this, but they will require persistence and perhaps sanctions to make progress. This will not be an easy struggle. As part of this effort, the U.S. should consider visa restrictions on Chinese individuals identified d as being involved in hacking, Treasury Department restrictions on the ability of such individual or Chinese companies involved in hacking to do business in the US or use the US financial system. The US could also consider indictments of suspected hackers and, as a final step, retaliatory trade measures. Other measures could include Other actions are also used to signal displeasure, such as canceling official visits, freezing visas issuance, or ending scientific cooperation. These steps al risk damaging the important trade relationship with China and they must be taken cautiously and in the context of a larger dialogue on cybersecurity, but if that dialog does not appear to be making adequate progress, sanctions must be used.

QFR – Congressman Burgess

1. When I asked you what small business can do to improve their ability to prevent, identify and mitigate the consequences of a compromise? Please elaborate on the strategies that were put in place by the Australian government to have an 85% success rate in preventing a security compromise.

The Australian Signals Directorate (ASD), an intelligence agency responsible for cybersecurity, analyzed why the most frequent attacks succeeded. They found that most successful attacks exploited basic vulnerabilities. This led them to rank vulnerabilities by frequency and success rate and to develop strategies to mitigate these attacks. ASD used the information from its analysis to develop a list of 35 mitigation steps. The first four of these steps provide the greatest defensive benefit. One of the strengths of the ASD and NSA approach is that it is based on measurements and repeatable data. Another strength is that since most successful attacks consist of several steps that allow the hacker to penetrate the system and exfiltrate data, these measures interfere with one or more of these steps, effectively stopping known or unknown attacks when compared to the reactive approach used in other kinds of defense. A third strength is that the initial data suggest that these measures can actually save money when compared to existing practices. The data on these two strategies is compelling.

I was in Australia last week for a government law enforcement / intelligence conference and talked to the Australian Signals Directorate about their mitigation strategies. They provided me with talking points used by one of their senior officials who is responsible for Cyber and Information Security, on an experiment they ran on effectiveness:

---------- BEGIN ASD TALKING POINTS----------

I know many of you have heard the ASD mantra about what to do - implement the Top 4; Catch, Patch, Match. Here they are if they slipped your notice.

Someone posed the question, is "Catch, Patch, Match" just a marketing slogan?

So we ran an experiment to test whether the theory stood up in practice. What we were really interested in was seeing how the Top 4 went against real world malware.

We built 1200 virtual machines and we gathered together around 1700 malware samples. We used malware that had been employed against Commonwealth government agencies and also that lurking out in the wild of the internet.

Some of our machines had no Top 4 mitigations at all, some had the full dose, and the balance had varying degrees of mitigation.
We started by running malware on machines that had no mitigation. If they penetrated then they were run through the next, lightly mitigated machines. And so on to the machines with the Top 4 fully implemented.

The final result from our experiment, with the Top 4 mitigation strategies fully implemented, was … zero!

Now it is worth keeping in mind that the Top 4 will not … let me say that again … will not be effective against all malware. But they are an excellent step in improving cyber security.

----------END ASD TALKING POINTS----------

ASD summarized the experiment to me by noting that the combination of "White listing, least privilege user access, OS patching and application patching" was "Out of the 1700 samples - zero executed." In other words, all attacks were stopped. Australia has made the strategies mandatory for all government agencies. The US would benefit substantially if the ASD strategies were reflected in the Cybersecurity Framework being developed by NIST but there is some risk that this will not happen, given reluctance in the Administration to take advantage of the Australian experience. This would be unfortunate but is perhaps unavoidable at this time.