

Oral Testimony
Cyber Espionage and the Theft of U.S. Intellectual Property and Technology
Committee on Energy and Commerce
U.S. House of Representatives

July 9, 2013

James A. Lewis, Center for Strategic and International Studies

I thank the Committee for the opportunity to testify. I will discuss three issues: why China steals intellectual property; what the effects of this are on the U.S. and China; and steps we can take to remedy this problem.

Cyber espionage in China is a routine practice, reflects deeper problems with intellectual property protection, and is so pervasive as to challenge Beijing's ability to control it.

Every Fortune 1000 company in the U.S. has been a target for Chinese hackers.

China has four motives for cyber espionage:

- First, they have an overwhelming desire to catch up with and to surpass the West.
- Second, they believe that rapid economic growth is politically essential for the party to maintain its dominance.
- Third, China has no tradition of protecting intellectual property.
- Finally, Chinese leaders fear that China has lost the ability to innovate and must depend on stolen technology.

China supports its strategic industries and State-Owned Enterprises through cyber espionage. For example, China made clean energy a priority and clean energy companies in the U.S. and Germany became targets.

China's economic espionage activities against the United States are greater than the economic espionage activities of all other countries combined.

The effect, however, is not one of clear-cut benefit to China.

China lacks the know-how and marketing skills to turn much of the stolen technology into competing products. There can be a lag of many years before there is damage to US businesses.

This is not true for confidential business information. The director of an allied intelligence service once described this theft of business confidential information as a "normal business practice" in China.

Cyber espionage hurts China's, by undercutting its efforts to create domestic innovation and by creating hostility and suspicion in its relations with many countries.

Espionage for national security purposes is routine among great powers. What is unacceptable is espionage for purely commercial purposes.

Frustration with the lack of progress has led to suggestions for ineffective sanctions or retaliation. It is not in our interest to start a war or crash China's economy. Hacking back has little real effect and runs contrary to U.S. law and international commitments.

Instead, the U.S. needs an engagement strategy with four elements. These are

- a sustained, high level attention;
- creating public disincentives for Chinese hacking;
- close coordination with allies; and
- improved domestic cyber defenses to make our companies harder to pillage.

Last month, a UN Group that included the U.S. and China said that international law and the principles of state responsibility apply to cyberspace. This agreement provides a foundation for rules on hacking.

Our goal should be to create global standards for responsible behavior and get China to observe them. To use a favorite Chinese expression, we want a “win-win” outcome rather than being a “zero sum” game, where for one side to win the other must lose.

Cyber espionage lies at the heart of the larger issue of China's integration into the international system.

China's economic growth has been of tremendous benefit to the world, but what was tolerable when China was an emerging economy is no longer tolerable when it is the world second largest economy.

I look forward to your questions.