The Chinese Hacking Indictments and Why Economic Espionage Is Different

Peter Swire, CIPP/US
Privacy Perspectives | **May 21, 2014**

On Monday, the Justice Department announced indictments against five named members of China's People's Liberation Army for hacking and theft of trade secrets. In reaction, the Chinese government denied the attacks and essentially said the U.S. spies, so the U.S. has no basis for complaining.

I think the Chinese government is wrong on both counts.

The U.S. cybersecurity community has long known that incessant cyber-attacks come from China. In 2008, in the

wake of the Obama election, I was talking with the security expert for a Washington think tank that had good connections with the new administration. This expert said that attacks were coming every night from China. They would begin just after breakfast time in the time zone in eastern China then take a break for lunch (the middle of our night). The presumably well-fed attackers would begin again after lunch. The targets included address books of the well-connected—one goal apparently was to map the social networks of the new U.S. trade and other officials.

The second argument from the Chinese government is essentially that there is no difference between what they do and surveillance by the NSA and other U.S. agencies. In response, there is a strong case that industrial cyber-espionage is different and deserves the sort of strong response shown this week by the Justice Department.

Unknown to many observers, the U.S. has a long-standing policy of not using surveillance to steal industrial secrets to advantage domestic industry. This issue came to the fore in the work of President Obama's Review Group on Intelligence and Communications Technology, on which I served as one of five members. In our Recommendation 31, we supported international norms or international agreements for specific measures that would promote economic growth and increase confidence in the security of online communications. Specifically, we recommended that "governments should not use surveillance to steal industry secrets to advantage their domestic industry."

One reason to stop industrial espionage is that it is a simple crime—stealing from a specific victim for the benefit of a specific other company. Attorney General Eric Holder, in his news conference announcing the indictments, pointed out that we would of course consider it criminal if a burglar pulled a truck up to an industrial facility to steal things from inside. Stealing trade secrets from a company is similar, to the loss of companies named in the indictment such as Alcoa, U.S. Steel and Westinghouse.

Criminal laws against industrial espionage serve broader goals than simply vindicating the victim. Protection of trade secrets fosters economic efficiency and protects investment and investment in intellectual property. As a matter of new technology, companies invest in trade secrets while they prepare to enter a market, and many innovations then ripen into patents that are published to the world and make the innovation known to follow-on

innovators. Military-grade cyber-attacks on those trade secrets steal from the innovator and also reduce the expected profit from the hard work of developing new products and services.

> *"In our Recommendation 31, we supported international norms or international agreements for specific measures that would promote economic growth and increase confidence in the security of online communications. Specifically, we recommended that "governments should not use surveillance to steal industry secrets to advantage their domestic industry."*

A related efficiency harm is that it is costly and difficult for ordinary corporations to protect themselves against military-grade cyber-attacks. The spending needed to protect trade secrets against that level of attack imposes costs across the broad swathes of industry that compete with other countries.

Beyond efficiency harms, industrial espionage also fosters unfair competition. One interesting wrinkle is that several of the companies that came forward were involved in unfair competition trade disputes with China. In 2011, a subsidiary of SolarWorld asked the U.S. Commerce Department to investigate whether Chinese competitors were involved in "dumping," or sale below cost designed to force out the U.S. producer. The Commerce Department indeed found evidence of illegal dumping. But it allegedly turns out that the hackers had stolen the chief financial officer's cash flow projections—the Chinese army was allegedly providing Chinese companies with the data needed to know just how long it would take to force SolarWorld out of the market.

The response from China has been to accuse the U.S. of "hypocrisy and double standards." There have been reports that the U.S. has done surveillance on corporate networks, with particular publicity about the Brazilian energy company Petrobras. The administration has explained that corporate surveillance does take place for reasons including terrorist financing and enforcing sanctions laws against countries such as Iran.

Where done under proper legal authorities, my view is that there are compelling reasons to carry out law enforcement and national security surveillance. In a world where war, crime and terrorism exist, nations continue to need tools to protect the security of their citizens.

More broadly, as the Review Group recommended, we should support the creation of global norms that support peaceful, efficient and fair use of the Internet by individuals and corporations.

One of the other norms we supported was that "governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems." Since World War II, the international trade system has reduced tariffs and expanded to include China and other countries that would never have joined originally. Having the Chinese military steal corporate secrets for the advantage of Chinese companies is contrary to the international trade system and the way the Internet should operate. The indictments this week are a positive step toward bringing a sensible rule of law to attacks in cyberspace.

1 Comments

If you want to comment on this post, you need to login

Peter Swire • May 22, 2014

Harvard Law Professor and former senior DOJ official Jack Goldsmith took a contrary positions here: http://www.lawfareblog.com/2014/05/the-u-s-corporate-theft-principle/ I have responded Jack's arguments there.