The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3779 | NOVEMBER 19, 2012

Chinese Economic Espionage Is Hurting the Case for Free Trade

Derek Scissors, PhD

Trade and investment with China benefits the U.S. This is evident in choices made by individuals and companies every day to buy Chinese goods and work with Chinese partners. Indeed, American business has been the chief proponent of a sound U.S.–China economic relationship.

The context makes intense Chinese economic espionage all the more regrettable. Chinese entities are targeting the very companies that are most interested in doing business and maintaining a good relationship across the Pacific. The situation is bad and may be deteriorating further.

It is time for a more pointed U.S. policy response that addresses the issue while maintaining or even improving bilateral economic relations. As always, the first requirement is information: American firms that are subject to Chinese cyber and other espionage activities should disclose them to the government on a confidential basis. If the results of these disclosures show a serious problem, the Obama Administration should consider making commercial espionage its top economic priority in talks with China. Failing progress in such discussions, it may be necessary to take certain actions against particular Chinese enterprises engaged in or benefitting from espionage.

The Setting: China and Cyber. Imports from the People's Republic of China (PRC) help support American jobs. Chinese investment in the U.S. has accelerated sharply this year because American firms want more Chinese investment. Chinese purchases are aiding the struggling American property market.[1]

The PRC's government and companies insist that they want to continue to trade with the U.S. and want more two-way investment. This is welcome. However, the value of the relationship to the U.S. is being undermined by Chinese economic espionage, another word for which is "theft."

Espionage is no longer cloaks and daggers. It has spread in terms of both targets (embracing economics as well as security) and methods, with computers now more dangerous than people. The national security dimension is important to the U.S. in general and the U.S.–China relationship. Even putting national security aside, though, there is a problem.

Mutually beneficial economic exchange occurs only when there is acceptance of the rule of law. If the legal protection of property rights is ignored, free exchange makes much less sense: One side just takes from the other. The U.S. has long had this problem with Chinese violation of American intellectual property, but the advent of cyber espionage has made it considerably worse. No longer does painstaking work have to be conducted to steal a single chemical process, for example; now a fully successful cyber attack can swipe the entirety of a company's knowledge.

Disturbing Trends. Americans complain, sometimes inaccurately, about many Chinese economic practices. A standard response from Beijing is that China is poor compared to the U.S. and needs time: Conditions are slowly improving. This is often reasonable, but it is untrue with regard to economic espionage, particularly economic cyber espionage. Greater Chinese capabilities and more advanced technology

This paper, in its entirety, can be found at **http://report.heritage.org/ib3779**

Produced by the Asian Studies Center

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

are not breeding less theft; in fact, they may be breeding more.

In the past few years, just among large companies, Dupont and Lockheed Martin have been targeted by attacks from China. So have American Superconductor, Coca Cola, Chesapeake Energy, and British Gas.[2] The latter group is noteworthy because they are all firms that were actively trying to do business with the PRC—trying to continue an existing partnership or create a new one. Chinese hackers are attacking the country's friends as well as its commercial rivals.

The Chinese government's sole response—angry denials—is making matters worse. It is not the slightest bit credible that all of these attacks occur without the consent of the central government. The Chinese partners or rivals of the attacked foreign firms are usually state-owned. Given that the Communist Party refuses to accept the independence of harmless social organizations, the frequency and increasing sophistication of these cyber attacks implies organization and capability that would never be tolerated unless under Party control.

How to Respond. American economic policy is flawed, and it is only reasonable to expect Chinese policy to be flawed as well. However, complaints about barriers to Chinese investment in the U.S. and the like ring hollow compared to economic espionage. Respect for property rights is a precondition for commercial exchange.

This matter can—and perhaps should—be handled on a confidential, government-to-government basis. Documentation of the extent of the problem would both clarify the priority that the U.S. should attach to the matter and spur a constructive Chinese response. The PRC should meaningfully commit to improving the situation—meaning fewer incidents and more accountability. If this does not happen, there will be still more strain on the back of an already bruised bilateral relationship. To make this problem more pointed, it is the traditional advocates of strong bilateral economic relations that are being harmed.

The U.S. should take the following actions:

- The federal government should first determine the extent of the problem. Companies should be asked to submit evidence of large-scale hacking to the Department of Homeland Security on a volunteer basis. The process for keeping this evidence confidential should be formulated to the satisfaction of at-risk firms.
- Depending on the results of this documentation, the Obama Administration should evaluate making espionage the top priority in economic negotiations such as the Strategic and Economic Dialogue.
- Depending on bilateral talks, the Department of Justice and other Cabinet departments may need to build a framework for legal action. If PRC-based cyber attackers cannot be prosecuted, restrictions should be placed on firms that are shown to benefit from espionage. For example, if an American company is targeted coincident with negotiations with a Chinese enterprise, the Chinese enterprise might be banned from some transactions for a certain time.

Last Straw? The U.S.–China economic relationship is not infinitely resilient. Beijing must understand that economic espionage is alienating China's best American friends. The U.S. should proceed carefully to address the situation, starting with gathering the necessary information.

*—**Derek Scissors, PhD,** is Senior Research Fellow in Asia Economic Policy in the Asian Studies Center at The Heritage Foundation.*

1. See Derek Scissors, Charlotte Espinoza, and Terry Miller, "Trade Freedom: How Imports Support U.S. Jobs," Heritage Foundation *Backgrounder* No. 2725, September 12, 2012, http://www.heritage.org/research/reports/2012/09/trade-freedom-how-imports-support-us-jobs; Derek Scissors, "Chinese Outward Investment: Acceleration Features the U.S.," Heritage Foundation *Issue Brief* No. 3656, July 9, 2012, http://www.heritage.org/research/reports/2012/07/chinese-foreign-investment-outward-investment-acceleration-features-the-us; and Michael Dolgow, "China's Gift to U.S. Homeowners," *Businessweek*, July 29, 2012, http://www.businessweek.com/articles/2012-07-29/chinas-gift-to-u-dot-s-dot-homeowners (accessed November 9, 2012).
2. Ben Elgin, Dune Lawrence, and Michael Riley, "Coke Gets Hacked and Doesn't Tell Anyone," *Bloomberg*, November 4, 2012, http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html (accessed November 9, 2012); Michael Riley, "Weak Company Cyberattack Filings Irk SEC," *CFO World*, January 10, 2012, http://www.cfoworld.com/accounting/28922/weak-company-cyberattack-filings-irk-sec (accessed November 9, 2012); Ed Crooks and Leslie Hook, "American Superconductor Sues Chinese Group," *Financial Times*, September 15, 2011, http://www.ft.com/intl/cms/s/0/df685246-df17-11e0-9af3-00144feabdc0.html#axzz1qvfY4yzA (accessed November 9, 2012); and Jason Mick, "NSA: China Is Destroying U.S. Economy Via Security Hacks," DailyTech.com, March 28, 2012, http://www.dailytech.com/NSA+China+is+Destroying+US+Economy+Via+Security+Hacks/article24328.htm (accessed April 9, 2012). For an abridged timeline, see Derek Scissors, "Chinese Commercial Espionage: U.S. Policy Recommendations," Heritage Foundation *Issue Brief*, No. 3564, April 9, 2012, http://www.heritage.org/research/reports/2012/04/chinese-commercial-espionage-us-policy-recommendations.