The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3564 | APRIL 9, 2012

Chinese Commercial Espionage: U.S. Policy Recommendations

Derek Scissors, Ph.D.

Sino–American economic conflicts are often characterized as "bad but improving." For example, the trade deficit is ugly, but exports to China are rising, protection of intellectual property is said to be slowly expanding, and so on. There is an important matter, however, where the situation is bad and the case that it is getting better is very thin: commercial espionage.

Commercial espionage overlaps economics and national security. The cyber variant—where networks are infiltrated and crucial knowledge pilfered—overlaps violations of intellectual property rights (IPR) and cyberwarfare attacks. China remains at the top of the offenders list in IPR infringement and cyberwarfare, so it is little surprise that it "leads" in commercial espionage.

The surprise is lack of improvement. China's political and business leadership either considers commercial espionage acceptable or believes they cannot be held accountable. Both misperceptions need to be corrected. The U.S. should make a sharp change in its response to commercial espionage—not to immediate retaliation but to making it unmistakably clear that such espionage is not acceptable.

More Than a Decade of Theft. To some extent, even a simple, quite incomplete chronology speaks for itself. The technology-oriented espionage of a decade or so ago has given way to broader attacks. Sometimes, there is no particular Chinese enterprise involved, or the persons engaged in espionage are seeking to form companies in the PRC using stolen intellectual property.

However, on other occasions, very prominent Chinese firms are linked to the cases. PetroChina, Beijing Auto, Sinovel, Datang Telecom, Pangang—these companies are quite large and either state-owned or state-connected. (Sinovel grew out of a state entity.) Among their other characteristics, state firms are protected in the PRC's courts and tend to share resources with other state firms far more easily than truly competing corporations.[1] It is very rare for a centrally controlled enterprise to hold a noticeable technological edge over another in the same sector and even rarer for courts to decide a case against a state firm.

This adds up to a disturbing conclusion: China's manufacturing rise has been illegally aided. Many advances are certainly due to the PRC's own strengths; others stem from voluntary cooperation by foreign partners. But it is all too easy to find examples of Chinese theft that correspond well to spurts in manufacturing capability in advanced electronics, energy, autos, etc.

Telecom is probably the most dramatic example. Chinese hackers may have had full access to Nortel's technology for a period of years. Such information is useful only to Nortel's competitors, which feature Chinese equipment makers, which became globally competitive players more rapidly than expected starting shortly after Nortel was hacked. It is very difficult to believe that this is a coincidence.

Technology broadly understood is America's comparative advantage. Theft of that technology—whether through dramatic cyber-attacks or simple infringement of intellectual property—undermines the value of trade and other economic exchange for the U.S.

This paper, in its entirety, can be found at **http://report.heritage.org/ib3564**

Produced by the Asian Studies Center

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

A Disturbing Trend

2001: Two people funded by state-owned Datang Telecom indicted for stealing secrets from Lucent.[2]

2002: Two people funded by Hangzhou city government indicted for stealing secrets from four firms.[3]

2003: PetroChina employee arrested for attempting to steal seismic imaging software from Silicon Valley firm (later pled guilty).[4]

2004: Canada's Nortel discovers that China-based hackers have compromised its entire network.[5]

2005: Chinese national working at U.S. unit of Dutch firm AkzoNobel begins stealing material needed to replicate advanced industrial coating.[6]

2006: Two people indicted for stealing proprietary information from auto parts maker Metaldyne and seeking to pass it to Chinese firms.[7]

2007: Chinese national employed by Dow begins transferring trade secrets to Chinese government-controlled institutes.[8]

2008: Former DuPont employee picked by state-owned Pangang to make titanium dioxide, supposedly using DuPont production method (later pled guilty to espionage).[9]

2009: Ford Motor employee arrested for stealing trade secrets—later found guilty—supposedly on behalf of Beijing Auto.[10]

2010: Dozens of multinationals disclosed as targeted in China-based hacking of Google.[11]

2011: American Superconductor sues top Chinese turbine maker Sinovel for stealing software used to drive wind turbines.[12]

2012: NSA director acknowledges that China-based hackers compromised a company that provides computer security services to defense firms such as Lockheed Martin.[13]

Technology theft helps the PRC—but not indefinitely. Commercial espionage is great for catching up, but it is a powerful disincentive to becoming a leader. Thieves have little reason to innovate, and the transition from stealing to inventing is a difficult one. Beijing should be increasingly willing over time to act to curb its companies' theft, but the government may not have the will or cohesion to do so.

Get the Ball Rolling. Chinese economic espionage is a persistent problem, but this does not imply that there is an obvious U.S. policy remedy. It does seem that American companies need help of some sort. American Superconductor and DuPont certainly cannot use the Chinese judicial system to seek damages from Sinovel and Pangang, respectively. Using U.S. or international courts might work, but if the Chinese entity ignores a judgment, what then?

Just stalling might also work: By the time an American company sees a judgment enforced, the technology involved may no longer be valuable. Perhaps the only answer is Washington pushing Beijing to discipline its firms. There are three things the U.S. could do in this regard:

1. Commercial espionage should be considered for inclusion as a key topic at the May Strategic and Economic Dialogue and other high-level bilateral meetings. For these meetings to have any value, the U.S. should have only one or two main economic goals. Espionage should be emphasized only if something else is pushed down the agenda (for example, the exchange rate).[14] American firms should accept that the threat will remain for some time and work together to better meet it. Information could be pooled on attacks, defenses, successes, and failures in a systematic and ongoing fashion among high-risk firms in telecom, energy, and elsewhere. The federal government could play a coordinating role to reassure companies of confidentiality.

2. The Departments of Commerce and Homeland Security should create a technical forum where companies and government can share knowledge and resources. Participation should ideally extend beyond well beyond defense-related entities. There are bills in Congress on cybersecurity with application to commercial espionage that propose federal involvement beyond just coordination—for example, in setting standards. These efforts are quite justified, but formal standards are all but impossible in a field that changes so rapidly. Other federal involvement runs the risk, due to vaguely defined terms, of leading to violations of civil liberties at home or escalating cyber-aggression overseas. This should not

be the first step. A more modest beginning might involve firms with U.S. government contracts.

3. Companies sometimes fail to report espionage.[15] Congress should require firms with government contracts to report—systematically and in a timely fashion—intrusions and unauthorized export of data to the Departments of Commerce and Homeland Security. These companies would have the option of requesting federal technical assistance in seizing stolen data or blocking entry.

Shrinking the Problem. It is tempting to look at China's commercial espionage record and demand immediate, powerful action. That may be satisfying, but it would probably not help the U.S. Actions should be taken as soon as possible, but the first actions should be measured.

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

1. For example, see China Wind Power Center, "Chinese Court Rules Against AMSC in Sinovel Dispute," February 7, 2012, at http://www.cwpc.cn/cwpc/en/node/7748 (accessed April 9, 2012), and Cellular News, "China Promotes Tower Sharing by Mobile Operators," October 6, 2008, at http://www.cellular-news.com/story/33991.php (accessed April 9, 2012).
2. News release, "New Indictment Expands Charges Against Former Lucent Scientists Accused of Passing Trade Secrets to Chinese Company," U.S. Department of Justice, April 11, 2002, at http://www.justice.gov/criminal/cybercrime/press-releases/2002/lucentSupIndict.htm (accessed April 9, 2012).
3. News release, "Pair from Cupertino and San Jose, California, Indicted for Economic Espionage and Theft of Trade Secrets From Silicon Valley Companies," December 4, 2002, at http://www.justice.gov/criminal/cybercrime/press-releases/2002/yeIndict.htm (accessed April 9, 2012).
4. Rachel Konrad, "Chinese Man Sentenced to 2 Years for Silicon Valley Fraud," Associated Press, December 18, 2004, at http://www.usatoday.com/tech/news/computersecurity/2004-12-18-corp-spy_x.htm (accessed April 9, 2012).
5. CBC News, "Nortel hit by suspected Chinese cyberattacks for a decade," February 14, 2012, at http://www.cbc.ca/news/world/story/2012/02/14/nortel-chinese-hackers.html (accessed April 9, 2012).
6. Ann Woolner et al., "The Great Brain Robbery," *Businessweek*, March 15, 2012, at http://mobile.businessweek.com/articles/2012-03-14/the-great-brain-robbery (accessed April 9, 2012).
7. David J. Lynch, "FBI Goes on Offensive Against China's Tech Spies," *USA Today*, July 25, 2007, at http://www.usatoday.com/money/world/2007-07-23-china-spy-2_N.htm (accessed April 9, 2012).
8. News release, "Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets," October 18, 2011, at http://www.justice.gov/opa/pr/2011/October/11-crm-1372.html (accessed April 9, 2012).
9. Karen Gullo, "Former DuPont Worker Pleads Guilty in Economic Espionage Case," *Businessweek*, March 2, 2012, at http://www.businessweek.com/news/2012-03-02/former-dupont-worker-pleads-guilty-in-economic-espionage-case (accessed April 9, 2012).
10. China Daily, "Ford Engineers Yuxiang Dong China Steal Secrets Jailed for 70 Months," April 14, 2011, at http://www.china-daily.org/China-News/Ford-engineers-Yuxiang-Dong-China-steal-secrets-jailed-for-70-months/ (accessed April 9, 2012).
11. Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, at http://www.wired.com/threatlevel/2010/01/operation-aurora/ (accessed April 9, 2012).
12. Ed Crooks and Leslie Hook, "American Superconductor Sues Chinese Group," *Financial Times*, September 15, 2011, at http://www.ft.com/intl/cms/s/0/df685246-df17-11e0-9af3-00144feabdc0.html#axzz1qvfY4yzA (accessed April 9, 2012).
13. Jason Mick, "NSA: China Is Destroying U.S. Economy Via Security Hacks," DailyTech.com, March 28, 2012, at http://www.dailytech.com/NSA+China+is+Destroying+US+Economy+Via+Security+Hacks/article24328.htm (accessed April 9, 2012).
14. See Derek Scissors, "Tools to Build the U.S.–China Economic Relationship," Heritage Foundation *Backgrounder* No. 2590, August 8, 2011, at http://www.heritage.org/research/reports/2011/08/tools-to-build-the-us-china-economic-relationship, and Derek Scissors, "Some Truths About Trade," The Heritage Foundation, *The Foundry*, February 13, 2012, at http://blog.heritage.org/2012/02/13/some-truths-about-trade/.
15. Joseph Menn, "Exclusive: Hacked Companies Still Not Telling Investors," Reuters, February 2, 2012, at http://mobile.reuters.com/article/idUSTRE8110YW20120202?irpc=932 (accessed April 9, 2012).