COUNCIL on FOREIGN RELATIONS

April 15, 2011

Innovation, Espionage, and Chinese Technology Policy

Prepared statement by

Adam Segal

Ira A. Lipman Senior Fellow for Counterterrorism and National Security
Council on Foreign Relations

Before the

House Foreign Affairs Subcommittee on Oversight and Investigations
United States House of Representatives
1st Session, *112*th Congress

Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology

Chairman Rohrabacher, Ranking Member Carnahan, and members of the committee, thank you for the opportunity to testify on this important subject.

Chinese cyber espionage has to be understood within the context of China's desire to reduce its dependence on the West for advanced technologies, and on the United States and Japan in particular. This goal is laid out in the 2006 National Medium- and Long-Term Plan for the Development of Science and Technology (MLP) which introduced the need for "indigenous innovation" (*zizhu chuangxin*) to lessen the "degree of dependence on technology from other countries to 30 percent or less," (down from 50 percent today, as measured by the spending on technology imports as a share of the sum of domestic R&D funding plus technology imports).[1] Moving from "made in China" to "innovated in China" is essential to the country's future; "Facts tell us that we cannot buy true core technologies in key fields that affect the lifeblood of the national economy and national security," states the MLP. China will become an "innovation oriented society" by 2020 and a world leader in science and technology (S&T) by 2050.

In pursuit of these goals, China has followed three, often intertwined, tracks: industrial policy, innovation strategy, and cyber and industrial espionage. Industrial policy involves top-down, state-directed technology programs often focused on specific sectors and the government research institutes. The MLP, for example, includes twenty science and engineering megaprojects in such areas as high-end generic chips, manned aerospace and moon exploration, developmental biology, and nanotechnology.

In order to promote indigenous innovation, Chinese policy makers have also used government procurement, developed competing technology standards, and required technology transfer from multinational corporations in return for market access. In 2009, for example, China announced that companies would have to demonstrate that their products included indigenous innovation and were free of foreign intellectual property if they wanted to be a recognized vendor in the government's procurement catalog. In April 2010, Beijing ordered high-tech companies to turn over the encryption codes to their smart cards, Internet routers, and other technology products in order to be included in the catalog.[2] The Chinese have been especially active on the standards front, developing new standards for third generation cellphones (TD-SCDMA), WiFi (WAPI, or WLAN Authentication and Privacy Infrastructure), DVDs (AVS, the audio video coding standard), RFID (Radio Frequency Identification), and other technologies.

The failure to protect intellectual property rights in the Chinese market leads to massive theft and piracy, and in turn improves the short-term competitiveness of Chinese firms. As Senior Director for Greater China at the U.S. Chamber of Commerce Jeremie Waterman said when he testified before the International Trade Commission, a weak legal environment allows Beijing to "intervene in the market for IP [intellectual property] and help its own companies 're-innovate' competing IPR as a substitute to foreign technologies."[3]

In contrast to these state-led efforts, innovation strategy is a more bottom-up, multifaceted effort to create a business environment supportive of innovation and entrepreneurship. These strategies are more dependent on the free market and private entrepreneurship. Often drawing on the experience of Silicon Valley and Route 128 in Boston, these policies focus on small start-ups, university-industry collaboration, and venture capital.

The last strand is the theft of intellectual property either through cyber espionage or more traditional industrial espionage. Since January 2010, Google, Nasdaq, DuPont, Johnson & Johnson, General Electric, RSA, and at least a dozen others have had proprietary information stolen by hackers, although how many of these attacks originated from China is uncertain.[4] Attacks are becoming more sophisticated and increasingly rely on spear phishing (targeted attacks that rely on publicly available information) and other social engineering techniques. In the physical world, Chinese nationals have been recently charged in the theft of radiation-hardened microchips and precision navigation devices.

These three tracks often overlap, in some places more clearly and in others more speculatively. It is not uncommon for a small private firm to attract government attention as it becomes successful. So, for example, a firm founded by a professor who wanted to commercialize research findings would move from the realm of innovation strategy to industrial policy as the company turned to the State High Technology Development Plan (also known as the 863 Program) for investment.

The relationship between technology development policies and espionage, while certainly present, is more difficult to draw out. The government has actively encouraged Chinese nationals working in science and technology fields in the United States and other advanced economies to return home through programs such as the national One Thousand Talents Scheme, Shanghai's Gathering Ten Thousand Overseas Students Project, and the various Overseas Students Parks dotted across the country. These "talents" are offered access to investment capital, subsidized real estate and other preferential policies when they return to Shanghai, Beijing, and other technology centers. In some instances, according to a *New York Times* report, Chinese nationals have applied for government funding to help develop technologies that were stolen from American companies.[5]

The relationship between the state and hackers is even murkier. As the "Shadows in the Clouds" report on computer exploitation notes, there is an emerging ecosystem of crime and espionage. Espionage networks adopt criminal techniques and networks "both to distance themselves from attribution and strategically cultivate a climate of uncertainty." Some of the information stolen by the hackers ends up on the black market, some of it, according to the report, ends up in the "possession of some entity of the Chinese government."[6] At the very least, much of the hacking is state tolerated, in many instances it is encouraged, and in some cases of espionage, it is directed by state actors.

U.S. Policy Responses

It is clear that the United States must do more to defend itself. In the September 2010 issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn III argued that though the "threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyber threat that the United States will face over the long term."[7]

There is, however, an emerging debate whether the traditional methods of cybersecurity—public-private partnerships and information sharing—are adequate to the threat. Given the attacks on Google and other technology companies, there is a real question whether the private sector can defend itself against state-backed attacks. Under these conditions, some have suggested extending the Defense Industrial Base Information Sharing Environment, a forum in which forty defense contractors share information on attacks in return for DOD assistance with network defense, to critical private sector firms. At the very least, private companies must get used to the idea that any information that is digitalized cannot be made completely secure. In this environment, the objective for the private sector is risk management, with the government and U.S. Cyber Command playing defensive and deterrent roles, respectively.

The other policy focus must be an attempt to change Chinese actions and incentives. Efforts to raise the issue of cyber espionage directly with Chinese policy makers have generally elicited two responses. Officials often have a Captain Renault-like response that Beijing is "shocked, shocked" that anything like illegal computer access could happen since hacking is illegal in China. Or they complain, with some justification, that China is itself victim to many cyber attacks, many of them originating in the United States. *The People's Daily*, for example, cites a 2006 report that the approximately 27,000 Trojan horse attacks on China came mainly from the United States.[8] The recent announcement that the FBI is sending a cyber security expert to cooperate with Chinese authorities on investigations is an important first step but to building some trust between the two sides on criminal hacking.

American technology companies need to be more vocal about the theft of their intellectual property. While U.S. trade officials often want to press their Chinese counterparts, they are often frustrated with the attitude of U.S. businesses operating in China. American companies complain about the high rates of piracy, but in any intellectual property rights case against China, no one wants to be named as the complainant. Few companies want to alienate the central government in Beijing, and many fear reprisal from local government officials, who levy fines for spurious safety and labor violations, refuse new building permits, or subsidize their competitors.[9]

The same issue is partly at play with computer intrusions. Right now, the majority of companies do not seem interested in knowing more about attacks because of cost and liability issues. According to a recent study by McAfee and SAIC, more than half of 1,000 companies surveyed in the United States, Britain and other countries did not investigate security breaches because of the cost.[10] But it can also be assumed that many do not publicize attacks for fear of alienating the Chinese government. When Google announced in January 2010 that it been undergoing a series of attacks that seemed to be coming from China, it also stated that those same attacks affected thirty other technology companies. Yet after the announcement, no other company admitted to being victim.

While few companies have the ability to leave the China market like Google did, there is evidence that vocal complaints and unified pressure can have some influence on Chinese policy makers, especially since China still depends on foreign companies for access to critical technologies. In the case of WAPI, the competing standard to WiFi, foreign companies refused to go along with requirements to transfer technology to Chinese companies and threatened not to sell wireless chips into the Chinese market. The U.S. government also got involved, with a letter, signed by Secretary of State Colin Powell, Commerce Secretary Don Evans, and U.S. Trade Representative Robert Zoellick that implicitly threatened to pursue the case at the World Trade Organization. Eventually the Chinese government backed down.

The other policy question is: can the United States appeal to those who want China to become more innovative but think industrial policy and indigenous innovation in particular are counterproductive? There are parts of the Chinese bureaucracy promoting innovation strategy; they advocate raising the country's technological capabilities through trade-friendly policies, such as providing greater transparency and enforcing IPR-protection regulations. They have not forgotten that China has benefited immensely from access to billions of dollars in foreign investment, global customers and distribution networks, and technology transfers from American, Japanese, and European firms. In addition, as more Chinese firms expand abroad, they are beginning to realize that their global competitiveness will be severely limited if the Chinese market is isolated as a result of indigenous innovation initiatives.

This "innovation strategy" faction should be sympathetic to similar arguments about the deleterious effects of cyber espionage on Chinese innovation capabilities. In fact, dependence on foreign secrets is likely to lessen the ability (and desire) of Chinese firms to push the technological envelope. The challenge for the United States is identifying and supporting those elements, though how capable they are in fighting against those interests promoting industrial policy and supporting cyber espionage is an open question.

Because China's leadership is broadly committed to the goals of reducing dependence on foreign technology any progress on either the industrial policy or cyber espionage front is bound to be slow and uneven. The United States should continue to try and shape the debate within China, but the most important actions will be improving the defense of its computer networks and intellectual property.

I thank the Committee for the opportunity to testify and will be happy to take any questions.

[1] "The National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)," State Council, People's Republic of China.

[2] Adam Segal, "China's Innovation Wall: Beijing's Push for Homegrown Technology," *Foreign Affairs*, September 28, 2010, http://www.foreignaffairs.com/articles/66753/adam-segal/chinas-innovation-wall

[3] Testimony of Jeremie Waterman before the US International Trade Commission on "China, Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the US Economy," June 15, 2010, http://www.itcblog.com/wp-content/uploads/2010/06/watermancomments.pdf

[4] "Significant Cyber events since 2006," Center for Strategic and International Studies, Last Modified March 9, 2011, http://csis.org/files/publication/110309_Significant_Cyber_Incidents_Since_2006.pdf; Michael Riley and Sara Forden, "Hacking of DuPont, J&J, GE Were Google-Type Attacks That Weren't Disclosed," *Bloomberg*, March 8, 2011,

[5] Christopher Drew, "New Spy Game: Firms' Secrets Sold Overseas, *The New York Times*, October 17, 2010

[6] Shadows in the Cloud: Investigating Cyber Espionage 2.0," Joint Report, Information Warfare Monitor, Shadowserver Foundation, April 6, 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

[7] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[8] America's Two-Faced Tricks Once Again Give It a Lead," translated from the Chinese "美国的两面手法又给自己当头一棒," *The People's Daily*, March 30, 2011, http://opinion.people.com.cn/GB/14278366.html

[9] Adam Segal, *Advantage: How American Innovation Can Overcome the Asian Challenge*, W. W. Norton and Co., January 10, 2011

[10] Brian Grow, "Special Report: In Cyberspy vs. Cyberspy, China has the Edge," *Reuters*, April 14, 2011, http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414