Heritage Lectures

Published by The Heritage Foundation

No. 907
Delivered September 15, 2005

November 4, 2005

Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage

Larry M. Wortzel, Ph.D.

As a former military intelligence officer who has tracked the activities of the People's Liberation Army and Chinese intelligence services for 35 years, I know of no more pervasive and active intelligence threat to America's national security than that posed by the People's Republic of China. The workforce available to the Chinese government and its corporations to devote to gathering information in the United States is nearly limitless.

There are some 700,000 visitors to the United States from China each year, including 135,000 students. It is impossible to know if these people are here for study and research or if they are here to steal our secrets. The sheer numbers defy complete vetting or counterintelligence coverage.

In 2003, for example, the State Department granted about 27,000 visas to Chinese "specialty workers," the H1-B visa. Some of these were intra-company transfers coming to the United States from U.S. firms operating in China. Between 1993 and 2003, the United States has granted an average of 40,000 immigrant visas to Chinese each year. The sheer magnitude if these numbers presents a great challenge to the Federal Bureau of Investigation, particularly when the U.S. is also concerned about terrorism, which occupies a lot of investigative time for agents.

The Chinese People's Liberation Army and the defense establishment in China started programs in the late 1970s and 1980s to create companies designed to bring in needed defense technology; the

Talking Points

- The Chinese defense establishment started programs in the late 1970s and 1980s to create companies designed to bring in needed defense technology to serve the interests of the PLA and the military–industrial complex.
- The Chinese government is able to identify potential collectors of information and, if necessary, to coerce them to carry out missions on behalf of the government because of the lack of civil liberties in China.
- In March 1986, the PRC launched a national high-technology research and development program with the specific goal of benefiting China's medium- and long-term high-technology development.
- The prudent course of action for the United States is to maintain law enforcement programs, counterintelligence programs, and security education and industrial security programs as the means to protect our nation

This paper, in its entirety, can be found at:
www.heritage.org/research/asiaandthepacific/hl907.cfm

Produced by the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

goal was to produce defense goods for the PLA and for sale to other countries.

- The General Political Department of the People's Liberation Army started a proprietary company, *Kaili*, or Kerry Corporation, that for years operated in the U.S. as a real estate and investment company.
- The General Equipment Department of the PLA operated a proprietary company, Polytechnologies, or *Baoli*, that had offices here in the U.S.
- In addition, the General Logistics Department operated a proprietary called *Xinshidai*, or New Era, that had offices in our nation and continues to be responsible for a network of PLA manufacturing plants in China.

These technically are independent legal entities under Chinese law, but the Central Military Commission of the Chinese Communist Party established them to serve the interests of the PLA and the military–industrial complex. Active or retired officers of the PLA or their families originally staffed these companies. The PLA and related defense science and technology research and development organizations in China regularly operate trade fairs to attract American high technology into China.

The Deputy Undersecretary of Defense for Technology Security and Counterproliferation has testified that there are between 2,000 and 3,000 Chinese front companies operating in the United States to gather secret or proprietary information, much of which is national security technology or information. The deputy director of the Federal Bureau of Investigation for counterintelligence recently put the number of Chinese front companies in the U.S. at over 3,200. Many of these front companies are the spawn of the military proprietary companies discussed in the preceding paragraph.

The nature of the Chinese state complicates the problem of knowing what the large numbers of travelers and students from China are actually doing. China is still an authoritarian, one-party state led by the Chinese Communist Party with a pervasive intelligence and security apparatus. The Chinese government is able to identify potential collectors of information and, if necessary, to coerce them to carry out missions on behalf of the government because of the lack of civil liberties in China. Let me quote the first three sentences of Chapter 1, Article 1, of the Chinese Constitution:

> The People's Republic of China is a socialist state under the people's democratic dictatorship led by the working class and based on the alliance of workers and peasants. The socialist system is the basic system of the People's Republic of China. Disruption of the socialist system by any organization or individual is prohibited.

The People's Republic of China is methodical in its programs to gather information from abroad. In March 1986, the PRC launched a national high-technology research and development program with the specific goal of benefiting China's medium- and long-term high-technology development. This centralized program, known as the "863 Program" for the date when it was announced, allocates money to experts in China to acquire and develop biotechnology, space technology, information technology, laser technology, automation technology, energy technology, and advanced materials.

When I was at the American Embassy in China and conducted due-diligence checks to confirm the nature of Chinese companies seeking to do high-technology business in the United States, I most often found that the address identified for a company on a visa application turned out to be a People's Liberation Army or PRC government defense research institute. Thus, the United States faces an organized program out of China that is designed to gather high-technology data and equipment of military use.

Screening to Protect Trade and Military Secrets

In January 1998, the Visas Mantis program was developed to assist the American law enforcement and intelligence communities in securing U.S.-produced goods and information that are vulnerable to theft. Travelers are subject to a worldwide name-check and vetting procedure when they apply for visas. The security objectives of this program are to prevent the proliferation of weapons of mass destruction and missile delivery systems; to

restrain the development of destabilizing conventional military capabilities in certain regions; to prevent the transfer of arms and sensitive dual-use items to terrorists; and to maintain United States advantages in militarily critical technologies.

This program operates effectively and can vet a Chinese student in as few as 13 days. Non-students may take longer, as many as 56 days. However, I can tell you, based on my trip to China two weeks ago, that the American Embassy in Beijing and the Consulate in Guangzhou are able to process and vet in about two weeks visas for non-student travelers who fully and accurately outline the purpose and itinerary of their trip.

Still, many U.S. companies complain about delays in getting visas for travelers they want to bring to the United States. Automation and data-mining software can speed visa processing to ensure that these companies can be competitive. The government also operates a "technology alert list" to identify legal travelers from China that may benefit from exposure to advanced U.S. technology with military application. Of course, the consular officers manning visa lines in embassies must be trained to look for signs of espionage for screening to be effective.

Many provinces and municipalities in China now operate high-technology zones and "incubator parks" specifically designed to attract back Chinese nationals who have studied or worked overseas in critical high-technology areas. When students or entrpreneurs return with skills or knowledge that the central government deems critical, they are given free office space in the parks, loans, financial aid, and administrative help in setting up a business designed to bring in foreign investment and technology. Their companies are given tax holidays. Innovative programs, such as those at Beijing's Zhongguancun High Technology Park and Guangzhou's High Technology Economic and Trade Zone, get central government help.

These are admirable programs that will develop entrpreneurial skills among well-educated Chinese citizens. However, as students and employees of U.S. companies return home, it is important to know that they are not taking back American economic or military secrets. Good counterintelligence and industrial security programs are very important to U.S. security, given this threat.

Inadequate Enforcement of Intellectual Property Laws

The enforcement of intellectual property protection laws in China is spotty and inconsistent at best. This is one of the major complaints of American high-technology companies about China's compliance with its obligations under the World Trade Agreement.[1]

The tendency to steal intellectual property and high-technology secrets in China is worsened when intellectual property laws are not enforced there. And the problem is further exacerbated when centralized Chinese government programs, such as the 863 Program mentioned earlier, are specifically designed to acquire foreign high technology with military application. This only creates a climate inside China that rewards stealing secrets.

I believe that U.S. government security, intelligence, and law enforcement agencies must focus on the national security. They should be looking for acts of espionage and for violations of the Arms Export Control Act or the Export Administration Act.

When it comes to corporate or industrial espionage that is not a matter of national security, I believe that the government owes American companies a good legal infrastructure to protect trademarks, patents, and copyrights; a system of education on industrial security; and a strong effort to ensure that China meets its own obligations to create a rule of law that protects the right of ownership and intellectual property.

However, I do not believe that American intelligence or security agencies should focus on forms of economic espionage that do not involve national security information. From the standpoint of congressional action, my view is that the Congress should reconsider the Export Administration Act with a view toward ensuring that its provisions

1. Editor's note: This visit, scheduled for September 7, was postponed because of Hurricane Katrina.

meet the needs of 21st century technology. The 1979 Export Administration Act expired in 2001. The Senate passed a new Act in 2001, but no revision passed the House.

The executive branch must regularly review the Commodity Control List to ensure that appropriate national security controls on exports protect the nation's security but do not unduly restrict the ability of American industry to compete in the world market. Generally, technologies that are widely available on the world market and not unique to the United States should not be unduly restricted unless they can be subject to mulitlateral export controls.

Finally, we cannot become paranoid and suspect that every traveler, student, and businessman from China is a spy or is out to steal technology. Many of the people that come to the United States absorb our values and bring them home. We must keep in mind that in earlier decades, in places like the Republic of China on Taiwan and in South Korea, the steady flow of returning students and immigrants who were exposed to American values and principles eventually eroded dictatorships and produced multi-party democracies. The prudent course of action for the United States is to maintain law enforcement programs, counterintelligence programs, and security education and industrial security programs as the means to protect our nation.

—Larry M. Wortzel, Ph.D., is a Visiting Fellow at The Heritage Foundation. This analysis is adapted slightly from testimony presented to the Subcommittee on Immigration, Border Security, and Claims of the Committee on the Judiciary of the U.S. House of Representatives.