Testimony of Larry M. Wortzel
Chairman, U.S.-China Economic and Security Review Commission

Before the Subcommittee on Crime, Terrorism, and Homeland Security
of the House Committee on the Judiciary
Hearing on "Enforcement of Federal Espionage Laws"

January 29, 2008

Chairman Conyers, Chairman Scott, Ranking Members Sensenbrenner and Gohmert, and Members of the Subcommittee, thank you for inviting me to address this hearing on the enforcement of federal espionage laws.

My name is Larry Wortzel and I presently serve as the chairman of the twelve member, bipartisan, bicameral United States-China Economic and Security Review Commission. As you know, the Commission members are appointed by the Congressional leadership. I have served on the Commission since 2001 and I also served as chairman for the 2006 reporting year. By mutual agreement, the twelve commissioners elect a chairman and a vice-chairman each year, rotating the positions between a Republican and a Democratic appointee. I was appointed to the Commission by Speaker Hastert.

I will address the issues raised about espionage by China by the Commission in its yearly report to the Congress, issued in November 2007. I also bring some personal experience on the matter to bear. During my 32 year military career, I spent 25 years in military intelligence with the United States Army. This experience involved gathering signals intelligence and human source intelligence foreign intelligence, primarily about China. For about five years I was a military attaché at the American Embassy in China. I was also trained as a counterintelligence officer and spent a number of years conducting

counterintelligence investigations and developing programs to protect emerging defense technology from foreign espionage.

I should note that when I refer to the Report to Congress by the US-China Economic and Security Review Commission, I will summarize the views and consensus of the commissioners, as outlined in the report. You could have read that yourselves, however; therefore, given my background and experience, I will also express my own views. When I do, I will identify them as such.

The Commission concluded in 2007 that China's defense industry is producing new generations of weapon platforms with impressive speed and quality. We believe that some of these advancements are due to the highly effective manner in which Chinese defense companies are integrating commercial technologies into military systems. However, we note that espionage provides Chinese companies an added source of new technology without the necessity of investing time or money to perform research. After a year of hearings, research, and classified briefings from agencies of the U.S. intelligence community, the Commission concluded that China's espionage activities are the single greatest threat to U.S. technology and strain the U.S. counterintelligence establishment. This illicit activity significantly contributes to China's military modernization and acquisition of new capabilities.

There is a long record in China going back over two centuries of sending government directed missions overseas to buy or shamelessly steal the best civil and military technology available, reverse engineer it, and build an industrial complex that supports the growth of China as a commercial and military power. Indeed, my own view is that today it is often difficult to distinguish between what we define as espionage

related to the national defense under the Espionage Act (18 USC 792-9), and economic espionage or the theft of proprietary information and trade secrets covered by the Economic Espionage Act (18 USC 1831-9). Indeed, for American companies and for the national defense of the United States, the impact of espionage can be the same, robbing U.S. companies of the costs of their research, giving technology with military application to China's armed forces, and undermining the security of American military personnel and our nation.

One reason that China's industries have been so effective at espionage is the centralized approach they have taken. In March 1986, the PRC launched a national high technology research and development program with the specific goal of benefiting China's long-term high technology development. This centralized program is known as the "863 Program" (or Torch Program). China's state council allocates money to acquire and develop biotechnology, space technology, information technology, laser technology, automation technology, energy technology and advanced materials.[1]

Our Commission recognizes that part of China's defense industrial base modernization strategy is to acquire advanced foreign equipment and technologies. While in some cases Chinese planners have chosen to purchase entire weapon systems directly, some Chinese and Western analysts do not see this as beneficial for the long-term modernization of China's defense industry.[2] Direct purchases are generally used as a temporary measure to fill critical gaps that China's indigenous defense companies are unable to fill. Some items purchased from foreign companies are dual-use components—

[1] The 863 name comes from the month and the year that the program was proposed.
[2] U.S.-China Economic and Security Review Commission, *Hearing on China's Proliferation and the Impact of Trade Policy on Defense Industries in the United States and China*, testimony of James Mulvenon, July 13, 2007. Mulvenon sees this as a "scathing indictment of the failures of the PRC defense-industrial base to fulfill its long-standing promises to the PLA."

those that can be used in military as well as civilian applications such as computers, semiconductors, software, telecommunications devices, and integrated circuits.[3]

The report also notes that partnerships forged between foreign companies and Chinese civilian companies also offer Chinese defense industries access to advanced foreign technologies. The nature of the regulatory and commercial environment in China places enormous pressure on foreign companies, including those of the United States, to transfer technology to Chinese companies as a part of doing business in China and to remain competitive globally.[4] Foreign companies are willing to provide not only technology but capital and manufacturing expertise in order to secure market access in China.[5] Indeed, many are, in fact, creating R&D facilities in China.

Still, we note in the report that access to restricted foreign technology is obtained by China through industrial espionage. We have heard from experts who advise us that China operates an aggressive clandestine effort to acquire additional technologies.[6] In recent years, this has become such a problem in the United States that U.S. Immigration and Customs Enforcement officials have rated China's espionage and industrial theft activities as the leading threat to the security of U.S. technology.[7]

Our law enforcement agencies, our intelligence community, and our corporate security professionals must contend with seven or more Chinese state-controlled

[3] U.S. Department of Defense, *Annual Report to Congress on the Military Power of the People's Republic of China,* (Washington, DC: July 2007), p. 29.
[4] Medeiros et al., *A New Direction for China's Defense Industry*, (RAND Corporation, Santa Monica, CA: 2005) p. 241.
[5] Medeiros et al., *A New Direction for China's Defense Industry*, (RAND Corporation, Santa Monica, CA: 2005) p. 241.
[6] U.S.-China Economic and Security Review Commission, *Hearing on China's Military Modernization and Its Impact on the United States and the Asia-Pacific*, testimony of William Schneider, Jr., March 29, 2007.
[7] U.S. Department of Defense, *Annual Report to Congress on the Military Power of the People's Republic of China,* (Washington, DC: July 2007), p. 29.

intelligence and security services that can gather information for the state-owned industrial sector inside China or overseas. These include

- the Ministry of State Security and its local or regional state security bureaus;
- the Public Security Bureau;
- the intelligence department of the People's Liberation Army (PLA), or Second Department;
- the PLA's Third, or Electronic Warfare Department;
- a PLA Fourth Department that focuses on information warfare;
- trained technical collectors from the General Armaments Department and the General Logistics Department of the PLA;
- the technical intelligence collectors of the military industrial sector and the Commission of Science Technology and Industry for National Defense;
- and the Communist Party Liaison Department r PLA General Political Department.

Frankly, I don't know if the Chinese government is funneling information or technology back into some of the now-privatized companies that engage in industrial or economic espionage in China. Also, I believe that the various science and research parks that operate under municipal control actively seek out new technology and so do the newer companies that operate outside government control in China.

The nature of the Chinese state also compounds the security problems. China is a totalitarian state, even if today there is far greater economic freedom there. The legal system in China still responds to the direction of the Chinese Communist Party. Thus the state has great power to compel citizens to cooperate and a far reach to retaliate if citizens

in China refuse to do the state's bidding. I think that reach is decreasing as the economy offers more opportunity for Chinese citizens and there are more opportunities for private employment there. But it is still difficult to avoid the pressure that a one-party, Leninist-structured state can bring to bear on its citizens.

I would like to discuss one case brought to trial by the United States Attorney's office in the Central District of California as an example of how hard it is to know for certain whether our intelligence and law enforcement agencies face economic espionage or more traditional espionage designed to injure the national security of the United States. In the Chi Mak case, in California, five members of a southern California family were charged with acting as agents of the People's Republic of China in 2005 and in 2006 with conspiring with each other to export United States defense articles to the People's Republic of China (a violation of the Arms Export Control Act, 22 USC 2778). This technology theft ring focused on acquiring corporate proprietary information and embargoed defense technology related to the propulsion, weapons and electrical systems of U.S. warships. Going through Chi's residence, agents of the Federal Bureau of Investigation and the Naval Criminal Investigative Service found instructions tasking Chi to join "more professional associations and participate in more seminars with 'special subject matters' and to compile special conference materials on disk."[8]

Chi Mak was a support engineer at L-3 Communications working on navy quiet drive propulsion technology. In two documents instructing Chi, one hand printed in Chinese and the other machine printed, the military technologies Chi was to seek involved:

- Space-based electromagnetic intercept systems

[8] CI Centre, http://www.cicentre.com/Documents/DOC_Chi_Mak.html

- Space-launched magnetic levitation platforms
- Electromagnetic gun or artillery systems
- Submarine torpedoes
- Electromagnetic launch systems
- Aircraft carrier electronic systems
- Water jet propulsion
- Ship submarine propulsion
- Power system configuration technology
- Weapons system modularization
- Technologies to defend against nuclear attack
- Shipboard electromagnetic motor systems
- Shipboard internal and external communications systems
- Information on the next generation of US destroyers (DDX).

The espionage effort appears to have been directed by a Chinese academic at a research institute for Southeast Asian affairs at Zhongshan University in Guangzhou, China. The Chi family encrypted the information it was passing back to China into a computer disk that appeared to contain television and sound broadcasts. It was literally embedded in the other data in encrypted form.

This effort has all of the earmarks of professional espionage tradecraft and state-directed espionage, with sophisticated control and sophisticated clandestine communications means. The government university in Guangzhou could have been cover for a state-directed espionage effort. However, Chi Mak and his alleged co-

conspirators could just as well have been part of a sophisticated economic espionage operation run out of a university research institute.

Mr. Chairman, I could go on for a long time. The Computer and Intellectual Property Section of the Department of Justice web site lists 33 cases of alleged violations of the Economic Espionage Act between 2000 and 2005, many of which seem to have involved China. Immigration and Customs Enforcement has a large number of arrests and indictments, as does the FBI. In the US-China Economic and Security Review Commission's annual report, we note that "Mr. Joel Brenner, the top counterintelligence official in the Office of the Director of National Intelligence, has noted that of the 140 foreign intelligence agencies continuously attempting to penetrate U.S. agencies, China is the most aggressive.[9] The FBI stepped up counterintelligence efforts against Chinese intelligence operations in the United States in July 2007, because of what FBI Director Robert Mueller called a "substantial concern" about those operations."[10] An American engineer living in Hawaii was indicted for working with a Chinese government agent and supplying stealth missile technology over the course of six visits to China. A Defense Intelligence Agency employee was convicted on lesser charges but was indicted for leaking classified information to China's military intelligence service and hoarding classified U.S. documents in his home.

We also noted in our report concerns that computer, or "cyber" penetrations of United States companies and government agencies represent another spectrum of the espionage threat from China with which our law enforcement and intelligence community must contend. In England, the head of one of Britain's intelligence agencies

[9] Jeff Bliss, "China's Spying Overwhelms U.S. Counterintelligence," *Bloomberg*, April 2, 2007.
[10] Bill Gertz, "FBI calls Chinese espionage 'substantial,' *The Washington Times*, July 27, 2007.

warned of cyber-penetrations by China. The attacks allegedly targeted Royal Dutch Shell and Rolls Royce. So China's espionage activities target advanced technology, economic data and military secrets in many countries.

Our Commission unanimously concluded that "as Chinese espionage against the U.S. military and American businesses continues to outpace the overwhelmed U.S. counterintelligence community, critical American secrets and proprietary technologies are being transferred to the PLA and Chinese state-owned companies."[11] In response to this espionage, the Commission recommended the following steps:

- In order to slow or stop the outflow of protected U.S. technologies and manufacturing expertise to China, the Commission recommends that Congress assess the adequacy of and, if needed, provide additional funding for U.S. export control enforcement and counterintelligence efforts, specifically those tasked with detecting and preventing illicit technology transfers to China and Chinese state-sponsored industrial espionage operations.
- The Commission recommends that Congress assess the adequacy of and, if needed, provide additional funding for military, intelligence, and homeland security programs that monitor and protect critical American computer networks and sensitive information, specifically those tasked with protecting networks from damage caused by cyber attacks.

[11] U.S. Department of Justice Press Release, "Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center," August 2, 2007; U.S. Department of Justice Press Release, "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China: First Conviction in the Country for Foreign Economic Espionage," December 14, 2006; Jeff Bliss, "China's Spying Overwhelms U.S. Counterintelligence," *Bloomberg*, April 2, 2007; Amy Argetsinger, "Spy Case Dismissed for Misconduct," *Washington Post*, January 7, 2005; Bill Gertz, "FBI calls Chinese espionage 'substantial,' *The Washington Times*, July 27, 2007; U.S. Department of Justice Press Release, "Guilty Plea in Trade Secrets Case," February 15, 2007; U.S. Department of Justice Press Release, "Fifth Family Member Pleads Guilty in Scheme to Export U.S. Defense Articles to China,", June 6, 2007.

- The Commission recommends that Congress instruct the director of national intelligence to conduct a full assessment of U.S. intelligence capabilities vis-à-vis the military of the People's Republic of China, and identify strategies for addressing any U.S. weaknesses that may be discovered as part of the assessment
- The Commission recommends that Congress urge the Administration to engage China in a military dialogue on its actions and programs in cyber and space warfare to include threat reduction mechanisms, the laws of warfare, and specifically how the laws of warfare apply to the cyber and space domains.

In closing Mr. Chairman, I want to thank you and the Members of the subcommittee for holding this hearing. The law enforcement and intelligence communities have been effective in meeting this challenge, even if overwhelmed by other national security challenges. In my view, the Economic Espionage Act is a very helpful tool, especially since the elements of proof of the Espionage Acts are often more difficult to prove, as I tried to illustrate in my description of the Chi Mak case. In other indictments the law enforcement community has relied on the Arms Export Control Act and the Export Administration Act.

I should also note that the United States-China Economic and Security Review Commission also prepared a classified report to Congress. This report is available for Members and their appropriately cleared staff to read in the Office of Senate Security.

Thank you again for the opportunity to appear before you and I would be happy to respond to any questions you may have.