"Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information"

Testimony of Larry M. Wortzel

before the House of Representatives

Committee on Science, Space and Technology Subcommittee on Investigations and Oversight

May 16, 2013

Chairman Broun, Ranking Member Maffei, members of the sub-committee, thank you for the opportunity to testify today. I will discuss balancing scientific cooperation, the protection of critical information, and the espionage threat from China. As a member of the U.S.-China Economic and Security Review Commission, I will present some of the Commission's findings on China's science and technology policy and its goals, priorities and strategies with respect to the United States. The views I present today, however, are my own.

A report prepared for the U.S.-China Economic and Security Review Commission makes it clear that China's *2006 Medium to Long-term Plan for the Development of Science and Technology* sets goals "of becoming an innovative nation by 2020 and a global scientific power by 2050."[1] In order to achieve this goal, the Chinese government has invested a great deal of money and effort in subsidizing industry, insisting on transfers of science and technology to China when approving foreign investment, and funding over fifty nationally directed science and technology parks.[2] It looks as though China will invest about $1.5 trillion in strategic emerging sectors in the next five years with research and development spending expected to increase from 1.7 percent of GDP in 2007 to 2.5 percent of GDP by 2020. For the purposes of this hearing,

however, we should be focused on the fact that China saves incalculable amounts of time, money and research effort through espionage and intellectual property theft.

The Chinese Academy of Sciences operates 100 research institutes and there are more than 45,000 other research institutes and laboratories in China responsive to Beijing's direction and planning.[3] This nationally directed infrastructure seeks to obtain technology from foreign firms in key scientific areas that often have military application. Many of China's researchers and scientists have trained at U.S. institutions or have worked in U.S. firms, also adding to the transfer of American technology.

Science and technology cooperation programs are vital to China's own long-term goals, but they also help foster bilateral cooperation between China and the United States. However, there also is a substantial espionage threat posed by the large number of Chinese nationals working at U.S. laboratories and academic institutions. The counterintelligence education web site maintained by the Federal Bureau of Investigation highlights the "insider threats" posed by foreign intelligence collection to research, technologies, and intellectual property ostensibly protected by export controls.[4] Indeed, of the ten incidents of "insider threat" espionage cited by the FBI, six cases are related to China. Three former U.S. officials, Mike McConnell, former Director of National Intelligence; Michael Chertoff, former Secretary of Homeland Security; and William Lynn, former Deputy Secretary of Defense, said in a January 27, 2012 *Wall Street Journal* opinion piece that: "The Chinese government has a national policy of espionage in cyberspace, pointing out that "it is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own." This cyber espionage takes place alongside or in conjunction with other forms of espionage.

The U.S.-China Economic and Security Review Commission's annual report of 2007 reviews how China acquires foreign equipment and technology to support its defense industrial base and documents six espionage prosecutions related to China.[5] That annual report recommended that Congress provide additional funding and emphasis on export control enforcement and counterintelligence efforts to detect and prevent espionage. In 2009, the Commission's annual report to Congress addressed espionage conducted by Chinese state-controlled research institutes and commercial entities.[6] In 2012, the Commission recommended that Congress ask the National Academy of Sciences for an assessment of Chinese strategies to acquire technology and to identify the extent to which industrial espionage has been used as a tool to advance China's interests.

According to the National Counterintelligence Executive, "of the seven cases that were adjudicated under the Economic Espionage Act (18 USC 1831 and 1832) in Fiscal Year 2010, six involved China." An article in a March 2012 manufacturing newsletter notes that "there have been at least 58 defendants charged in federal court related to Chinese espionage since 2008."[7] China's targets have included are stealth technology, naval propulsion systems, electronic warfare systems for our ships and aircraft, and nuclear weapons.

There is a certain natural tension between the goal of preventing espionage by China (or any other country) and maintaining scientific openness. National Security Decision Directive 189 (NSDD 189), of September 21, 1985, makes it clear that U.S. national policy is that "to the maximum extent possible, the products of fundamental research remain unrestricted;" when restrictions are needed, the answer is that the products be classified as national security information according to U.S. statute.[8] The directive went on to define "fundamental research" as "basic and applied research, the results of which ordinarily are published and shared broadly

within the scientific community, as distinguished from proprietary research from industrial design, production, and product utilization, the results of which are restricted for proprietary or national security reasons." In a 2010 memorandum to defense agency heads and military department secretaries, then Under Secretary of Defense for Acquisition, Technology and Logistics Ashton B. Carter restated Department of Defense policy on fundamental research to ensure that it followed NSDD 189. He also instructed the Department of Defense that where controls are needed, classification of the product is the "only appropriate mechanism."[9]

This tension between what needs to be protected for national security and openness in scientific research is not new. In 1984, when I was a credentialed counterintelligence special agent for the Army and an investigator for the Counterintelligence and Security Policy Directorate of the Office of the Secretary of Defense, I had personal experience with this issue. In the interest of scientific cooperation and openness, a U.S. government computer data base containing oceanographic data such as bathymetric readings, undersea currents, and salinity was linked to computers in the Academy of Sciences of the Union of Soviet Socialist Republics. Some of these data were collected by U.S. Navy oceanographic research ships. The Department of the Navy approached the Office of the Secretary of Defense and the National Security Council expressing concern that although the information was fundamental research, sharing it with Moscow presented a national security concern. According to the Navy, the stored data sets provided a great deal of information critical for submarine navigation and could support the launch of ballistic missiles from submarines. Members of Congress got quite upset about Navy and DOD attempts to restrict fundamental research and I was called upon to testify before the Oceanography subcommittee of the House Committee on Merchant Marine and Fisheries about the entire matter.[10] Ultimately, research results that needed protection had to be classified. Now

here we are, thirty years later, still wrestling with the potential national security implications of foreign access to fundamental research.

I can suggest a few approaches that our nation might take. Obviously, perhaps it is time to once more evaluate the distinctions among basic, applied research and advanced technology development. What was true in 1985 may need to be updated to remain true today. To be candid, however, I think the scientific community and the country would come down in about the same place. A report on basic scientific research by the Defense Science Board last year did not suggest more controls on research, but instead recommended that the Department of Defense develop a technology strategy and remain involved in cutting edge basic research.[11] There are many threats to our security today, China included, but if we could live with open fundamental research during the Cold War, we can probably live with it today. After all, U.S.-China relations are substantially different than were U.S.-Soviet relations.

Instead of trying to restrict scientific research and experimentation, we ought to look more carefully at the institutions where research is being conducted and who is involved in the research. Also, some types of research may require more controls. In his May 24, 2010 memorandum on fundamental research, then Under Secretary Carter said that "there will be compelling reasons for DOD to place controls on some research that is performed on campus at a university, but such occasions should be rare and each must be scrutinized."[12]

If laboratories or academic institutions are engaged in fundamental research and at the same time are involved in research on proprietary, export-controlled or classified matters, it is incumbent on the government or industry to ensure that foreign nationals do not get unauthorized access to export controlled or classified research. Also, the information systems of institutions

involved in controlled or classified research should be separate from those that are open to all researchers.

If a strong case can be made that there are some new or emerging technologies that require additional protection, that argument must stand up to public and scientific scrutiny. Leaders of the U.S. Army are most worried about developments in the areas of biological agent research, robotics, information and cyber warfare systems, nano-technology, and explosives or energetics. Other military services expand this list to include directed energy systems, chip and integrated circuit technology, and new materials and processes. At what point does research on these issues move from basic or applied research, which is "fundamental," to research that requires export controls or classification? And does that standard of open fundamental research apply to every country in the world?

The FBI and the Defense Security Service, which administers the Defense Industrial Security Program, make the point that foreign nationals from some countries seem to have a higher track record of engaging in espionage. But they don't give academia a list of those countries.

When you look at China, you must consider the political environment in the home country of a particular researcher. You are dealing with a citizen of an authoritarian state that is ruled by a single political party. The Chinese Communist Party runs the country, the police, intelligence agencies, the university heads, as well as members of the judiciary, who are all members of the Communist Party. All residents are potential hostages to party dictates in a nation that has no rule of law. People in China applying for passports and permission to study or conduct research overseas may be interviewed by the security services. The future employment of these individuals, their place or residence, and the residences and employment of their family

or loved ones is subject to Party dictates. A foreign national from China, or a state like China, is vulnerable to coercion and to having his or her loved ones held hostage. And there is no right of refusal for citizens of these states when the government asks them to gather information.

No policy on fundamental research will resolve this problem, however. It is up to American government security services and the FBI to appropriately administer programs that involve classified or export controlled information. And it is up to the government to ensure that foreign nationals do not get access to information that should not be disclosed to them.

In my personal view, Congress should direct the executive branch to maintain a classified list of countries, people and companies that pose a serious espionage threat to our government and industry. Such a listing could be validated across the intelligence community. When nationals from those countries are involved in research at places that also have programs involving classified or export-controlled information, it is up to the government to develop security and risk mitigations measures.

In 2012, a news article in *Bloomberg* used the attention-grabbing headline "American Universities Infected by Foreign Spies."[13] The story here is compelling, but the headline may be a little exaggerated. Certainly there are cases of foreign researchers attempting to gather export-controlled information or even engaging in economic espionage. But the infection is not a fatal one, nor is it so serious that we need to completely revise how we understand fundamental research. If we attempted to do that, we would probably cripple undergraduate and graduate education in the United States. However, some of the examples cited in this article are instructive. A Chinese researcher, Yu Xiaohong, allegedly attempted to conceal her academic background and make a visit to a researcher on celestial bodies and navigation at the University of Michigan. It turned out that she was from a Chinese People's Liberation Army advanced

educational and research institution and had written an earlier paper on anti-satellite warfare. The U.S. professor she wanted to visit became suspicious of her intentions and stopped the exchange. In other cases, Chinese researchers have engaged in economic espionage or have taken trade secrets. The FBI has been pretty successful at prosecuting such cases. This suggests that Congress might provide more resources to the FBI and other federal agencies charged with protecting classified and export-controlled information to conduct more investigations and to increase education about the foreign intelligence collection threat. It is fair to assume that most of the researchers who apply for and undertake scientific and technical research for the government have the best interests of the United States at heart. If trained to be observant, they may report suspicious activity.

There is probably some utility to asking scientists to further develop concepts of the distinctions between applied fundamental research and developmental research. My sense is that the distinction is a little opaque, like the definition of "national security."[14] Executive Order 13526 or December 29, 2009, "Classified National Security Information," says that "scientific technological, or economic matters relating to the national security" may be classified, and it goes on to define national security as "the national defense or foreign relations of the United States."[15] That still is rather ambiguous. It is clear, however, that if a university or laboratory is conducting research for the government, it is up to the government to set the standards for who may have access to the research, how the research is to be protected (if at all), and how fundamental research is to be segregated from developmental research with national security applications.

Those distinctions cannot be left to the security or intelligence community alone, because generally the experts there are not involved in advanced scientific research. Any effort at

determining when or if to restrict access to scientific research must involve members of the scientific community and industry. Some things, however, may be self-evident. We probably might want to take a harder look at graduate students from Iran or North Korea working on advanced explosive research or applied nuclear physics.

One example for ways to better-identify potential espionage threats to our national security and to screen nationals of the countries posting such threats is provided by some of the language in S. 884, the "Deter Cyber Theft Act." In this bill, the Director of National Intelligence is directed to compile and report to Congress a list of foreign countries that engage in economic or industrial espionage and, among other things, a list of targeted technologies. Applying that approach to laboratories and universities engaged in advanced research would help oversight programs to be more cognizant of which foreign researchers get access to what government research projects. It would facilitate screening of foreign nationals working on government projects, and if the most critical technologies and processes for defense or national security application were prioritized, tell us where to be more discriminating in allowing foreign nationals access to research.

Finally, if there are new emerging technologies that require export controls to protect U.S. national security Congress should inquire as to what they are and oversee how such new controls are imposed.

---

[1] Micah Springut, Stephen Schlaiker, and David Chen, *China's Program for Science and Technology Modernization: Implications for American Competitiveness,* A report prepared by Centra Technology Inc., Arlington, VA (Washington, DC: U.S.-China Economic and Security Review Commission, 2011), 6.

[2] Susan M. Walcott, "Chinese Industrial and Science Parks: Bridging the Gap," ‖. *Professional Geographer* 54:349-364 (2002), http://libres.uncg.edu/ir/uncg/f/S_Walcott_Chinese_2002.pdf

[3] Springut, Schlaiker and Chen, *China's Program for Science and Technology Modernization*, 18.
[4] Federal Bureau of Investigation, *Counterintelligence, "*Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education," http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-and-national-security
[5] U.S. China Economic and Security Review Commission, *Annual Report 2007* (Washington, DC: November 2007), 104-106.
[6] U.S. China Economic and Security Review Commission, *Annual Report 2009* (Washington, DC: November 2007), 158-59.
[7] http://www.manufacturing.net/articles/2012/03/let-me-count-the-ways-china-is-stealing-our-secrets
[8] The White House, *National Security Decision Directive 198: The National Policy on the Transfer of Scientific, Technical and Engineering Information,* September 21, 1985.
[9] The Undersecretary of Defense, Memorandum on Fundamental Research, The Pentagon, Washington, DC, May 24, 2010.
[10] Subcommittee on Oceanography, Committee on Merchant Marine and Fisheries, House of Representatives, 98th Congress, Second Session, "U.S. Marine Scientific Research Capabilities Oversight," September 26, 1984, Serial 98-54.
[11] Office of the Under Secretary of Defense for Acquisition, technology and Logistics, *Report of the Defense Science Board Task Force on Basic Research* (Washington, DC: Department of Defense, January 2012.
[12] The Undersecretary of Defense, Fundamental Research, p. 2.
[13] Daniel Golden, "American Universities Infected by Foreign Spies Detected by FBI," *Bloomberg*, April 8, 2012 http://www.bloomberg.com/news/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi.html
[14] See Executive Order 13526 of December 29, 2009, "Classified National Security Information," *Federal Register*, 75:2, January 5, 2010, Part 1, Section 1.4 (e).
[15] Ibid, Part 6, (cc).