



U.S.-CHINA ECONOMIC & SECURITY REVIEW COMMISSION

WILLIAM A. REINSCH, CHAIRMAN
DENNIS C. SHEA, VICE CHAIRMAN

Representative Paul Broun, M.D.
Chairman
Subcommittee on Oversight
Committee on Science, Space and Technology
U.S. House of Representatives
2321 Rayburn House Office Building
Washington, DC 20515-6371

Dear Chairman Broun,

I am pleased to respond to your questions regarding my testimony before the Subcommittee on May 16, 2013. These responses represent my own views and not those of the U.S.-China Economic and Security Review Commission.

1. Does the U.S. have a comprehensive strategy of its own to counter China's robust, nationally-directed strategy to steal American technology and ingenuity? If not, what more should we be doing?

The United States has a comprehensive national counterintelligence strategy as provided for in the Counterintelligence Enhancement Act of 2002 (Public Law 107-306 of November 27, 2002). The National Counterintelligence Executive (NCIX) serves as the head of counterintelligence for the United States Government and reports to the Director of National Intelligence. The law also informed the Director of National Intelligence that it is the sense of the Congress that the DNI should seek the views of Attorney General, the Secretary of Defense, and the director of the Central Intelligence Agency in selecting the National Counterintelligence Executive.

The NCIX is responsible for producing a strategy for the counterintelligence programs of the United States, and that strategy must be updated every three years. The last update I was able to locate was dated 2009 (although it does not seem to have been published until 2010); therefore a new strategy may be in development. The 2009 counterintelligence strategy does not mention China specifically. However, I have met with the staff of the NCIX section responsible for China and East Asia a number of times. They are highly competent counterintelligence professionals drawn from across the intelligence community. In general, the strategies and reports to Congress from NCIX identify, characterize, and seek to address pervasive and global threats. Internally, and in classified strategies inside the intelligence community, the NCIX develops strategies specific to China. Some examples of NCIX documents are:

- The U.S. for the first time published the Counterintelligence National Strategy in 2005 to focus resources on the most serious current and emerging threats to U.S. technology and ingenuity. The strategy has several goals, one of which is to protect "U.S. advanced technologies and sensitive information in the defense, intelligence, economic, financial, public health, and science and technology sectors."
- In 2007 and 2009, the NCIX developed National Counterintelligence Strategies.

- In May of 2010 the National Counterintelligence Executive released the 2009 National Counterintelligence Strategy that identified the “protection of U.S. economic advantage, trade secrets and know-how” as a key component of the strategy.
- The Office of the National Counterintelligence Executive publishes a biannual report to congress titled Foreign Spies Steal U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic and Industrial Espionage, 2009-2011.

China’s espionage has become a far greater threat to the United States since the mid-1990s. This expanded threat is a result of Beijing’s increasing demand for strategic intelligence, its reliance on technical intelligence collection to support its national industrial development and science and technology plans, and expanding collection capabilities. As the number of Chinese students, researchers, academics, and businessmen working in the United States increases, it will become more difficult to discern a Chinese traditional or nontraditional collector from a legitimate entity due to the openness and ease with which academic and commercial business is conducted in the United States. Therefore, it is imperative that the U.S. develop a comprehensive and dynamic classified list of nations and actors that pose the most serious espionage threat to the U.S. government and industry.

Development of this list would require input and maintenance from throughout the U.S. Department of Defense and Intelligence Community. It almost certainly would include China, which was identified in the 2009 NCIX report on the theft of U.S. Economic Secrets as “the world’s most active and persistent perpetrators of economic espionage.” From this list, additional limitations on access to sensitive research or technology could be imposed on foreign individuals from those nations of concern. Though the entire document should remain classified, its key conclusions and recommendations should be released to the public when such release would not compromise intelligence sources and methods. Releasing as much of the document to the public as possible would help educate the staffs at academic institutions and laboratories and ensure they are aware of the threat posed by China.

I note that in the Reagan Administration, the Interagency Groups designed to coordinate national policy operated directly under the National Security Advisor. At that time there was an Interagency Group, Counterintelligence (IG/CI) with a full time director on the National Security Council (NSC). So far as I know, at the present time, there is no full-time NSC official with responsibility for U.S. counterintelligence (although there is a full-time cyber security director on the NSC).

Finally, Congress might want to examine the budget elements of the Foreign Counterintelligence Program (FCIP), which is under the budgetary control of the DNI to see if enough attention is devoted in the Program to China.

2. Concerning U.S. efforts to balance scientific cooperation and security, how would you define sensible policies vs. bad policies?

Sensible policies must promote open and collaborative academic and scientific research and exchange while protecting information that is moving from fundamental research into defense or industrial applications. 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. Also, sensible policies should recognize that certain nations have targeted programs to steal foreign technology.

Bad policies place too much weight on arguments that all scientific exchange must be open and do not recognize that there may be new, cutting edge innovations or research that has near-immediate application in the defense or national security sector. Finally, in my experience, bad policies often are associated with a bureaucratic approach by administrators who have no practical experience in the production of materials or systems and who do not understand the transition from fundamental ideas and research into applied experimental development.

3. How does the U.S. implement policies that protect our technologies and information while avoiding accusations of profiling?

In general, U.S. policy should focus on protecting technologies and information. For example, the U.S. could take the following measures:

- Ensure U.S. businesses are fully aware and compliant with laws and regulations pertaining to the release of export-controlled technologies to foreign nationals in the United States.
- Clearly codify distinctions between different levels of research, and then define security requirements – with consequences for negligence – for each level. With respect to China, and other countries with strong records of economic espionage, cyber espionage, theft of intellectual property, reverse engineering, and the proliferation of weapons, the U.S. should expand and refine the export-control system to refine the licensing and export of materials, equipment, and forms of technology, including dual-use technology. My view is that if a particular technology is ubiquitous, there is little reason to try to protect it under license. Whereas, if the U.S. or U.S. allies are far ahead in a technology area with direct military application, or a dual-use technology, then that technology may deserve protection.

However, I have no philosophical problem with profiling in counterintelligence programs. Indeed, decades of experience in intelligence collection and counterintelligence lead me to conclude that it is pretty dumb not to profile. If a nation has an established record globally of stealing intellectual property, abusing its citizens, coercing its citizens to steal property, and has no strong rule of law, it is fair to pay more attention to the nationals of that country.

Also, in intelligence collection, for decades the preferred method of operation for China's intelligence services has been to target Chinese nationals, ethnic Chinese in foreign countries, and the citizens of foreign countries with a strong attachment to China because of family connections, business investments, cultural interest, or academic interest. However, China's intelligence services recently has shown increased willingness to target individuals without ties to China who have access to information Beijing wants to collect. Therefore, in counterintelligence programs, it makes no sense to ignore these traditional methods of operations.

The U.S. should increase the public's awareness of China's use of students, scientists, and scholars attending U.S. universities and research universities as collectors on behalf of China, whether witting or unwitting. Beijing likely encourages Chinese students to study specific technology areas in the United States that support China's national research and development objectives. Any Chinese organizations associated with intelligence activities that sponsor academic research activities, social development, or international exchanges should be monitored and investigated.

4. What steps can our academic institutions and labs take to defend from attacks directed specifically at their cyber infrastructure, and can we share those suggestions to American businesses and government agencies?

Implementing security “best practices” almost certainly would reduce the effectiveness of Chinese cyber efforts. While not ensuring perfect security, such practices would make it more difficult for cyber actors to gain an initial foothold and maintain persistent access in the networks of academic institutions and labs. In particular, information systems housing research and development data that is likely destined for use in classified or unclassified national security programs (such as weapons) should be encouraged, or even required, to implement these best practices.

- Placing sensitive information on stand-alone networks rather than Internet-connected computers would cut off the most common method used by intruders to compromise and steal data from computer systems.
- Using multifactor authentication – generally a password in combination with a piece of hardware or biometric identifier – makes using stolen passwords difficult or impossible without also stealing or copying the physical authentication token.
- Encrypting data at rest and disabling unused ports and computer media would make it more difficult for intruders to conduct cyber-attacks.
- Enhancing user awareness of common social engineering tactics would help lessen the number of successful compromises.

China probably has the technical capability to compromise and extract data from closed academic and scientific institution networks by exploiting users who transfer files between Internet-connected and closed networks with removable media devices. China could face challenges conducting these “air gap attacks” against closed U.S. networks that have strong policies and procedures for moving data via removable media and examining it for malicious content.

Academic institutions and labs could cancel or limit their interactions with Chinese institutions and labs that are linked with Chinese cyber actors or who are known to have benefited from Chinese cyber activity or intellectual property theft.

The U.S. Government should publish and make available to laboratories and academic institutions a list of the known cover or proprietary organizations used by Chinese intelligence services as places of employment or study for intelligence collectors.

5. How can we prevent over classification and ensure that classifiers comply with existing criteria for classifying documents?

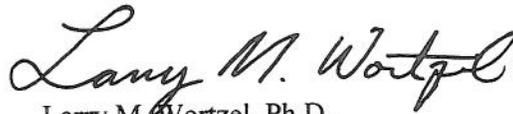
President Obama’s 2009 Executive Order No. 13526 acknowledges the need to prevent over classification. Nevertheless, there remains a significant gap between written guidelines on proper classification and the actual practice of classification. In recent reports addressing the issue, both the Brennan Center for Justice at New York University School of Law and the Public Interest Declassification Board suggest this gap is attributable to an environment that incentivizes risk-avoidance and over classification and provides no incentive to refrain from or challenge over classification. These reports make a number of recommendations, of which I believe the following are the most important:

- Introducing a minimal administrative burden upon original and derivative classifiers, such as a brief questionnaire asking these individuals to justify their classification, to counteract the tendency of rote classification.

- Incorporating occasional audits by the agency's Office of the Inspector General and stronger training programs to increase accountability into the accounting process.
- Implementing "safe harbor" or "hold harmless" rules for derivative classifiers who fail to follow original classification decisions when those decisions are not clearly conveyed. Distinguishing under classification in these instances with willful or negligent unauthorized disclosures. This recommendation could alter the tendency for such an individual to avoid the risk of and sanctions associated with under classification.
- As a corollary to the above, clarify the specific protections afforded intelligence sources and methods, particularly to derivative classifiers.

Thank you for the opportunity to respond to these questions. If I can be of any more assistance in matters regarding espionage threats against federal laboratories of federally funded research in academia please contact me.

Sincerely,

A handwritten signature in cursive script that reads "Larry M. Wortzel".

Larry M. Wortzel, Ph.D.
Commissioner