arrival, Li requested and was granted political asylum in the United States.[12] While he has not disclosed why the Chinese sent him to come to the United States as a graduate student, it is plausible the Chinese thought a student cover would make him more innocuous and able to collect information and make personal connections, or provide him with exposure and experience.

Send Unsolicited Email or Invitations

A foreign intelligence agent, business competitor, or other duplicitous actors may pose as a researcher and send an unsolicited email to a US researcher in the hopes of establishing contact or getting answers to a question. They may send unsolicited invitations to submit papers or attend conferences. They may use flattery or seek information that can be further used to target the researcher or someone with better access. Sometimes the unsolicited email is a request to review someone else's research or technology paper. In this case, the duplicitous actor is hoping the targeted professor will correct mistakes he/she sees in the provided paper and, in that way, obtain valuable insights and restricted information. Unlike computer intrusions, unsolicited email may not have attached malware but is an attempt to start a correspondence. It is a quick and cheap way to test whether a targeted person will respond and, if so, what subject will cause them to respond. If information can be obtained via simple email exchange, it will save time, effort, and money.

A possible scenario: A researcher at a US university receives an email asking to collaborate. He does not recognize the sender, but would like to collaborate and decides to respond. The sender asks for data on how to conduct a particular experiment, and the US researcher responds hoping to get the results of the experiment. The sender of the email provides a draft paper and asks for input; the US professor notes errors in the paper and corrects them. In the meantime, the sender asks for more data or research clarifications. Several months later, the US researcher realizes that for all the "collaboration" the two have been doing, he has no idea of the true identity or location of the sender, has received no information of value in return, and it now appears the sender was essentially milking the US researcher for unpublished and sensitive information.

Another possible scenario: A researcher receives an unsolicited invitation to submit a paper for an international conference. She submits a paper and it is accepted. At the conference, the hosts ask for a copy of her presentation. The hosts hook a thumb drive to her laptop, and unbeknownst to her, download every file and data source from her computer.

Fund or Establish Programs at a University

In 2005 Belgium's intelligence agency, Sûreté de l'Etat, announced the defection of a Chinese spy who had been coordinating industrial espionage agents throughout Europe for ten years. During that time, the defector worked at European universities and was a member of the Chinese Students and Scholars' Association of Leuven. "According to an intelligence official, the association enabled Beijing's Ministry of State Security to maintain contact with a wide spectrum of Chinese citizens living across the continent."[13] The defector gave the Sûreté de l'Etat the names and activities of hundreds of people who were supplying information to China from a variety of business organizations.

It is easier for a spy to operate in an environment where he is trusted than where he is scrutinized. An organization may donate money or goods to a university to establish cultural centers, fund academic programs, or facilitate joint research. The funding agency may place stipulations on how the programs or centers are run—stipulations that ultimately benefit that organization. The funding organization may be able to place their own recruits in positions with little or no oversight from the university. Donations also establish a good will attitude and build a sense of trust between the donating institution and the university.

How many foreign students are in the United States for duplicitous reasons?

Most foreign students, researchers, or professors studying or working at US universities are here for legitimate and proper reasons. Based on interviews, observations, defector information, and double-agent operations, the FBI concludes that only a small percentage of foreign students or visiting professors are actively working at the behest of their government or other organizations.

Why is the FBI concerned?

The FBI is mandated to protect the nation from internal and external threats. National security priorities include:

- Keep Weapons of Mass Destruction (WMD) from falling into the wrong hands
- Protect the secrets of US Government agencies and US contractors
- Protect US critical assets

Beyond these goals, there are laws and regulations that seek to safeguard intellectual property, protect personal information, and ensure that government funding is used appropriately. These laws help protect US businesses, universities, and individuals from theft and fraud. Ultimately, it is every university's responsibility to safeguard their information. The FBI is actively partnering with universities to assist in those efforts. The FBI can provide counterintelligence tools and awareness training that will aid in recognizing what is suspicious behavior and how to better protect facilities and information. If invited, the FBI will collaborate with a US university or college on a broad array of areas relating to:

- Cyber security
- The safety and integrity of higher education in the United States
- Intellectual property developed through US university research
- Sensitive and classified research
- Researchers' ability to get first-to-market with their ideas
- Research funded by the US Government—ultimately by the US taxpayers
- Keeping US students and professors from being recruited by foreign intelligence services
- Personal and sensitive information (identity theft, fraud, stolen research, and so forth)
- Campus safety and safety awareness of US students studying abroad
- Animal rights terrorism
- Eco rights terrorism

National Security Higher Education Advisory Board

The US Government created the National Security Higher Education Advisory Board (NSHEAB) in September 2005. It was designed to bridge historical gaps between the US Intelligence Community and academe with respect to national security issues and is comprised of approximately 20 presidents and chancellors who represent higher education institutions. The NSHEAB promotes cooperation and understanding between higher education and several government agencies to include the FBI.

Conclusion

Knowledge and information are valuable assets and are an integral part of university activities, but not all campus information is for public consumption. Individuals and organizations that want to obtain innovative or restricted information may have ulterior motives and may misrepresent themselves and their intentions in order to gain access to restricted information, or they may outright steal it. This white paper provides a sampling of means used by duplicitous actors and organizations. Universities and researchers should protect their intellectual property and be cognizant that there are dishonest actors and organizations that take advantage of the environment of sharing on US campuses of higher education.

Endnotes

[1] Associated Press, "Ex-Prof Gets 4 Years for Passing Military Secrets." 1 July 2009.

[2] Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America after the End of the Cold War* (New York: G.P. Putnam's Sons, 2007), 274.

[3] Scott W. Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy* (Annapolis MD: Naval Institute Press, 2007).

[4] Ginger Thompson, "Couple's Capital Ties Said to Veil Spying for Cuba." *New York Times* 19 June 2009. And United States Department of Justice. Press Release, "Former State Department Official and Wife Arrested for Serving as Illegal Agents of Cuba for Nearly 30 Years," 5 June 2009. And United States Department of Justice. Press Release, "Former State Department Official Sentenced to Life in Prison for Nearly 30-Year Espionage Conspiracy." 16 July 2010.

[5] United States Department of Justice Press Release, *Texas Resident Arrested on Charge of Attempted Use of Weapon of Mass Destruction.* 24 February 2011.

[6] *Comrade J,* 170-171.

[7] Bill Gertz, *Enemies: How America's Foes Steal Our Vital Secrets—and How We Let it Happen.* (New York: Crown Forum, 2006), 138.

[8] Evan Perez, "Alleged Russian Agent Claimed Official Was His Firm's Adviser." *The Wall Street Journal* 2 July 2010. And Naveen N. Srivatsa and Xi Yu. "Alleged Russian Spy Blends Into Harvard." *The Harvard Crimson* 30 June 2010.

[9] United States Department of Justice Affidavit, "US v Christopher R. Mestos et al," 1 June 2010.

[10] Ibid.

[11] Jose Cohen, "Castro's Intelligence Service and the US Academic Community." *ICCAS Monograph Series* January 2002.

[12] Jeff Stein, "Li Fengzhi, Ex-Chinese Spy, Granted Asylum." *The Washington Post* 5 October 2010. And Jeff Stein, "Li Fengzhi, Chinese Spy Who Defected to U.S., Facing Deportation." *The Washington Post* 2 September 2010.

[13] Damien McElroy, "China Aims Spy Network at Trade Secrets in Europe." *The Telegraph* 3 July 2005.

U.S. Department of Justice

Federal Bureau of Investigation

Counterintelligence Division

National Security Higher Education Advisory Board

National Security

Higher Education Advisory Board

American Council on Education
Arizona State University
Association of American Universities
Carnegie Mellon University
Cornell University
Duke University
Georgia Institute of Technology
Iowa State University
Michigan State University
New York University
Northwestern University
Rice University
The Pennsylvania State University
The State University of New York
University of California – Los Angeles
University of Colorado-Boulder
University of Florida
University of Maryland - College Park
University of Massachusetts
University of Rochester
University of Texas at Austin
University of Washington

Peter Lee

Peter Lee is the Head of the Computer Science Department at Carnegie Mellon University. He joined the faculty after completing his doctoral studies at the University of Michigan in 1987. Today he is a leading figure in computer science research, particularly in areas related to software security and reliability. An elected Fellow of the Association for Computing Machinery, several of his papers have received "test of time" awards for contributions that have demonstrated long-term impact. His work on "proof-carrying code" received the ACM SIGOPS Hall of Fame Award, for seminal contributions to computer systems research.

As the Head of the Computer Science Department, Peter Lee oversees one of the world's top research organizations, with over 80 faculty members (including two active Turing Award winners) and top-rated degree programs at both the doctoral and undergraduate levels. Prior to assuming his current position, Dr. Lee was briefly the Vice Provost for Research, where he provided administrative oversight and strategic guidance for the university's research activities, an enterprise that exceeds $450M in annual expenditures.

Peter Lee is called upon as an expert in diverse venues, including distinguished lectures at major universities, memberships on senior government advisory panels, and corporate advisory boards. Recently, he testified before the Science and Technology Committee off the U.S. House of Representatives. He is the incoming Chair of the Board of Directors of the Computing Research Association, member of the NRC Computer Science and Telecommunications Board and the Computing Community Consortium Council, and Vice-Chair of the Defense Advanced Research Projects Agency's Information Scienceand Technology Board.

Recent Significant Professional Activities:

Principal Investigator, Computing Innovation Fellows Project, May 2009 to present. Creating more than 100 research and higher education postdoctoral fellowships for new computing PhDs.
The National Academies, Computer Science and Telecommunications Board of the National Research Council (CSTB), September 2008 to present.
DARPA Information Science and Technology (ISAT) Board, September 2003 to present. Vice chair since August 2008.
Computing Research Association, March 2005 to present. Incoming Chair of the Board of Directors.
ACM SIGPLAN Executive Committee, 1997-1999, and again in 2005-present. Elected member.
DARPA Information Exploitation Office (IXO), Nov. 2003 to Aug. 2008. Member of the Senior Advisory Group.
Cedilla Systems Incorporated, Pittsburgh, November 1998 to December 2000. President and Co-founder (with George Necula). A security technology start-up.
Defense Science Board, March 2001 to September 2002. Co-chair, Technology Panel of the 2001 Summer Study on Defense Science and Technology.
Microsoft Corporation, December 1998 to March 2000. Expert Witness in the *Sun v. Microsoft* "Java lawsuit."

Assistant Director Marcus Thomas – Operational Technology Divisioin

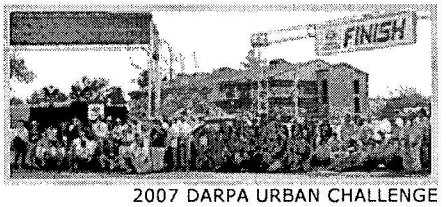
Mr. Thomas was born in 1962 in Chattanooga, Tennessee, and earned his Bachelor of Science in Engineering degree in 1985 from the University of Tennessee. Before entering the FBI, Mr. Thomas worked as a designer within the Nuclear power industry.
Mr. Thomas entered on duty as a Special Agent with the FBI on April 21, 1986 and served as a Special Agent for more than 21 years. Upon completion of training at Quantico, he was assigned to the Washington Field Office, where he worked Domestic Terrorism, Criminal Investigations, and Foreign Counterintelligence.
In 1991, Mr. Thomas was appointed as a Supervisory Special Agent to the Technical Services Division, a precursor to the present-day Operational Technology Division. Since that time, Mr. Thomas has held a variety of positions and responsibilities associated with providing technical support to field office investigative operations. These positions include Unit Chief (1996), Advanced Telephony Unit, Section Chief (2000), Cyber Technology Section, and Deputy Assistant Director (2002) of the Operational Technology Division. In December, 2006, he was named Assistant Director, Operational Technology Division. Mr. Thomas can be reached during duty hours at [redacted] b6 b7C
or via enterprise e-mail at [redacted]@fbinet.fbi.
Mr. Thomas resides in Stafford, Virginia and [redacted]

ABOUT DARPA

DARPA is the research and development office for the U.S. Department of Defense. DARPA's mission is to maintain technological superiority of the U.S. military and prevent technological surprise from harming our national security. We also create technological surprise for our adversaries.

DARPA funds unique and innovative research through the private sector, academic and other non-profit organizations as well as government labs.

DARPA research runs the gamut from conducting scientific investigations in a laboratory, to building full-scale prototypes of military systems. We fund research in biology, medicine, computer science, chemistry, physics, engineering, mathematics, material sciences, social sciences, neuroscience, and more.



2007 DARPA URBAN CHALLENGE

DARPA's First 50 Years

DARPA was established as a DoD agency in 1958 as America's response to the Soviet Union's launching of Sputnik. In the years since, DARPA's freedom to act quickly and decisively with high quality people has paid handsome dividends for DoD in terms of revolutionary military capabilities.

Today, America faces completely different threats and adversaries than it did when DARPA was established in 1958, and the Agency continually evolves to reflect this changing national security landscape. DARPA's proud history of achievement and its culture of excellence are testimony to the vital role the Agency has played in the nation's security and technological superiority.

Learn more about DARPA's history of innovation.