U.S. Department of Justice
Federal Bureau of Investigation

April 2011

Higher Education and National Security:

The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education

This white paper was prepared by the Counterintelligence Strategic Partnership Unit of the FBI.
This paper is unclassified in its entirety.

Foreword

This white paper was prepared by the FBI's Counterintelligence Strategic Partnership Unit to provide awareness to administrators, senior researchers, export control offices, and technology transfer offices at higher education institutions about how foreign intelligence services and non-state actors use US colleges and universities to further their intelligence and operational needs. This paper is unclassified and fulfills part of the FBI's goal of building awareness with public and private entities about counterintelligence risks and national security issues.

Executive Summary

The United States is a society of openness and freedom, values especially central to campuses of higher education. Foreign adversaries and competitors take advantage of that openness and have been doing so for many years.

There are foreign nations that seek to improve their economies and militaries by stealing intellectual property from a world technology leader like the United States. There are also foreign adversaries that seek to gain advantages over the United States. These nations use varied means to acquire information and technology to gain political, military, and economic advantages. There are also foreign companies and entrepreneurs who want to obtain research data in order to improve their own products or get to market first with innovative ideas or products being developed at US universities.

The open environment of US campuses of higher education may be misused in order to:

- Steal technical information or products
- Bypass expensive research and development
- Recruit individuals for espionage
- Exploit the student visa program for improper purposes
- Spread false information for political or other reasons

To accomplish one or more of the above goals, duplicitous or opportunistic actors or organizations may use a variety of methods such as:

- Conduct computer intrusions
- Collect sensitive research
- Utilize students or visiting professors to collect information
- Spot and recruit students or professors
- Send unsolicited email or invitations
- Send spies for language and cultural training, and to establish credentials
- Fund or establish programs at a university

Most foreign students, researchers, or professors studying or working in the United States are here for legitimate and proper reasons. Only a very small percentage is actively working at the behest of another government or organization. However, some foreign governments also pressure legitimate students to report information to intelligence officials, often using the promise of favors or threats to family members back home.

Higher Education and National Security

Introduction

American higher education institutions are centers of knowledge, discovery and intellectual exploration. The people of the United States value and take pride in the openness and opportunities for learning; they welcome foreign students and understand why other countries encourage and sponsor their own citizens to enroll in US universities. The knowledge, culture, and skills brought by foreign students enhance the educational experiences of other students and teachers. Due to globalization, today's college education is international in nature. Professors share their knowledge with students and colleagues—not just at their own university, but all over the world—and students from a variety of countries study together in the same program. Information is a valuable asset on campuses, and most of it is shared liberally; however, some information is private or restricted. Information that is not openly shared may include pre-publication research results, proprietary information, classified research, or certain lab techniques and processes.

Who tries to improperly obtain information from US campuses?

There are a variety of people and organizations within and outside the United States who may seek to improperly or illegally obtain information from US institutions of higher education: foreign and domestic businesses, individual entrepreneurs, competing academics, terrorist organizations, and foreign intelligence services.

Foreign and domestic businesses compete in a global economy. Some foreign governments provide resources and information, including competitive intelligence gathering and corporate espionage on behalf of their indigenous companies as a way to promote the overall economic well-being of their country. Foreign intelligence services pursue restricted information and so may seek out people who have, or will eventually have, access to restricted information. Individual entrepreneurs may capitalize on opportunities to bring new technology or services to their country in order to fill a niche currently supplied by non-native companies. To jump start business, they may steal research or products that would otherwise be costly to create or replicate. Academics may steal research and use it or claim it as their own for a variety of reasons. Terrorist organizations may want information on products or processes they can use to inflict mass casualties or damage.

What is a foreign intelligence service?

A foreign intelligence service is a foreign organization, usually part of the government, whose primary purpose is to gather and analyze information it deems valuable. Their ultimate goal for collecting information is to benefit their own country politically, militarily, and economically. Often the organization directs its agents to collect specific information on specific topics. An employee of an intelligence service who has been specially trained on how to collect and analyze information is an intelligence officer. The collected information or its analytic product is intelligence. Another purpose of a foreign intelligence service is to spread the

influence and ideology of its regime, or damage the claims and image of another regime. In this case, the intelligence service provides information. This may be done openly through propaganda, diplomatic statements, offers of training, or covertly using rumor, false-news stories, fabricated studies, bribery, or any number of other means.

Foreign intelligence services target information. To get to the information they will target people who have that information or who might be able to get the information in the future—someone with placement and access. The open environment of a university is an ideal place to find recruits, propose and nurture ideas, learn, and even steal research data, or place trainees who need to be exposed to our language and culture—a sort of on-the-job-training for future intelligence officers. Foreign intelligence services have been taking advantage of higher education institutions and personnel for many years, either through deliberate stratagems or by capitalizing on information obtained through other parties. Intelligence services are patient, sometimes waiting several years before expecting a return on an intelligence investment. Foreign intelligence services, by their nature, are secretive and unobtrusive. A successful operation by a foreign intelligence service is one where a target never knows they interacted with that service.

Why target university campuses?

To Obtain Restricted Information or Products

Despite university warnings on the restrictions on his research, University of Tennessee professor Reece Roth employed a Chinese and an Iranian student to assist in plasma research while working on a classified US Air Force project that stipulated no foreign nationals could work on the project. Roth also traveled to China with his laptop computer containing export-restricted information and had a sensitive research paper emailed to him there through a Chinese professor's email account. Roth claimed the research was "fundamental" and not sensitive, but a jury concluded otherwise.[1] In September 2008, Roth was found guilty on 18 counts of conspiracy, fraud, and violating the Arms Export Control Act; he was later sentenced to four years in prison. [Atmospheric Glow Technologies, the company set up to commercialize plasma research and the lab where the US Air Force project was researched, pled guilty to 10 counts of exporting defense-related materials.]

A country or company does not have to orchestrate the actual theft of the research in order to capitalize on it. It is unknown how the Chinese used the information they obtained from Roth, but because they invited him to visit China and he had a sensitive report emailed to him while there, it should be assumed they were interested in his research and planned to utilize it.

The US government has determined some technologies should not be shared with other countries because it would remove that technological edge that serves to protect the United States (militarily, economically, or otherwise), or the technology would be dangerous in the hands of certain groups. The knowledge of how to counter US technological advantages is also protected. Organizations that research, test, or manufacture restricted technologies may be enjoined from

Export restrictions of goods and technology

- US Department of Commerce Export Administration Regulations (EAR) - "Dual Use" items
- US Department of State International Traffic in Arms Regulations (ITAR) - Inherently "Military Use" items
- US Department of Treasury Office of Foreign Assets Control (OFAC) - Trade Embargoes

exporting them to other countries without first obtaining approval. Providing export-restricted items or information to a foreign national located in the United States may be regarded, under export control law, as equivalent to exporting the item or information because it is now in the actual possession of a foreign national.

To Bypass Expensive Research & Development

Sergei Tretyakov was the head of political intelligence for Russia's foreign intelligence service, the SVR [the *Sluzhba Vneshney Razvedki* is one component of the old Soviet KGB service], in New York City from 1995-2000. In other words, he was a Russian spy. He described how a man in California traveled to New York, met with an SVR agent, and handed over years of US government funded medical research. The research studies had not been released to the public because many of them contained proprietary information based on medical patents held by US companies. The man who provided the data to the SVR agent was a Russian immigrant who wanted to help Russia and refused to be paid for the information; however, he did agree to be reimbursed for his air travel. Tretyakov observed:

> The reports were extremely technical, and I noticed each had a dollar amount in the index that described exactly how much the US government had spent to pay for this research.…[Russia obtained] scientific research that cost the US government forty million dollars for the price of eight hundred dollars in airplane tickets![2]

As this case shows, a country or private company can save much time and money by bypassing research and development and jumping directly to an applied or practical application. Again, the organization does not have to direct someone to steal information in order to benefit from its theft. When a foreign company uses stolen data to produce products, at a reduced cost, that compete against American products, this can have direct harmful consequences for US businesses, and for universities that might receive revenue through patents and technology transfer.

While information is shared on campuses, there is still an ethical, and sometimes legal, responsibility to protect research. With the extensive amount of primary research done at universities, many researchers hope to gain recognition for innovative research. However, if their research is published by someone else first, they may lose that distinction and credit. Research is often funded by private companies or the government who may need a first-to-market practical application from the research to make it worth their investment. Stealing the research then could equate to stealing money from the funding organization.

To Find Recruits to Place in Valuable Positions

Ana Montes agreed to assist the Cuban Intelligence Service while she was a graduate student pursuing a master's degree in International Studies from Johns Hopkins University. Upon graduation, she specifically sought and obtained employment where she could acquire information valuable to Cuba. She worked as a Latin America analyst at the Defense Intelligence Agency and provided classified information to Cuba on a regular basis for sixteen years until she was arrested in 2001. Perhaps the worst damage of her spying was that Cuba shared the information she provided with other countries not friendly to the United States. It is also likely

her information contributed to the death and injury of American and pro-American forces in Latin America.[3] Not only did Montes provide information to the Cubans, but she shaped analysis and thereby influenced US policy toward Latin America. After her arrest, Montes claimed she spied for Cuba because she did not agree with US policy toward Cuba and Nicaragua in the 1980s. It is believed she voiced this opinion during graduate school, and someone alerted the Cuban Intelligence Service and recommended her as a potential recruit. She did not expect to be paid by the Cubans for her service and received very little remuneration from them. She is now serving 25 years in prison.

Ana Montes is an example of a spy motivated by ideology. US college campuses are an especially good place to look for people with particular ideological views. Campuses are known for their open discussions and debates. Foreign intelligence services sometimes find students with particular political or ideological beliefs by attending campus rallies, by interacting with particular clubs, or reading campus newspapers and blogs. When they discover someone they think will help, they may approach that person and entice him/her to join their cause.

Cuba has sought other ideological recruits. Kendall Myers worked as an adjunct professor at Johns Hopkins University School of Advanced International Studies and as a contract instructor at the State Department's Foreign Service Institute. Intrigued by Cuba, he accepted an invitation to visit. The Cubans assessed Myers as one who would help Cuba, and recruited him as a spy. They encouraged Myers to get a job with the State Department or the CIA. Myers returned to being an instructor with the State Department in 1980, and eventually worked full-time in the State Department's Bureau of Intelligence and Research until he retired in 2007. Myers took classified information and, with the help of his wife, passed it to Cuba. He and his wife were arrested in June 2009 and pled guilty to serving as illegal agents of Cuba for nearly thirty years. Myers was sentenced to life in prison and his wife was sentenced to 81 months.[4]

While it is not a crime in the United States to hold particular political or ideological ideals, it is a crime to pass classified information to those not authorized to receive it. Both Montes and Myers specifically sought positions within US government agencies that gave them greater access to classified information with the goal of passing that information to a foreign nation.

Foreign intelligence services use a variety of enticements to recruit spies: money, blackmail, revenge, and flattery, for example.

To Exploit the Student Visa Program for Improper Purposes

Khalid Ali-M Aldawsari, a Saudi student studying chemical engineering at Texas Tech University, was arrested in February 2011 on a charge of attempted use of a weapon of mass destruction. A notebook was found at Aldawsari's residence that appeared to be a diary or journal:

> [E]xcerpts indicate that Aldawsari had been planning to commit a terrorist attack in the United States for years. One entry describes how Aldawsari sought and obtained a particular scholarship because it allowed him to come directly to the United States and helped him financially, which he said "will help tremendously in providing me with the support I need for Jihad."[5]

To Spread False Information for Political or Other Reasons

According to Sergei Tretyakov, a former KGB/SVR officer, the KGB ordered the Soviet Academy of Sciences to come up with a report that would scare the Western public and keep NATO from placing Pershing missiles in Western Europe:

> The story, which had been approved by KGB propagandists, described experiments in the Karakum desert in South Central Asia that were being done by a Soviet specialist in atmospheric physics… [Other Soviet] scientists claimed they had used a mathematical model to estimate how much dirt and debris would be blasted into the atmosphere during a nuclear attack in Germany.[6]

The KGB had the report published in a Swedish journal. In the intelligence world, this is called disinformation. Disinformation may be blatant deception or small fabricated kernels in a large milieu of reliable facts. In the academic arena where research is often based on previous research, when results from a study can be shared quickly and easily with other researchers, it is important to science that people share *accurate* results. If subsequent research is based on incorrect data, many of those subsequent conclusions could be inaccurate as well. Expanding scientific horizons is not always the main motivating factors for research or publications in other countries. Foreign researchers may be under pressure to make their research conclude what their government wants it to conclude, or they may be ordered to write completely fabricated studies.

What methods are used to target information at US universities?

Conduct Computer Intrusions

Today's computer-connected world provides abundant access for criminals, terrorists, opportunists, and intelligence services to exploit the access cyber networks afford. They can hack into a system and steal research and other information, send phishing email with malware attached, and exploit social networking sites. They search for restricted information, people who have access to the information, and information that can be used to coerce or entice people with access to share restricted data. There have been computer intrusions into US universities from numerous countries. US universities receive large numbers of unsolicited requests for information and millions of hits on their Web servers each day. Computer hackers, especially those funded by a foreign government, are capable of breaching firewalls and exploiting vulnerabilities in software. They are also skilled at deceiving trusting or unassuming individuals through scams.

Collect Sensitive Research

A possible scenario: An Asian student gets accepted into a graduate program at a US university. The student has connections with a research group at a university back in Asia and is allowed to establish a formal collaboration between the two research labs. The Asian student invites personnel from the Asian university lab to visit the US university. Without permission, the visitors take photographs of all the equipment in the lab including the make and model of the equipment in order to reproduce the US university's lab at the Asian university. About a year into the collaboration, the graduate advisor becomes concerned that too much information is

going out to the Asian research lab and not enough is coming back to the US university. Although the research is unrestricted, the graduate advisor recognizes that applications of the research could have national security implications. The Asian lab has more resources and is able to follow-up on ideas more quickly but the sharing of data and results is unbalanced, so the graduate advisor decides to end the collaboration.

Sometimes, as research develops, the application of that knowledge leads to products that have national security implications. Defectors and double-agent operations have affirmed intelligence services are very interested in acquiring technologies during the research and development phase regardless of classification,[7] since the application and new research may later become classified.

Utilize Students or Visiting Professors to Collect Information

Andrey Bezrukov was arrested in June 2010 for being an agent of Russia. He was a spy who entered the United States under an assumed name (Donald Heathfield) and false past. He attended Harvard's Kennedy School of Government from 1999-2000 and earned a Masters in Public Administration. After graduating, Bezrukov developed associations with professors at various universities including George Washington University and Oxford University. He allegedly targeted a professor who was once Al Gore's national security advisor. Bezrukov also attended Kennedy School reunions, specific society meetings, and think tank events that gave him access and exposure to people as he socialized with policy-makers and tried to cultivate intelligence targets.[8]

In this case, Russia sent a spy to a US university in order for him to cultivate friendships and associations with students and professors likely to move on to government positions. He therefore had a seemingly innocent basis to get off-the-record and inside information from any "friend" in a position with access to information.

Some countries may recruit students before they come to the United States and task them to send technological information they acquire back to their home country. Students may comply based upon a sense of loyalty for their home country's government or as a result of coercion and exploitation. In some instances, foreign students are funded by their government and therefore can serve, at no cost to the US university, as assistants to professors doing research in a targeted field, which gives the student access to the research data and its applications. Some countries may direct the student to seek US citizenship giving them greater access to restricted research. Most information taught at universities is available to anyone who enrolls. However, when information is classified, patented, proprietary, or export restricted, there are rules and laws imposed to protect and control that information.

Foreign business competitors may also send employees as students in order to obtain information valuable to their company. They may misrepresent themselves as students and not acknowledge their employment with a foreign company. A possible scenario: In order to obtain competitive intelligence or insider information on Business A, Business B has one of their employees apply and enroll in a program at a university that is doing research for and funded by their competitor, Business A. That employee/student may even apply for an internship at Business A. The unsuspecting Business A would not imagine a student intern was already a full employee of their competitor.

Spot Students or Professors with Access

In 2009, Russia sent the following instructions to one of its spies, Lidiya Gurveva (using the name Cynthia Murphy), while she was pursuing an MBA degree at Columbia Business School, Columbia University:

> [S]trengthen…ties w. classmates on daily basis incl. professors who can help in job search and who will have (or already have) access to secret info… [r]eport to C[enter] on their detailed personal data and character traits w. preliminary conclusions about their potential (vulnerability) to be recruited by Service.[9]

They also directed her to " 'dig up' personal data of those students who apply (or are hired already) for a job at CIA."[10] Guryeva was arrested in June 2010 for acting as an agent of a foreign power and was deported back to Russia.

This example demonstrates a foreign intelligence service searching for students who may soon have access to targeted information. Intelligence services also collect information on the programs, officers, professors, and demographics of US universities. After studying the information and, if they find a person to target, they will study his/her motivations, weaknesses, politics, and ambitions. Familiarizing themselves with a professor's work will help them determine a pretext for contacting the professor and how best to influence or recruit the professor.[11] They may spend years targeting an individual, and develop a relationship whereby the student or professor provides information, either wittingly or unwittingly, to the foreign country. For example, the foreign intelligence service may capitalize on existing political or social biases whereby they can coax a professor to share information based on a real or perceived cause (e.g. Myers). They may appeal to the ethnic nationality of a student and ask him/her to help their ancestral homeland. They may invite a professor to visit their country (e.g. Roth), sometimes at no expense to the professor. While the professor is in country, the government may gain access to the professor's digital storage devices (laptop, PDA, cell phone) and obtain sensitive research and personal information. The foreign intelligence service may use information to coerce or entice the professor to provide data in the future. Likewise, American students on study abroad may be evaluated as potential recruits by the host country's intelligence service.

Foreign agents often target students or professors from their own country first, anticipating they will agree out of a sense of patriotism or nationalism. However, they will also target anyone who appears to have the potential to be a good recruit.

Send Spies for Language and Cultural Training and to Establish Credentials

As discussed above with Bezrukov and Guryeva, some foreign students are not here in order to obtain a traditional university education. They attend college in the United States to increase their understanding of the language and culture, make contacts, gain an education in a particular field, and send information back to their home country. In some cases, they may lay low and do nothing criminal for several years.

Li Fengzhi was a Chinese intelligence agent for thirteen years before the Chinese Ministry of State Security sent him to the United States, in 2003, to pursue a doctoral degree in international politics and diplomatic philosophy at the University of Denver. Shortly after his

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.