U.S. Department of Justice
Federal Bureau of Investigation

April 2011

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 higv csand freedom

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

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, the successor 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 senta f -16e5 Tw 8lp,5yr-19.72usi he

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 experim

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

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 Emails 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

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.