

Bloomberg

American Universities Infected by Foreign Spies Detected by FBI

By Daniel Golden - Apr 8, 2012

Michigan State University President Lou Anna K. Simon contacted the Central Intelligence Agency in late 2009 with an urgent question.

The school's campus in [Dubai](#) needed a bailout and an unlikely savior had stepped forward: a Dubai-based company that offered to provide money and students.

Simon was tempted. She also worried that the company, which had investors from [Iran](#) and wanted to recruit students from there, might be a front for the Iranian government, she said. If so, an agreement could violate federal trade sanctions and invite enemy spies.

The CIA couldn't confirm that the company wasn't an arm of Iran's government. Simon rejected the offer and shut down undergraduate programs in Dubai, at a loss of \$3.7 million.

Harkening back to Cold War anxieties, growing signs of [spying on U.S. universities](#) are alarming national security officials. As schools become more global in their locations and student populations, their culture of openness and international collaboration makes them increasingly vulnerable to theft of research conducted for the government and industry.

"We have intelligence and cases indicating that U.S. universities are indeed a target of foreign intelligence services," Frank Figliuzzi, [Federal Bureau](#) of Investigation assistant director for counterintelligence, said in a February interview in the bureau's Washington headquarters.

'Academic Solicitation'

While overshadowed by espionage against corporations, efforts by foreign countries to penetrate universities have increased in the past five years, Figliuzzi said. The FBI and academia, which have often been at loggerheads, are working together to combat the threat, he said.

Attempts by countries in East Asia, including China, to obtain classified or proprietary information by "academic solicitation," such as requests to review academic papers or study with professors, jumped eightfold in 2010 from a year earlier, according to a 2011 U.S. [Defense Department report](#). Such approaches from the [Middle East](#) doubled, it said.

“Placing academics at U.S. research institutions under the guise of legitimate research offers access to developing U.S. technologies and cutting-edge research” in such areas as information systems, lasers, aeronautics and underwater robots, the report said.

World-Class Talent

Welcoming world-class talent to American universities helps the U.S. sustain global supremacy in science and technology, said University of Maryland President Wallace Loh. He chairs the U.S. Department of Homeland Security’s academic advisory council, which held its first meeting March 20 and is expected to address such topics as federal tracking of international students.

Foreign countries “can never become competitive by stealing,” he said. “Once you exhaust that technology, you have to start developing the next generation.”

Foreigners on temporary visas made up 46 percent of science and engineering graduate students at [Georgia Institute of Technology](#) and Michigan State and 41 percent at Massachusetts Institute of Technology in 2009, according to a federal survey. [China](#) sent 76,830 graduate students to U.S. universities in 2010-2011, more than any other country and up almost 16 percent from the prior year, according to the Institute of International Education in [New York](#).

Finding Recruits

While most international students, researchers and professors come to the U.S. for legitimate reasons, universities are an “ideal place” for foreign intelligence services “to find recruits, propose and nurture ideas, learn and even steal research data, or place trainees,” according to a 2011 [FBI report](#).

In one instance described in the report, the hosts of an international conference invited a U.S. researcher to submit a paper. When she gave her talk at the conference, they requested a copy, hooked a thumb drive to her laptop and downloaded every file. In another, an Asian graduate student arranged for researchers back home to visit an American university lab and take unauthorized photos of equipment so they could reconstruct it, the report said.

A foreign scientist’s military background or purpose isn’t always apparent. Accustomed to hosting visiting scholars, Professor Daniel J. Scheeres didn’t hesitate to grant a request several years ago by Yu Xiaohong to study with him at the [University of Michigan](#). She expressed a “pretty general interest” in Scheeres’s work on topics such as movement of celestial bodies in space, he said in a telephone interview.

Unaware of Credentials

She cited an affiliation with the [Chinese Academy of Sciences](#), a civilian organization, Scheeres said. The Beijing address Yu listed in the [Michigan](#) online directory is the same as the Academy of Equipment Command & Technology, where instructors train Chinese military cadets and officers. Scheeres said he wasn’t aware of that military connection, nor that Yu co-wrote a 2004 article on improving the precision of anti- satellite weapons.

Once Yu arrived, her questions made him uncomfortable, said Scheeres, who now teaches at the [University of](#)

[Colorado](#). As a result, he stopped accepting visiting scholars from China.

“It was pretty clear to me that the stuff she was interested in probably had some military satellite-orbit applications,” he said. “Once I saw that, I didn’t really tell her anything new, or anything that couldn’t be published. I didn’t engage that deeply with her.”

Wrote About NASA

Yu later wrote a paper on the implications for space warfare of the NASA Deep Impact mission, which sent a spacecraft to collide with a comet. She couldn’t be reached for comment.

American universities have also trained Chinese researchers who later committed corporate espionage. Hanjuan Jin, a former software engineer at Motorola Inc., was found guilty in February in federal court of stealing the Schaumburg, Illinois-based company’s trade secrets and acquitted of charges she did so to benefit China’s military. She is scheduled for sentencing in May and has also filed a motion for a new trial.

Jin joined the company, now known as [Motorola Solutions Inc. \(MOT\)](#), after earning a master’s degree from the University of [Notre Dame](#) in South Bend, [Indiana](#). While at Motorola, she received a second master’s, this time in computer science, from the [Illinois Institute of Technology](#) in [Chicago](#). IIT’s own research wasn’t compromised, institute spokesman Evan Venie said in an e-mail. A Notre Dame spokesman declined to comment.

Study Abroad Targets

More Americans are heading overseas for schooling, becoming potential targets for intelligence services, Figliuzzi said. More than [270,000 Americans](#) studied abroad for credit in 2009- 2010, up 4 percent from the year before. President Barack Obama has announced an initiative to send 100,000 American students to China, and China has committed 10,000 scholarships for them.

As a junior at Grand Valley State University in Allendale, Michigan, Glenn Duffie Shriver studied at East China Normal University in [Shanghai](#). After graduation, he fell in with Chinese agents, who paid him more than \$70,000. At their request, he returned to the U.S. and applied for jobs in the State Department and the CIA. He was sentenced to four years in prison in January 2011 after pleading guilty to conspiring to provide national-defense information to intelligence officers of the People’s Republic of China.

“Study-abroad programs are an attractive target. Foreign security services find young, bright U.S. kids in science or politics, it’s worth winning them over,” Figliuzzi said.

Front Companies

Unlike its counterparts in other countries, which rely on their own operatives, China’s intelligence [service](#) deploys a freelance network including students, researchers and false- front companies, said David Major, president of the Centre for Counterintelligence and Security Studies in Falls Church, [Virginia](#) and a former FBI official.

China has “lots of students who either are forced to or volunteer to collect information,” he said. “I’ve heard it said, ‘If it wanted to steal a beach, [Russia](#) would send a forklift. China would send a thousand people who would pick up a grain of sand at a time.’”

China also has more than 3,000 front companies in the U.S. “for the sole purpose of acquiring our technology,” former CIA officer S. Eugene Poteat, president of the Association of Former Intelligence Officers in McLean, Virginia, wrote in the fall/winter 2006-2007 edition of “Intelligencer: Journal of U.S. Intelligence Studies.”

U.S. and Canadian universities reaped \$2.5 billion in 2011 from licensing technology, up from \$222 million in 1991, according to the [Association of University Technology Managers](#) in Deerfield, Illinois.

‘Opened Some Eyes’

Universities “may not fully grasp exactly who they’re spinning off their inventions to,” Figliuzzi said. “The company could be a front for a foreign power, and often is. We share specific intelligence with university presidents, and we’ve opened some eyes.”

Michigan State’s Simon learned to be wary of front companies by serving on the National Security Higher Education Advisory Board, established by the FBI and CIA in 2005. It “makes you more aware that you need to look below the surface of some of these offers,” she said. “A short-term solution may turn into an institutional embarrassment.”

[Arizona](#) State University President Michael Crow also sits on the board. “It’s all a little perplexing and overwhelming,” he said. “We’re in the business of trying to recruit more students from China. We’re operating at a total openness mode, while we recognize there are people working beyond the rules to acquire information.”

The Chinese embassy in [Washington](#) and the Ministry of Foreign Affairs in Beijing didn’t respond to e-mailed questions.

Enabling China

Over the years, American universities have enabled China “to leapfrog into the cutting edge of military capability on the way to superpower status,” Richard Fisher, senior fellow on Asian Military Affairs at the International Assessment and Strategy Center in Alexandria, Virginia, said in an e-mail.

Chen Dingchang, the head of a Chinese military-sponsored working group on anti-satellite technology, led a delegation in 1998 to the University of [Florida](#) to learn about diamond-coating manufacturing, used in missile seekers and other systems, said Mark Stokes, executive director of the [Project 2049](#) Institute in Arlington, Virginia, which studies Chinese aerospace technology. In a 1999 report in a Chinese journal, the authors, including Chen, said the university’s cooperation would assist in overcoming a technical bottleneck in China’s development of anti-satellite warheads.

‘Unlikely to Advertise’

“A university may not know that a visiting engineer could be conducting sponsored research on a military program that could hurt Americans in the event of a conflict,” Stokes said. “An engineer supporting a People’s Liberation Army program is unlikely to advertise his or her purpose.”

The University of Florida is “unable to verify” the incident, spokesman Stephen Orlando said.

Chen is a technology adviser at China Aerospace Science and Industry Corp., which didn’t respond to an interview request.

University administrators have traditionally viewed their role as safeguarding academic freedom and making sure that all students, domestic or foreign, are treated the same.

“I’ve been to campuses where deans would say to Chinese students, ‘The FBI is coming to talk to you. You have no responsibility to talk to them,’” Major said. “Very hostile environments.”

Some faculty members remain uneasy about a partnership with federal investigators. “The FBI thrives on a certain degree of paranoia, and it operates in secrecy,” said [David Gibbs](#), a history professor at the University of Arizona. “The secrecy goes against so much of what universities are about, which is openness and transparency.”

Stanford University

[Stanford University](#) avoids seeking contracts for “export- controlled” research, which only Americans can work on without a license because it has implications for economic or national security.

“Stanford does not, nor will it, restrict participation of students on the basis of citizenship,” President John Hennessy testified at a January 2010, congressional hearing in Palo Alto, [California](#). More than half of Stanford’s doctoral candidates in the physical sciences and engineering come from outside the U.S., he said.

Asked by Dana Rohrabacher, a Republican congressman from California, if he had read that Chinese military intelligence uses Chinese students, Hennessy said, “I am aware of that.”

“Universities need to think that they are patriotic Americans, too,” Rohrabacher responded.

Hennessy is on sabbatical and unavailable to comment, Lisa Lapin, a Stanford spokeswoman, said in an e-mail.

More Collaboration

After becoming Pennsylvania State University president in 1995, Graham Spanier sought closer collaboration with law enforcement. Reading that a president at another state university expressed shock that a faculty member was under investigation for terrorist ties, he resolved not to be similarly taken aback. He arranged a meeting with representatives of national security agencies including the FBI, CIA, Secret Service and Naval Criminal Investigative Service.

“This had never occurred before,” Spanier said in a phone interview. “Nobody from higher education had reached

out.”

If they were making inquiries at Penn State, they should let him know, and he would help, Spanier told them. “That began a very fruitful collaboration,” he said.

Shifting priorities after the Sept. 11, 2001, attacks to terrorism and espionage from organized crime and kidnapping, the FBI expanded the Penn State model into a national board.

Handpicked Board

Spanier approached other university presidents, and 90 percent agreed to serve, he said. Michigan State’s Simon took over as chair after Spanier stepped down as Penn State president last November in the wake of a scandal over sex-abuse allegations against a former assistant football coach. Simon and the FBI and CIA have agreed to expand the board and start a subcommittee on cyber-hacking.

The FBI handpicks universities for the board, Figliuzzi said. It looks at how much research they conduct, as well as “sensitive cases -- where is there a potential problem? Then we make an invitation.”

Board members must have security clearances. FBI officials brief them about cases on their campuses, and the presidents in return guide federal investigators through the thickets of higher education.

Problem Solved

When a foreign entity compromised the computer system of a major university, the bureau contacted the school’s information- technology administrators, who denied that they had a security breach. The FBI consulted Spanier, who persuaded the university’s president to meet with the bureau.

“That opened the door to a higher level of cooperation,” he said. “The problem was solved.”

Similarly, the bureau warned Simon that research in behavioral science by a foreign graduate student at Michigan State “might breach the security of corporate America,” she said. “We were able to find a way for the student to complete his research and still modify it in a way that took away the national security issues.”

Beyond resolving such cases, the FBI has also alerted board members to the overall threat, most dramatically through a presentation by a former Russian spy. As a colonel in Russian intelligence and its deputy resident in New York from 1995 to 2000, Sergei Tretyakov set his sights on [Columbia University](#) and New York University, according to “Comrade J: The Untold Secrets of Russia’s Master Spy in America After the End of the [Cold War](#)” (2008), by Pete Earley.

Mingled With Professors

“We often targeted academics because their job was to share knowledge and information by teaching it to others, and this made them less guarded than, say, UN diplomats,” Earley quoted Tretyakov as saying. A typical task was to

obtain information about “a study of genetically engineered food being done at New York University.”

At the board meeting, Tretyakov described to the presidents how Russian spies used to go to campus events and mingle with professors. “It certainly seemed very bold to me that they felt they could interact with faculty and students and attend seminars,” Spanier said. “We never really think about that happening on our campuses.”

In 2009, around the time Tretyakov was briefing the presidents, a Russian spy, Lidiya Guryeva, was pursuing a master’s degree in business at Columbia under the name [Cynthia Murphy](#), the 2011 FBI report said. Russian intelligence instructed her to strengthen “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,” and to report on their potential “to be recruited by Service.”

Columbia and NYU declined to comment.

Tretyakov died in June 2010. That month, Guryeva was arrested for acting as an agent of a foreign power and deported to Russia.

To contact the reporter on this story: Dan Golden in Boston at dlgolden@bloomberg.net

To contact the editor responsible for this story: Lisa Wolfson at lwolfson@bloomberg.net; Jonathan Kaufman at jkaufman17@bloomberg.net

©2012 BLOOMBERG L.P. ALL RIGHTS RESERVED.