WSJ.com THE WALL STREET JOURNAL. ONLINE

Phantom Menace

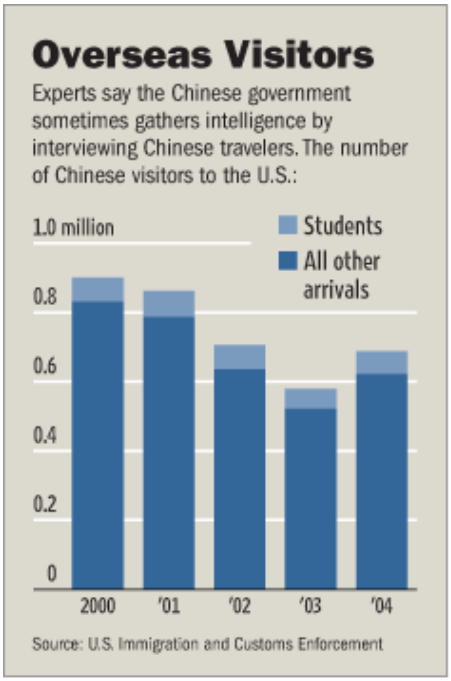
FBI Sees Big Threat From Chinese Spies; Businesses Wonder

Bureau Adds Manpower, Builds Technology-Theft Cases; Charges of Racial Profiling Mixed Feelings at 3DGeo

By JAY SOLOMON
Staff Reporter of THE WALL STREET JOURNAL
August 10, 2005; Page A1

WASHINGTON -- Back in the 1980s, David Szady was among the premier Soviet spy catchers at the Federal Bureau of Investigation, studying every aspect of the Kremlin's mole network. Today, he's mobilizing agents across the country to sniff out spies from a new rival: Beijing.

"China is the biggest [espionage] threat to the U.S. today," says Mr. Szady, now 61 years old and assistant director of the FBI's counterintelligence division.



In one of their biggest initiatives after the fight against terrorism, the FBI and Justice Department have sent hundreds of new counterintelligence agents into the bureau's 56 field offices, many with a specific focus on China. There is a cloak-and-dagger element to some of this: A principal FBI team focusing on Chinese economic espionage, including some undercover operatives, occupies an unmarked floor in a Silicon Valley office park near a popular Chinese restaurant.

But this is an altogether different battle from the one with the Soviets. Thousands of Chinese nationals regularly come to the U.S. as students and businessmen, some working for major U.S. defense contractors -- something the Russians could only have dreamed of during the Cold War. They are welcomed with open arms by universities and companies who prize their technical acumen and links to capital and low-cost labor back home.

The vast majority of them are here innocently working or studying. Counterespionage experts say the trouble often starts when they are contacted by Chinese government officials or one of the more than 3,000 Chinese "front companies" the FBI alleges have been set up in the U.S. specifically to acquire military or industrial technologies illegally. Sometimes they are wooed with cash, but often the motivation is nationalism.

"They can work on so many levels that China may prove more difficult to contain than the Russian threat," Mr. Szady says.

Even as concerns mount in Washington about China's growing economic and military might, the government faces charges of racial profiling from Asian-American advocacy groups and ambivalence

from some business groups. Working with sometimes vague laws on technology exports, it is having trouble making some of its cases stick.

The government is currently prosecuting about a dozen cases against individuals alleged to have sent technology -- sometimes designs, sometimes software, sometimes high-tech equipment -- to China illegally. FBI officials say at least three more cases will likely go ahead in the coming months. Over the past five years, the total number of such charges has grown by around 15% annually, according to some FBI agents.

Most of the cases involve small, lesser-known tech firms. But **Sun Microsystems** Inc. and **Transmeta** Corp. were the targets in one alleged plot, where two Chinese nationals who had worked at the software and semiconductor giants were arrested at the San Francisco airport allegedly holding proprietary data from the companies. The pair were charged with economic espionage and the case is pending. The FBI's Business Alliance, established a year ago, has been meeting regularly with leading defense contractors to understand what technologies they're developing and what potential threats are posed by company employees. The participants include **Lockheed Martin** Corp., **General Dynamics** Corp. and **Raytheon** Co.

Growing Threat

The FBI campaign is part of a broader shift in Washington, where more and more policy makers see China's rapid economic rise as a threat to the U.S. both militarily and economically. That growing sentiment is seen in the heated debate over the recent failed bid by China's state-owned oil company **Cnooc** Ltd. for California's **Unocal** Corp. The Pentagon has caused a stir in recent months by raising the prospect that China's secretive military buildup could pose a significant long-term threat to Asia and the U.S.

Chu Maoming, the spokesman for the Chinese embassy in Washington, calls the FBI's assertion that Beijing is coordinating spying activities inside the U.S. "totally groundless."

Many people in Silicon Valley are concerned that the FBI is overreaching. Asian-Americans worry about a new wave of racial profiling and say the crackdown is reminiscent of the 2000 case of Wen Ho Lee, a Taiwan-born American scientist who was fired from his job at Los Alamos National Laboratory and was prosecuted for allegedly giving away nuclear secrets to Beijing. After months in solitary confinement, all the espionage charges were eventually dropped, though Mr. Lee pleaded guilty to a lesser charge of mishandling top-secret information.

Business executives, meanwhile, fear a chill in commerce. "There's a bit of a disconnect between how the law-enforcement agencies see" the risk of espionage and how the business community does, says Harris Miller, the Arlington, Va.-based president of the Information Technology Association of America, one of the high-tech industry's principal lobbying groups. He says many U.S. companies are dependent upon manufacturing and conducting research in places like China -- and on the talents of Chinese employees.

"There's a real advantage to work with foreign nationals, as they're very talented," Mr. Miller says. "You don't want to turn them away just because they are not born in the U.S."

Even some of the victims of alleged Chinese espionage have mixed feelings about the FBI's campaign.

Software maker 3DGeo Development Inc. suspected it had a spy problem when it brought in for training Yan Ming Shan, an employee of one of 3DGeo's clients, state-owned oil company **PetroChina** Co. The

Chinese oil giant had earlier sent an employee to train at 3DGeo's Santa Clara, Calif., campus, but he was ejected after trying to gain access to the software company's secured systems. Mr. Shan then appeared and was expelled after doing the same thing. Mr. Shan was later arrested at San Francisco International Airport and accused of seeking to pass on some of 3DGeo's proprietary software programs to PetroChina.

Mr. Shan, a Chinese national, was sentenced last December to two years in prison for illegally accessing 3DGeo's computers.

Dimitri Bevc, 3DGeo's president, says the episode highlights a dilemma for the company, which is seeking to secure its intellectual property but also expand its business in Asia. "There's incredible demand from Chinese firms that are hungry for technology," says Mr. Bevc. "But we are built on our own intellectual property."

Now Mr. Bevc is afraid his company is being punished in the Chinese marketplace. The company is still seeking payments from PetroChina for work completed in September 2001, says Mr. Bevc. Meanwhile, 3DGeo's sales representative told Mr. Bevc his Chinese sales prospects have been drying up. "What we heard back was...that 3DGeo did something wrong" by taking action against Mr. Shan, who served most of his sentence while awaiting trial and has since returned to China, says Mr. Bevc.

PetroChina declined to comment on the case. Nicholas Humy, an attorney for Mr. Shan, said his client pleaded guilty only to illegally accessing 3DGeo's computer system and not to stealing the company's software or seeking to pass it on to a foreign entity. "The government never proved to a jury...that Mr. Shan was trying to commit industrial espionage," Mr. Humy said.

October Trial

On the military side, prosecutors at the San Jose, Calif., offices of the Department of Justice are preparing for an October trial of two Silicon Valley residents. The pair were indicted in June 2004 for allegedly signing contracts with Chinese military-related entities to provide high-tech gear and consulting work for the mass production of thermal-imaging cameras. Technology industry officials say the case highlights the murkiness of export laws.

The case involves Night Vision Technology Corp., a San Jose-based firm that procures infrared technology and other high-tech equipment for overseas buyers, particularly in Taiwan. The company is headed by Martin Shih, 62, a Taiwanese-Canadian executive with wide experience as an electrical engineer, working both in Canada and in California with satellite-communications company Loral Space & Communications Ltd. Mr. Shih's Taiwanese-American consultant, Philip Cheng, was also charged.

Pretrial motions filed by the two men's attorneys speak to the belief of many in the technology industry that U.S. laws guarding technology exports are difficult to interpret because so often the technologies have legitimate commercial applications. They also say products like infrared cameras can't be blocked for export because they have numerous commercial applications, such as use in consumer-electronics items. The lawyers also point out that the equipment can be purchased on the open market in countries such as France.

"The indictment does not allege -- and the government cannot plausibly argue" that the infrared products "were 'specifically designed, modified, or configured for military use,' " according to one of the motions by the lawyers, quoting from the indictment.

An attorney for Mr. Shih, K.C. Maxwell, said her client would plead not guilty in the October trial. An attorney for Mr. Cheng, Matt Pavone, declined to comment.

The FBI has had a difficult time making similar charges stick against other alleged Chinese spies. In May, Qing Chang Jiang, a Chinese national in the import-export business, was acquitted in a California court on charges of illegally selling microwave amplifiers, which can be used in radar and missile systems, to the Beijing government.

The technology is involved in so many nonmilitary commercial applications that many companies aren't aware they need a license to export it, say attorneys who have worked on these cases. Mr. Jiang's lawyer says that the U.S. company he got the technology from, L-3 Communications Holdings Inc.'s Narda Microwave-West, told him he didn't need a license and so he went ahead with the sale.

A spokeswoman for L-3 Communications declined to comment. But the U.S. Department of Commerce said L-3 Communications was aware an export license was required and that the company worked closely with the government on the case.

Mr. Jiang was convicted on a lesser charge of making false statements to federal investigators and is currently awaiting sentencing in California. His attorney, Tom Nolan, believes the U.S. government is systematically targeting Asian businessmen. "They're trying to prevent Chinese industry from doing business in the U.S.," he says.

Asian-American community leaders note that the number of Asian-Americans applying for government research jobs plummeted after the Wen Ho Lee case, and warn of a similar mutually destructive chill now. "At a time when the U.S. government is so dependent on the scientific skills of our community, it seems crazy that they've taken steps that dampen our desire to serve," says Cecilia Chang, a Fremont, Calif.-based Asian-American activist who led many protests and donation drives for Mr. Lee.

And that could have a big impact on American academia and commerce. About 150,000 Chinese students are currently studying in the U.S., according to the FBI, and the number of new admissions has been rising. Nearly 64,000 Chinese students entered the U.S. last year, according to U.S. Immigration and Customs Enforcement, up from 55,000 in 1998. All told, about 700,000 Chinese tourists and business executives visit the U.S. each year.

The swirl of suspicions and tensions between the FBI, China and the Chinese-American community has surfaced even among the bureau's own agents. Mr. Szady has made a point of hiring more Asian-Americans into his counterespionage network. Yet in the past two years, the FBI brought charges against two of its own Chinese-American employees in Los Angeles, accusing them of having aided Beijing. One case was thrown out this year and the other is pending.

Mr. Szady acknowledges the inherent complexity of monitoring the Chinese community in the U.S., and says he's trying to find a balance: "How do you protect without being overbearing?" But he argues that it's the Chinese government, not the FBI, that is blurring the lines between legitimate transborder commerce and national rivalry. He says that Beijing doesn't recognize the concept of Chinese-American. In the government's eyes, "they are all overseas Chinese," says Mr. Szady, a lanky former chemistry student dubbed the "Z Man" by his agents.

Warming Relations

Mr. Szady and other FBI experts believe China began intensifying its spying operations in the late 1970s, when warming relations between Washington and Beijing opened the way for hundreds of thousands of Chinese to begin visiting the U.S. annually. These analysts say units of the People's Liberation Army and China's Ministry of State Security oversee intelligence operations, and that the state-run Institute of Applied Physics and Computational Mathematics has targeted U.S. weapons labs.

In addition, the Beijing government runs an extensive, informal, decentralized spy network, counterespionage experts allege. In most cases, Beijing's spy agencies don't send trained agents to the U.S. to penetrate companies and government agencies, but rather simply seek to glean information from the hundreds of thousands of Chinese who visit and study in the U.S. every year. They also try to get Chinese-Americans to provide information, appealing to their desire to help uplift China's economy.

"In almost all of its collections operations, China is not so much looking at opportunities for stealing things...as devising all sorts of opportunities for you to come to the conclusion that you would be willing to give at least some of these things," says Paul Moore, who was the FBI's top China analyst from 1978 through 1998. "It's the mundane, day-to-day contacts that are killing us, not the exotic spy operations."