

# The Washington Post

## Chinese Spy 'Slept' In U.S. for 2 Decades

Espionage Network Said to Be Growing

By Joby Warrick and Carrie Johnson  
Washington Post Staff Writers  
Thursday, April 3, 2008

Prosecutors called Chi Mak the "perfect sleeper agent," though he hardly looked the part. For two decades, the bespectacled Chinese-born engineer lived quietly with his wife in a Los Angeles suburb, buying a house and holding a steady job with a U.S. defense contractor, which rewarded him with promotions and a security clearance. Colleagues remembered him as a hard worker who often took paperwork home at night.

Eventually, Mak's job gave him access to sensitive plans for Navy ships, submarines and weapons. These he secretly copied and sent via courier to China -- fulfilling a mission that U.S. officials say he had been planning since the 1970s.

Mak was sentenced last week to 24 1/2 years in prison by a federal judge who described the lengthy term as a warning to China not to "send agents here to steal America's military secrets." But it may already be too late: According to U.S. intelligence and Justice Department officials, the Mak case represents only a small facet of an intelligence-gathering operation that has long been in place and is growing in size and sophistication.

The Chinese government, in an enterprise that one senior official likened to an "intellectual vacuum cleaner," has deployed a diverse network of professional spies, students, scientists and others to systematically collect U.S. know-how, the officials said. Some are trained in modern electronic techniques for snooping on wireless computer transactions. Others, such as Mak, are technical experts who have been in place for years and have blended into their communities.

"Chi Mak acknowledged that he had been placed in the United States more than 20 years earlier, in order to burrow into the defense-industrial establishment to steal secrets," Joel Brenner, the head of counterintelligence for the Office of the Director of National Intelligence, said in an interview. "It speaks of deep patience," he said, and is part of a pattern.

Other recent prosecutions illustrate the scale of the problem. Mak, whose sentence capped an 18-month criminal probe, was the second U.S. citizen in the past two weeks to stand before a federal judge after being found guilty on espionage-related charges.

On Monday, former Defense Department analyst Gregg W. Bergersen pleaded guilty in Alexandria to charges that he gave classified information on U.S. weapons sales to a businessman who shared the data with a Chinese official.

In March, the Reston company WaveLab pleaded guilty to violating export laws when it shipped militarily sensitive power amplifiers to China, according to court papers. A lawyer for the company

said it neglected to get proper licenses and did not engage in "underhanded" behavior.

Dongfan Chung, a Boeing engineer arrested in February for allegedly passing classified space shuttle and rocket documents to Chinese officials, was accused in court documents of responding to orders from Beijing as long ago as 1979 -- making him a second alleged longtime agent.

Yesterday, federal prosecutors in Chicago indicted a software engineer for allegedly stealing business trade secrets and trying to take more than 1,000 paper and electronic documents from a telecommunications company on a one-way trip to China last year.

The cases are among at least a dozen investigations of Chinese espionage that have yielded criminal charges or guilty pleas in the past year. Since 2000, Immigration and Customs Enforcement officials have launched more than 540 investigations of illegal technology exports to China.

The FBI recently heightened its counterintelligence operations against Chinese activities in the United States after Director Robert S. Mueller III cited "substantial concern" about aggressive attempts to use students, scientists and "front companies" to acquire military secrets.

Recent prosecutions indicate that Chinese agents have infiltrated sensitive military programs pertaining to nuclear missiles, submarine propulsion technology, night-vision capabilities and fighter pilot training -- all of which could help China modernize its programs while developing countermeasures against advanced weapons systems used by the United States and its allies.

"The intelligence services of the People's Republic of China pose a significant threat both to the national security and to the compromise of U.S. critical national assets," said William Carter, an FBI spokesman. "The PRC will remain a significant threat for a long time as they attempt to develop their military capabilities and to develop their economy in order to compete in today's world economy."

While military technology appears to be the top prize, the Chinese effort is also aimed at commercial and industrial technologies, which often are poorly protected, several officials said. "Espionage used to be a problem for the FBI, CIA and military, but now it's a problem for corporations," Brenner said. "It's no longer a cloak-and-dagger thing. It's about computer architecture and the soundness of electronic systems."

Calls placed to the Chinese Embassy in Washington requesting comment on recent spy cases were not returned. But Chinese officials have repeatedly denied that their country is stealing military technology. "We have reiterated many times that allegations that China stole U.S. military secrets are groundless and made out of ulterior motives," Chinese Foreign Ministry spokesman Qin Gang said at a recent news conference in Beijing, commenting on the Mak case.

But U.S. intelligence and defense officials say China has been able to use technology of U.S. origin in a new generation of advanced naval destroyers and quiet-running, stealthy submarines.

Some of those secrets may have been obtained with the help of Mak, a 67-year-old electrical engineer who became a naturalized U.S. citizen in 1985 along with his wife, Rebecca Chiu Mak. The two settled in Southern California, where Mak eventually accepted a job with Power Paragon, a defense contractor that specialized in advanced naval propulsion technology. In 1996, Mak was given a

security clearance at the "secret" level, which gave him access to sensitive engineering details for U.S. ships and submarines.

In 2003, Mak became the subject of an intensive federal investigation that included court-ordered wiretaps, secret property searches and the clandestine installation of a video camera inside his home. Through surveillance, FBI agents discovered that Mak was in the process of copying thousands of pages of technical documents onto computer disks, which he arranged to send to China using his brother and sister-in-law as couriers.

According to court documents, the Moks encrypted the disks to avoid detection and used coded words to arrange a drop-off of the disks to a Chinese intelligence operative. In one phone conversation, the brother, Tai Wang Mak, intimated that he would be traveling with his wife and a third companion he described as his "assistant" -- a reference, prosecutors said, to the disks, hidden in his luggage.

The plan was foiled on Oct. 28, 2005, when agents arrested Tai Wang Mak as he was preparing to board a plane at Los Angeles International Airport. Chi Mak and his wife were arrested at their home the same day.

A key piece of evidence was a to-do list of apparent intelligence targets, written in Chinese script. The note, which had been shredded, was retrieved from Chi Mak's garbage and painstakingly reassembled to reveal what prosecutors said were instructions from Beijing on the kinds of technology Mak should seek to acquire.

Mak, who testified in his defense at his six-week trial, denied he was a spy and said the information he copied was available from nonclassified sources on the Internet. Defense witnesses said that much, if not all, of the documents acquired by Mak were not officially classified, though transmitting them to China was prohibited under U.S. export laws. Mak's attorney, Ronald O. Kaye, said his client was a scapegoat for other U.S. intelligence failures and a "symbol of the government's cold war against the Chinese."

In another recent case, former Northrop Grumman scientist Noshir Gowadia, who helped build the B-2 bomber, was indicted last fall for allegedly sharing cruise missile data with the Chinese government during a half-dozen trips to China. He is scheduled to go on trial in October.

A defense lawyer for Gowadia did not return calls, but Gowadia's family in Hawaii has told local journalists that the charges stem from a misunderstanding.

Robert Clifton Burns, a Washington lawyer who specializes in export cases, said the Chinese acquisition of sophisticated U.S. technology "is fast coming out from under the radar" as authorities crack down on such shipments to foreign powers. But Burns, who closely tracks prosecutions in the area, said the government sometimes overstates the risks of exporting U.S. items.

"People who violate export laws should be thrown in jail, no question about it," Burns said. But he added that there are also people "who would be better addressed by . . . a civil result where they get a small fine."

*Staff researcher Julie Tate contributed to this report.*

[View all comments](#) that have been posted about this article.

© 2008 The Washington Post Company