

**The New York Times** Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers [here](#) or use the "Reprints" tool that appears next to any article. Visit [www.nytreprints.com](http://www.nytreprints.com) for samples and additional information. [Order a reprint of this article now.](#)

October 17, 2010

# U.S. Companies Are at Risk of Spying by Their Own Workers

By **CHRISTOPHER DREW**

Huang Kexue, federal authorities say, is a new kind of spy.

For five years, Mr. Huang was a scientist at a [Dow Chemical](#) lab in Indiana, studying ways to improve insecticides. But before he was fired in 2008, Mr. Huang began sharing Dow's secrets with Chinese researchers, authorities say, then obtained grants from a state-run foundation in [China](#) with the goal of starting a rival business there.

Now, Mr. Huang, who was born in China and is a legal United States resident, faces a rare criminal charge — that he engaged in economic espionage on China's behalf.

Law enforcement officials say the kind of spying Mr. Huang is accused of represents a new front in the battle for a global economic edge. As China and other countries broaden their efforts to obtain Western technology, American industries beyond the traditional military and high-tech targets risk having valuable secrets exposed by their own employees, court records show.

Rather than relying on dead drops and secret directions from government handlers, the new trade in business secrets seems much more opportunistic, federal prosecutors say, and occurs in loose, underground markets throughout the world.

Prosecutors say it is difficult to prove links to a foreign government, but intelligence officials say China, Russia and Iran are among the countries pushing hardest to obtain the latest technologies.

"In the new global economy, our businesses are increasingly targets for theft," said Lanny A. Breuer, the assistant attorney general in charge of the Justice Department's criminal division. "In order to stay a leader in innovation, we've got to protect these trade secrets."

Mr. Huang, 45, who says he is not guilty, is being prosecuted under an economic espionage provision in use for only the seventh time. Created by Congress in 1996 to address a shift toward industrial spying after the cold war, the law makes it a crime to steal business trade secrets, like software code and

laboratory breakthroughs. The crime rises to espionage if the thefts are carried out to help a foreign government.

Economic espionage charges are also pending against Jin Hanjuan, a software engineer for [Motorola](#), who was arrested with a laptop full of company documents while boarding a plane for China, prosecutors said. Over the last year, other charges involving the theft of trade secrets — a charge less serious than espionage — have been filed against former engineers from [General Motors](#) and [Ford](#) who had business ties to China. And scientists at the [DuPont Company](#) and Valspar, a Minnesota paint company, recently pleaded guilty to stealing their employer's secrets after taking jobs in China.

In two past espionage cases involving American computer companies, defendants said they saw a chance to make money and acted on their own, knowing that the information would be valuable to Chinese companies or agencies. In several cases, Chinese government agencies or scientific institutes provided money to start businesses or research to develop the ideas; that financing is what gave rise to the espionage charges.

The U.S.-China Economic and Security Review Commission, appointed by Congress to study the national security issues arising from America's economic relationship with China, said in a report last year that even in instances without direct involvement by Chinese officials, China's government "has been a major beneficiary of technology acquired through industrial espionage."

China has denied that its intelligence services go after American industries. China's Foreign Ministry declined to comment on the subject, but spokesmen for the Chinese foundation and the university that worked with Mr. Huang said they were not aware of any espionage.

"If it's true, we will start our own investigation into it," said Chen Yue, a spokesman for the Natural Science Foundation of China, which gave Mr. Huang grants to conduct research there.

American officials and corporate trade groups say they fear economic spying will increase as China's quest for Western know-how spreads from military systems to everyday commercial technologies.

After focusing for decades on low-cost assembly operations, China "feels it really needs to turn the corner and become a technology power in its own right," said James Mulvenon, the director of the Center for Intelligence Research and Analysis in Washington, which tracks Chinese activities for federal agencies and corporate clients.

Mr. Mulvenon said China is trying to woo back thousands of ethnic Chinese scientists who have trained or worked in the United States. "They basically roll out the red carpet for these guys," he said.

As economic crimes become easier to commit — in some cases as simple as downloading data and

pressing “Send” — security analysts say some American companies must share the blame for thefts because they do not adequately monitor employees.

At Motorola, for example, court records show that Ms. Jin, the software engineer, downloaded company documents during two sick leaves and tapped into the company’s computers from China, where, prosecutors say, she met with a company linked to the Chinese military. Ms. Jin, a naturalized United States citizen who was born in China, says she is not guilty, and is awaiting trial in Illinois.

Catching and prosecuting wrongdoers is also made difficult by the refusal of some companies to report breaches.

“When you have public companies with their stock values tied to their assets, the last thing they want the buyer of that stock to think is that their assets are compromised,” said Michael Maloof, the chief technology officer of TriGeo Network Security, a company that provides computer monitoring systems.

The first economic espionage case, filed in 2001 against a Japanese scientist, collapsed when Japan refused to extradite him. The six other cases have involved China, and the Justice Department won the first three.

In one case, two Silicon Valley engineers admitted to stealing secrets about computer chips, then arranging financing from Chinese government agencies to start business. In another case, a retired Boeing engineer was convicted after a search of his home found documents on United States military and space programs, as well as letters from Chinese aviation officials seeking the data.

The Justice Department lost a case involving two California engineers. The government focused on documents showing that the engineers were working with a venture capitalist in China to seek financing for a microchip business from China’s 863 program, which supports development of technologies with military applications.

But the men were arrested before they filed the grant application. The judge in the case concluded in May that the government had needed to prove that the men had “intended to confer a benefit” on China, “not receive a benefit from it.”

In Mr. Huang’s case, according to the indictment, he had received money from the Natural Science Foundation of China, a government organization, to conduct insecticide research.

Mr. Huang grew up in China, and has lived in the United States or Canada since 1995. While working for Dow’s farm chemicals unit, Dow AgroSciences, he also took a job as a visiting professor at a Chinese university and made eight trips to China, court records show.

Besides directing research at the university while at Dow, he later smuggled samples of a bacterial strain from Dow to China in his son's suitcase, the authorities said.

Mr. Huang's lawyer, Michael Donahoe, said at a recent hearing that the case was "hypothetical." But Cynthia Ridgeway, an assistant United States attorney, said that with Dow's Chinese patent due to expire in 2012, Mr. Huang had "the full recipe" needed to try to take its business to China.

Last week, a judge denied Mr. Huang's request for bail. He is awaiting trial in federal custody in Indiana.

*Sarah Chen contributed research.*