Foreign spying against US companies on the rise, FBI says

June 29 2012, By Ken Dilanian, Tribune Washington Bureau

Driven in part by the global financial crisis, foreign intelligence services, corporations and computer hackers have stepped up efforts to steal technology and trade secrets from American companies, the FBI's top spy hunter told Congress on Thursday.

A related threat - illegal sales of U.S. technology - was highlighted when a major military contractor, United Technologies Corp., and two subsidiary units agreed in federal court to pay a $75 million fine for illegally selling embargoed software and components to China that the country used to build a sophisticated attack helicopter called the Z-10.

U.S. officials said Thursday that the fine and other penalties would settle criminal and administrative charges against United Technologies, which is based in Hartford, Conn., and its subsidiaries, Pratt & Whitney Canada and Hamilton Sundstrand. The U.S. prohibits the exporting to China of U.S. military equipment and technology.

Foreign efforts to obtain U.S. technology in violation of U.S. law are not new, but the cost is rising and is a threat to national security, said C. Frank Figliuzzi, who heads the FBI's counterintelligence division. He said U.S. companies have suffered more than $13 billion in losses from economic espionage in the current fiscal year.

"What we're seeing is that foreign nations and their intelligence services are understanding more than ever before that it's cheaper to steal our technology than to use their budget resources in this time of economic

crisis to develop it themselves," Figliuzzi told the intelligence subcommittee of the House homeland security committee.

"The theft of U.S. proprietary technology, including controlled dual-use technology and military-grade equipment, from unwitting U.S. companies is one of the most dangerous threats to national security," said John P. Woods, assistant director of national security investigations at U.S. Immigration and Customs Enforcement.

Computer hackers operating from abroad use increasingly sophisticated attacks to infiltrate corporate networks and siphon out intellectual property secrets. But so-called insiders - employees or contractors who steal documents, or download files onto portable media - are responsible for a growing percentage of cases.

In February, for example, a federal grand jury indicted a San Francisco couple and others suspected of conspiring to steal trade secrets from DuPont for a Chinese state-owned company. Figliuzzi said it was the first U.S. criminal case alleging state-sponsored economic spying.

The group allegedly stole information on the production of titanium dioxide, a white pigment used to color paper, plastics and paint. Delaware-based DuPont holds the largest share of the $12 billion annual market in the compound. It is one of the largest economic espionage cases in FBI history.

With that case and others, the FBI has made 10 arrests for economic espionage this fiscal year. Courts have indicted 21 individuals or companies and convicted nine defendants, Figliuzzi said.

Speaking to reporters after the hearing, Figliuzzi said investigators had become more adept at determining who is behind cyber spying from abroad. But he said there is no consensus on how to pursue those people,

particularly if they are working for a foreign government.

"That's the big question," he said.