The world wants what America has, from cutting-edge computer software to scientific research and sensitive defense technology, and nations and overseas companies are increasingly using espionage to get it.

In fact, the FBI believes more foreign spies than ever are operating in the United States.

Even as it concentrates on preventing terrorism, the FBI is overhauling its counterintelligence efforts to blunt the threat. Agents are less focused on finding spies among diplomats and embassies - hallmarks of the long Cold War with the Soviet Union - and more interested in espionage directed at corporations, research centers and universities.

"Left unchecked, such a situation could greatly undermine U.S. national security and U.S. military and economic advantage," FBI Director Robert Mueller told Congress recently.

For instance, the FBI believes China has more than 3,000 "front" companies in the United States whose real purpose is to direct espionage efforts. Many of the thousands of Chinese visitors, students and business people who come to this country each year also have a government intelligence task to perform, authorities say.

The FBI ranks China as the greatest espionage threat to the United States in the next 10 years to 15 years.

"They figured out that what they want is throughout the United States, not just embassies, not just consulates," David Szady, FBI assistant director for counterintelligence, said in an interview with The Associated Press. "It's a major effort."

China is not alone. Russia remains an espionage power, and the United States also must be vigilant
against adversaries such as Iran and North Korea. Friendly countries such as Taiwan and India also pose a threat.

There are 40,000 foreign diplomatic officials in the United States, some of whom are intelligence officers. Saudi Arabia alone has 900 officials in this country.

Modern espionage can range from finding out where an aerospace company produces gyroscopes for satellites to socializing with a U.S. nuclear research scientist in hopes of gaining scraps of knowledge. In one recent case, adhesive maker Avery Denison estimated a $50 million loss after a spy sold company secrets to a Taiwanese conglomerate.

To meet this challenge, the FBI has transferred 167 agents into counterintelligence and set up an anti-espionage operation for the first time in all 56 field offices. Each is putting together a comprehensive survey of the potential espionage targets in their domain to give the FBI its first broad national picture.

At the same time, the bureau must learn from mistakes like the case of Wen Ho Lee, a former Los Alamos National Laboratory scientist initially charged in 1999 with 59 counts of mishandling nuclear weapons information. Lee eventually pleaded guilty to a single charge and, in an extraordinary move, President Clinton issued an apology and said Lee's long captivity "can't be justified" based on the outcome.

"The FBI did a poor job" in that case, Szady said.

The FBI in early 2001 caught one of its own, Robert Hanssen, but he had been spying for the Soviet Union and Russia for years, resulting in at least three deaths of U.S. informants and an immense intelligence loss.

Partly to blame, FBI officials say, was the drift away from counterintelligence after the Soviet Union collapsed in 1991. The number of agents doing the work was cut by 30 percent - exact numbers are classified - and there was a perception that catching spies was a dead-end for FBI careers.

After the Sept. 11 attacks, it became clear to Mueller that the FBI would have to revamp its counterterrorism and counterintelligence operations to meet threats coming from all corners of the globe.

Mueller made fighting espionage the No. 2 priority behind stopping terrorism, with the same philosophy of tracking and stopping spies rather than waiting to prosecute them. Training was strengthened, the career track resurrected and a cadre of intelligence analysts is being built.

Preventive efforts include FBI meetings with corporate executives, university officials and others to gauge vulnerabilities. It also means undercover work at conferences that draw foreign scientists and development of intelligence "assets" who describe for an FBI agent what the foreign government wants.

The FBI still is examining what went wrong in the case of Katrina Leung, a Chinese-born woman recruited in Los Angeles by FBI Agent James J. Smith to provide information about the Beijing government. Prosecutors say Leung actually was a Chinese spy who used her long-term affair with Smith to get access to sensitive government documents. She has pleaded innocent. Smith also faces charges.

Szady said FBI headquarters will exercise greater oversight of intelligence assets, with far greater attention paid to red flags that might indicate a source has been compromised. In the Leung case, little was done after top FBI officials learned that she had passed classified information to China's intelligence service.
On the Net:

FBI: http://www.fbi.gov/

LOAD-DATE: August 4, 2003