Office of Current Production and Analytic Support
CIA Operations Center

News Bulletin Wall Street Journal pg. A1 June 17 1991

Corporate Targets

As Cold War Fades, Some Nations' Spies Seek Industrial Secrets

They May Intercept Messages, Plant Moles to Get Data Useful to Own Companies

Caterpillar Resorts to Codes

By William M. Carley
Staff Reporter of The Wall Street Journal

In Houston's posh River Oaks section, a guard at an executive's home recently noticed two men grabbing bags of trash and throwing them into a van. As the van roared off, the guard scribbled down the license number, which was traced to the French consulate in Houston. Bernard Guillet, French consul general, now says he and an assistant were only picking up bags of grass cuttings to fill a hole dug for a consulate swimming pool that couldn't be completed because of a zoning dispute.

But going through trash is routine for intelligence operatives. Federal Bureau of Investigation agents suspected that French intelligence was after documents discarded by corporate executives living nearby—documents possibly containing information useful to French companies.

Going through garbage isn't illegal, and the FBI says only that it found no violation of U.S. law. Mr. Guillet calls suspicions of espionage "ridiculous." Nevertheless, the episode illustrates why some U.S. companies increasingly suspect that foreign intelligence agencies, working for nations traditionally friendly as well as those often unfriendly, are seeking to scoop up sensitive, potentially valuable information.

Tempting Target

"The U.S. is ahead in many technologies," making it a tempting target, says Stansfield Turner, director of the Central Intelligence Agency under President Carter. The retired admiral says that while at the CIA, he saw "a number of instances" of foreign intelligence agencies getting data from U.S. companies, "and I think that's increasing as it's rapidly becoming one big international market out there."

U.S. corporations have long battled foreign companies trying to get their trade secrets, of course. International Business Machines Corp., for example, has been a target of Japanese computer makers trying to steal technical data. But compared with companies, government intelligence agencies have far greater resources.

According to current and former U.S. officials, several foreign intelligence services are intercepting overseas communications of U.S. companies, including telexes, facsimile messages and phone calls, either by capturing satellite signals or picking up transmissions passing through government-owned telephone exchanges.

Employees Recruited

Intelligence services also recruit nationals working for U.S. subsidiaries abroad to act, in effect, as spies. Last year, a French magazine reported that French employees of IBM and Texas Instruments Inc. handed over company documents to French intelligence agents, who in turn passed them on to a French computer maker.

And some foreign intelligence agencies do "bag jobs," searching briefcases and luggage that executives leave in hotels. A former FBI agent based in Asia says intelligence agents for China often go through briefcases in Hong Kong hotels, photographing anything that looks interesting.

It's nearly impossible to measure how much data U.S. companies are losing to foreign intelligence services. "They may be getting your most confidential marketing strategies by intercepting satellite transmissions, and there's almost no way you can find out," says Noel Matchett, a Silver Spring, Md., consultant formerly with the National Security Agency. NSA is the defense agency that intercepts foreign and protects U.S. communications.

A Major Change

But many view the problem as serious. Oliver Revell, until recently FBI associate deputy director, says some foreign services "are gearing their whole apparatus to collect our proprietary information." Mr. Revell cites a recent item in the Soviet press, in which a KGB official says the spy agency will begin collecting "economic" information for Soviet enterprises.

At the behest of the Senate Intelligence Committee, the CIA has been studying just how serious the threat is. Meanwhile, the FBI, says Deputy Assistant Director R. Patrick Watson, is reorganizing its counterintelligence division to go after more than Soviet spies stealing military secrets. The new goal, he says, is to cover, "across the board," foreign intelligence agencies that might steal corporate technology that is unclassified but still critical. Later this year, he adds, FBI agents will begin interviewing scientists and engineers at U.S. companies to try to determine how such technology is lost and how to stop it.

Some U.S. companies aren't waiting. Caterpillar Inc. has begun putting nearly all its overseas communications in code. Du Pont Co. has hired James Geer, who as chief of the FBI's counterintelligence division until 1989 was in charge of foiling spies. Boeing Co.'s security department has warned executives traveling abroad to keep a tight grip on sensitive documents, never leaving them in hotels.

The long history of industrial espionage by French intelligence services illustrates what U.S. companies are facing. Over 10 years ago, a sales team for a U.S. high-tech company traveled to Paris to offer Air France a device to upgrade its planes' performance. The innovation was considered so secret that there were only five copies of a document detailing the device, its costs and the sales team's negotiating strategy.

But at a meeting with the U.S. sales team, an Air France official asked questions that indicated he already knew what was in the document. Asked about it, he admitted he had read it.

The executive heading the U.S. sales team was furious. But jottings on the copy eventually returned by the airline official indicated that it was the American executive's own copy that had been reproduced and turned over to Air France.

How? "It was the hotel maid," says the U.S. company's security director. While the U.S. executive was out for an evening in Paris, the maid, working for French intelligence, removed, copied and replaced the document. Then, French intelligence gave the copy to government-owned Air France, the airline official said. Air France didn't respond to repeated requests for comment.

A Bug Is Found

Though caught in the act, the French haven't dropped such tactics. At the headquarters of IBM-France in Paris several years ago, a "bug"—a tiny transmitter—was found in the president's office. At first, IBM security men assumed that a competitor had planted it.

But then doubts developed about the Frenchman on the IBM security staff who had discovered the bug. "How often do you walk into the president's office and within 15 minutes find a bug? Hardly ever," says an American familiar with the case.

The Frenchman on the security staff also turned out to have close connections with the government. "He could get government permits in hours where it normally took the company days," the American says. The Americans eventually concluded that the Frenchman had been either planted on the security staff or recruited there by French intelligence and that he had "discovered" the bug to establish his credibility within IBM.

Although an IBM spokesman declines to comment, the American familiar with the case says the French security official is no longer with the company. But the official quickly got another top security job—at a French aerospace company linked to the French government.

Whether or not IBM was right in this case, French intelligence undoubtedly is still collecting information by recruiting French citizens working for American companies. "Our [French] employees, especially those who have served in the French military, tell us that they are visited regularly by French intelligence agents," says the security director of an American company. The agents' "pitch is patriotism, and their questions are, 'What are your business plans, what are your research projects?' "

Divided Loyalties

This technique raises touchy issues. If a foreign employee is approached by his own government, another security director of a U.S. company says, "you have a man on the horns of a dilemma. What is this man going to do?"

Just one recruit can do a lot of damage, as last year's disclosure involving Texas Instruments and IBM illustrates. At TI's facility near Nice, headquarters for its semiconductor and computer operations in Europe, one company official was giving French intelligence unusually sensitive technical information. It was passed on to the French government-owned computer firm Cie. des Machines Bull, said L'Express, the French magazine. Two U.S. government officials confirm this.

TI declines to comment. Bull says its management doesn't know of any data passed to it. It also has repeatedly denied any involvement in espionage against IBM and says such activity would contravene company policy. The French Embassy in Washington says neither intelligence nor political officials will comment.

Similar information was siphoned out of IBM and passed to Bull, a U.S. government official says. According to L'Express, FBI agents confronted French employees of the two companies during the employees' visits to the U.S. When some denied feeding information to French intelligence, the FBI specified the information transmitted and locations where the employees would rendezvous with intelligence agents. Faced with specifics, employees admitted their actions. They were fired. As in the TI case, the French Embassy won't comment.

As spying has begun shifting to economic subjects, the targeted companies have changed, too. Instead of a McDonnell Douglas Corp. assembling a hot new fighter plane, the targets now are more likely to be in basic research and development, the FBI's Mr. Revell says. Among probable targets are companies such as Corning Inc. and its fiber-optic technology; Du Pont and its polymers, coatings and lightweight but high-strength materials; or IBM's electronics research. "We can't just lock up defense plants; the problem of protecting critical technology is much broader than that," Mr. Revell says.

Other Likely Targets

In addition to high-tech companies, other likely targets are companies such as Bechtel Group Inc. that bid on big overseas engineering projects. If a foreign intelligence service intercepted a phone call or fax containing the U.S. company's bid information in advance of the final bidding date, a competitor could use the data to underbid the U.S. company. Or the bidding strategy could be passed to a customer, perhaps allowing it to wangle a lower price from the U.S. company. Bechtel, says one U.S. security consultant, is "extremely concerned"; a Bechtel spokesman says only that "it's a genuine issue."

Often companies aren't sure they're targets. Though lacking hard evidence, Caterpillar officials became convinced their messages were being intercepted after examining the pattern of overseas bidding, an industry official says. "It's amazing how close the competitors' bids were," he says. A Caterpillar spokesman declines to comment on this but says the company has been using code since switching to satellite communications vulnerable to interception in late 1988.

U.S. companies are trying various defense tactics. When executives of one U.S. concern travel to certain countries, they now seek anonymity, the security director says. They fly on commercial carriers rather than the corporate jet and make plane and hotel reservations at the last minute so foreign agents can't easily arrange to put them under surveillance.

At American Telephone & Telegraph Co., a manager about to make an initial business trip abroad is put through a half-day seminar by the security department. Among tips: Don't use a laptop computer on the plane if a seatmate might read sensitive material.

Some companies also are increasing use of secure phones, which scramble conversations. In late 1989, TRW Inc.'s electronic-products subsidiary began producing a device that encodes fax messages. It has sold several thousand, including nearly 60 to one U.S. multinational, says Paul Graham, an official at the TRW unit.

Increasing security of information, however, isn't always easy. Many scientists and engineers believe in the free flow of ideas to further scientific progress. Security directors say top managers, asked for bigger security staffs or expensive encoding devices, often don't want to spend the money, and worry that foreign governments with sophisticated intelligence services can crack corporate codes anyway.

And other considerations can intervene. The security director of one U.S. electronics company says he recently suggested that a new device be developed in Europe rather than Japan, for fear the invention might be stolen by Japanese intelligence agents or competitors. But his U.S. bosses rejected the idea because they think the best research in that area of electronics is being done in Japan and because developing the product there would help penetrate the big Japanese market.

Once a company feels threatened, however, nothing is too trivial to protect. General Electric Co.'s jet-engine division, based in Cincinnati, is installing fax-encoding devices in its offices around the world; units are already operating in Israel, Japan, Britain and Turkey. When queried for this newspaper article, GE's Cincinnati officials fired off messages about the article to company executives abroad. Even these messages were sent in code.

Should U.S. Agencies Spy On Foreign Corporations?

By a WALL STREET JOURNAL *Staff Reporter*

Since some foreign governments spy on U.S. corporations, why shouldn't U.S. agencies spy on foreign companies?

Some in the U.S. intelligence community advocate that. They want to level the playing field in world markets.

An executive at one big U.S. company says he was recently approached by a Central Intelligence Agency official seeking support for the idea. In return, the CIA man suggested, the company might be fed data gleaned from foreign companies. The executive says his company rejected the idea. A CIA spokesman says, "We're not in the business of industrial espionage, and we're not out soliciting support for that."

The idea, in any case, is controversial. "It's the dumbest idea I ever heard of," says retired Lt. Gen. William Odom, former director of the National Security Agency, which eavesdrops for the Defense Department. Gen. Odom, now with a Washington think tank, says that even if U.S. spy agencies got data from foreign firms, which U.S. company would be given the data? Moreover, U.S. spying would anger friendly nations.