Economic Spying by Foes, Friends Gains Momentum

Clandestine quest for proprietary secrets, technologies offers edge.

By Robert H. Williams

Foreign spying against U.S. corporations currently is widespread, involving an estimated 20 nations, including longtime allies in Europe, Asia and the Middle East. This ballooning trend in economic espionage is expected to expand even further in the years ahead as trade and market competitiveness issues increasingly supplant military concerns.

Billions of dollars already have been lost to business adversaries in Israel, Japan, France, the United Kingdom, the Commonwealth of Independent States and a host of other countries that increasingly are relying on technologically sophisticated operations to wrest critical trade and scientific secrets from U.S. firms, government and universities. This is according to officials at a hearing before the House subcommittee on economic and commercial law.

This industrial spying goes far beyond military technology and systems. It embraces numerous commercial products ranging from computers and software to practically any item possessing inherent value.

"Clearly, the risks to sensitive business information are dramatically increasing as foreign governments shift their enormous espionage resources away from military and political targets to world commerce. Intelligence agencies from the former Soviet bloc nations and our allies in Europe and the Far East are actively targeting U.S. corporations. The information they seek is not simply technological data but also financial and commercial information that will give overseas competitors a leg up in the world marketplace," said Rep. Jack Brooks (D-TX), chairman of both the subcommittee and the parent House Judiciary Committee.

Encryption Technology

During recent hearings before the panel, Brooks suggested that application of encryption technology could thwart foreign intelligence services eavesdropping on telecommunications networks. He added that law enforcement agencies are worried that these electronic safeguards probably will be appropriated by terrorists, drug lords and other criminals.

Milton J. Socolar, special assistant to the U.S. comptroller general, General Accounting Office, disclosed that foreign nations are using advanced and undetectable systems to steal proprietary information and technologies. He cited a number of nations, including France, whose Direction Generale de la Securite Exterieure (DGSE) regularly seeks to clandestinely gain trade information in the United States and elsewhere.

Socolar said DGSE compiled a secret dossier on proposals from U.S. and former Soviet Union aerospace firms involved in a fighter aircraft deal with India. This information was provided to France's Avions Marcel Dassault-Breguet Aviation, which produces the Mirage jet. The upshot is that the French firm won the contract.

Other specific examples provided by Socolar tag the Israelis for turning over a top-secret airborne reconnaissance camera system from the U.S. company Recon Optical, Incorporated, to Electro-Optics, an Israeli defense contractor. Recon sued Israel, and the case was settled in 1991.

Meanwhile, he said, France's DGSE "acquired proprietary information for IBM's next-generation personal computer." This intelligence apparently was referred to Campagnies des Machines Bull, a business adversary of IBM. Another example related to a French national, employed by Corning, Incorporated, who sold fiber optic technology secrets to DGSE, which, in turn, offered the technology secrets to a competitor in France.

Computer Pirating

Socolar is not prepared to charge the Japanese government with economic espionage, but he noted the "government-to-industry relationship" there and recalled instances of illegal activities regarding proprietary information from U.S. companies. He specifically cited Hitachi employees who offered guilty pleas to transporting stolen IBM property. At stake were design documents for the U.S. firm's most powerful computers.

Robert M. Gates, director of Central Intelligence, who asserted that the United States will not be party to economic spying, declined in an open hearing to identify specific countries. "I can note, however, that some governments in Asia, Europe, the Middle East and, to a lesser degree, Latin America, as well as some former communist countries— nearly 20 governments overall—are involved in intelligence collection activities that are detrimental to our economic interests at some level," Gates mentioned to the subcommittee.

He explained that the end of the Cold War appears to have altered dramatically the thrust of the foreign intelligence threat, shifting its preoccupation from military questions to economic and technology objectives. Some governments, Gates pointed out, are bent on gaining access to "U.S. government policy deliberations concerning foreign trade, investments and loans and positions on bilateral economic negotiations." Company bids on contracts; data on commodity prices; and other financial trends, such as banking and stock market information and interest rates, also are of keen interest to nations seeking to extend their own economic agendas.

Sub Rosa Activity

Gates said that a number of foreign intelligence services aggressively are attempting to influence both government and business decisions that have economic importance for them. This sub rosa activity embraces recruiting agents to influence events at all levels. "Several other governments engage in aggressive lobbying on behalf of their national firms—to the point of exerting political and economic leverage in a heavy-handed manner," he asserted.

William S. Sessions, director of the Federal Bureau of Investigation (FBI), also noted the expanding scope of foreign intelligence operations against the United States, saying that the "collection strategies of adversaries and allies alike will not only focus on defense-related information, but also include scientific, technological, political and economic information." Sessions added that this information is vital for those countries attempting to construct market economies that are able to compete internationally.

The Commonwealth of Independent States, for example,

is expected to escalate economic espionage efforts to advance its economy. "Defectors have stated that the new Russian intelligence service will target the increasing number of U.S./Russian joint business ventures in an effort to steal highly desirable Western technology," the director said, noting that, when a nation does not have the money to pay for technology, theft is accepted as a viable alternative.

He cautioned the subcommittee that critical technologies "require a concentrated effort of protection from foreign powers to preserve the economic vitality of this country and ensure the continued competitiveness of the United States in the international marketplace."

Sessions said that, for the FBI, a major problem in this technology arena is finding a way to protect valuable unclassified information from foreign intelligence services. Corporate leaders and their counterparts in the U.S. intelligence community currently are attempting to define the parameters of this problem. As this project evolves, Sessions said, the FBI is dealing with all allegations of attempts by foreign governments to illegally acquire proprietary technology and economic information that impinges on national security.

Problems for the FBI

The FBI, Sessions said, has a problem. Current criminal law gives the agency limited authority to "counter the unfair economic advantage of foreign businesses and industry, which often is fostered by foreign governments and their intelligence services." He explained, however, that the antitrust laws, antidumping rules, tariff and trade reciprocal actions and economic enforcement provisions are designed to level the international trade competition.

Several representatives of companies that are victims of foreign economic espionage also appeared before the subcommittee. Marshall C. Phelps, Jr., vice president of commercial and industrial relations at IBM, said his company has lost billions of dollars to foreign companies that illegally gained technology and product information from the electronics giant. He added that the company's basic input/output system that governs the interaction between the computer and disk drives and the keyboard has been "deliberately and repetitively misappropriated" by numerous foreign and domestic companies that are manufacturing cheap knockoffs or clones of the IBM personal computer.

The company's main frame computer systems and supporting software, likewise, have been targets. Phelps said foreign laws provide no remedy, particularly with respect to software.

James E. Riesbeck, executive vice president of Corning, Incorporated, said his company has been successful in protecting its technology secrets from domestic competitors, but it has encountered severe problems overseas, particularly in Europe. French government-sponsored industrial espionage has been directed at the company's fiber optic technology, he added.

Corporate Need for Help

"It is very difficult," Riesbeck said, "for an individual corporation to counteract this activity. The resources of a corporation—even a large one such as Corning—are no match for industrial espionage activities that are sanctioned and supported by foreign governments."

The company is allocating increased funding for security, but he told the panel that the espionage problem will worsen. He said that corrective steps must be taken to safeguard corporate communications dispatched to foreign locations over public switched networks. Encryption devices, he said, must be established in global communications systems.

He also recommended that U.S. intelligence agencies become aggressive participants in a "public-private partnership." In the future, Riesbeck said, the U.S. intelligence community must play a pivotal part "in charting our national economic destiny, in monitoring significant international technological developments and in conducting counterintelligence to help protect our economy from those who do not play by the rules." A counter industrial espionage response by the United States, he added, is not desirable.

Brooks suggested a go-slow approach on spreading encryption technology. He also insisted that there must be a full-dress review by Congress before a decision is made to expand the charters of the Central Intelligence Agency and National Security Agency to eliminate the foreign economic espionage threat.

. . . — . —

Government, Commercial Systems Vulnerable to Espionage Schemes

The means to protect voice, data, facsimile and other information media for government and business users already exists, said Dr. James J. Hearn, deputy director for information systems security at the National Security Agency. A primary device is a digital, secure telephone that originally was developed for the Defense Department.

In his appearance before the House subcommittee on economic and commercial law, Hearn declared that information in both government and private sector communications and computer systems is prey for foreign intelligence agencies.

"It is certainly possible for an adversary to gain access to the information in many of our systems. Moreover, our foreign adversaries are taking advantage of our vulnerabilities. This foreign threat, combined with domestic vulnerabilities, leads to grave concern," Hearn said.

He pointed to the secure telephone unit (STU)-III as a partial remedy to illegal intercepts in the United States and abroad. Versions of the STU-III currently are securing communications among U.S. embassies and the overseas sites of U.S. companies.

"Properly used, these devices can secure voice, data and fax transmissions, but they must be used, and, when in use, can only protect information from place to place. This may be when the information is most vulnerable, but the STU-III cannot ensure that information is not available to the adversary at some other time in its life," he cautioned.

The penetration of unclassified computer systems that were scrutinized by the National Security Agency and other government entities resulted largely from inadequate security processes, he said. This unlawful infiltration, he mentioned, was largely the result of foes snatching "low hanging fruit," rather than inadequate technology protections.

Awareness is the key, he added. Hearn referred to the recent Michelangelo computer virus scare. Computer experts had predicted that between 15 and 18 percent of the personal computers in the United States would be affected, but the fear of losing valuable information prompted most users to take remedial steps.