United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Economic and Commercial Law,
Committee on the Judiciary
House of Representatives

For Release
on Delivery
Expected at
10:00 a.m. EDT
Wednesday
April 29, 1992

ECONOMIC ESPIONAGE

The Threat to U.S. Industry

Statement of Milton J. Socolar
Special Assistant to the Comptroller General

GAO/T-OSI-92-6

GAO Form 160 (12/91)
OPR:OIMC/PCC

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today at your request to talk about our ongoing examination of issues involving foreign economic espionage.

The theft of U.S. proprietary information or technology by foreign companies has long been a part of the competitive business environment. However, as the world political climate changes with the end of the Cold War, the surreptitious gathering of economic and technological information has taken on added significance. The unauthorized acquisition of U.S. proprietary or other information by foreign governments to advance their countries' economic position is growing--referred to as economic espionage. The loss of proprietary information and technology through espionage activity will have broadening detrimental consequences to both U.S. economic viability and our national security interests.

The United States, a leader in creative technological research and development, is a prime target for economic espionage. In recent months, government officials have begun to speak out about this problem. In a recent speech, Central Intelligence Agency (CIA) Director Robert Gates focused on the changing activities of foreign intelligence efforts when he reported, "[S]ome foreign intelligence services have turned from politics to economics and the United States is their prime target." President Bush also expressed concern about such activities when he stated in a speech,

"We must . . . thwart anyone who tries to steal our technology or otherwise refuses to play by fair economic rules."

Sophisticated and often undetectable methods are used in economic espionage. Unfortunately, U.S. companies targeted by foreign intelligence agencies may not know--and may never know--that they have been targeted or compromised. In addition, many companies that know they have been victimized want to avoid the negative publicity associated with the loss of valuable trade secrets and other proprietary information. Industry representatives are thus reticent to publicize incidents of espionage.

While it is not possible for me to quantify the scope of economic espionage conducted by foreign intelligence agencies, there is evidence of a real and growing problem. It has been known for many years that the KGB has been misappropriating U.S. corporate secrets. Indeed, the FBI has estimated that the efforts of the KGB and its surrogates saved the Soviet Union billions of dollars and years of research and development efforts in gaining Western technologies and expertise.

A former director of the French secret service, DGSE (Direction Generale de la Securite Exterieure), publicly admitted that he directed French industrial and technological intelligence forces to gather economic information from the United States and

other countries. In one instance, he stated that the DGSE compiled a detailed secret dossier of the proprietary proposals from U.S. and Soviet companies who were competing with a French company for a billion dollar contract to supply fighter jets for India. Negotiators for the French company, which builds the Mirage jet, were stated to have then used the information provided by DGSE to obtain the contract.

The following instances of economic espionage that we found in open source documents further illustrate the nature of the problem:

-- Recon Optical, Inc., a U.S. company, contracted with the Israeli government to design a top-secret airborne spy-camera system. After months of disagreement between Recon and Israel, Israeli agents allegedly gave Recon's plans for the system to Electro-Optics, an Israeli defense contractor. Recon brought suit against Israel, and the case was settled in 1991. Court records of the settlement are still sealed.

-- In two other instances, the French DGSE was allegedly involved in the misappropriation of proprietary information from two U.S. companies. In the first case, the DGSE acquired proprietary information for IBM's next-generation personal computer. The DGSE reportedly provided the information to Campagnies des Machines Bull,

an IBM competitor. In the second case, a French national, working for Corning, Inc. in France, sold information and trade secrets to DGSE regarding Corning's latest fiber optic technology. DGSE, in turn, allegedly provided this information to a French competitor of Corning.

In some instances, U.S. business people have aided foreign competitors in obtaining information. For example, in one case a U.S. scientist sold the trade secrets of U.S. pharmaceutical companies to foreign corporations. The research and development costs associated with the pharmaceutical products alone were estimated at $750 million.

A complicating factor in examining the problem of economic espionage is the difficulty in determining whether a particular theft of information is the result of foreign government or foreign business activity. This occurs when the company perpetrating the theft is in a country whose government-to-industry relationship is substantially different than what prevails in the United States.

The government-to-industry relationship in Japan makes it difficult to determine if the Japanese government is involved when Japanese companies successfully acquire U.S. corporate secrets in an unauthorized manner. For example, in 1982 Hitachi employees pleaded guilty to conspiring to transport stolen IBM property--in

this case, design documents and components for every major part of IBM's newest and most powerful generation of computers, which were not yet on the market. Hitachi, a manufacturer of IBM-compatible products, planned to use this technology to eliminate costly and time-consuming research, thereby shortening the lead time required to bring compatible Hitachi products to the marketplace.

The clandestine operations by the DGSE and other foreign intelligence agencies can be contrasted sharply with the U.S. intelligence community's view that it should not conduct industrial or economic espionage to benefit U.S. companies. As CIA Director Gates recently stated, U.S. intelligence "does not, should not, and will not engage in industrial [or economic] espionage." Mr. Gates' position is consistent with the views of U.S. industry leaders; they have stated that it would be highly undesirable to have the CIA engage in this type of activity due to ethical and practical reasons. For example, what would the intelligence community's dissemination policies be with respect to foreign company secrets?

Cryptographic and other information technologies exist that can protect against the vulnerability of the electronic transmission of sensitive information. Such technology is readily available under internationally accepted industry standards. U.S. industry could use this technology to afford a high degree of protection to its proprietary information. The intelligence community, however, appears to be insisting upon the development of

a different standard for U.S. industry for electronic communications between it and the government. This separate standard is weaker than what is commercially available, is an added burden on commercial activities, and raises the question as to whether any practical purpose would be served by the requirement. The issues involved, although they may lie within the national security area, merit public discussion.

Technological advances in computers have made it easier for foreign intelligence agencies and others to monitor the electronic commerce of U.S. industry. U.S. companies may be less able to protect themselves from the espionage apparatus of a foreign government than from a competitor. This problem is made more acute by the globalization of economic competition and the use of advanced communication technologies to conduct business. We need to examine openly the extent to which the government should be hampering industry's use of generally available cryptographic technology that would better protect electronic business communications.

The CIA and the Federal Bureau of Investigation (FBI) maintain foreign counterintelligence efforts to protect national security. However, the efforts of these agencies do not appear to be sufficiently coordinated to adequately protect U.S. industry against economic espionage. This suggests that there are significant policy issues requiring resolution. In addition, the

National Security Agency (NSA) maintains electronic intelligence capabilities that may include gathering economic information. Under the Computer Security Act of 1987, NSA's role is to provide technical advice to the National Institute of Standards and Technology (NIST). NIST's responsibility, under the act, includes assisting government agencies and private entities in protecting unclassified, but sensitive, computer data from compromise.

Many of the issues in economic espionage, concerning the roles of the FBI and CIA, are similar to those raised during the hearings leading to the enactment of the Computer Security Act of 1987. A wide range of concerns had been raised at that time, regarding President Reagan's decision to give the Department of Defense (DOD) responsibility for computer security involving unclassified, but sensitive, data located in civilian agencies and the private sector.

As you know, Congress responded by holding hearings that resulted in legislation giving the responsibility to the Commerce Department instead of DOD. Pursuant to the act, the Commerce Department is responsible for issuing computer security standards that allow industry to use the best commercially available technology.

In closing, economic espionage is an important problem that this country has to face. The criminal justice and intelligence

agencies have not adequately addressed this problem. Economic espionage must be looked at very carefully. There should be a thorough review of which agencies should be involved in this area together with what their responsibilities should be. No decision should be made without benefit of a full public debate. Currently, most of the discussions are being conducted within the intelligence community, without the benefit of public debate. In the final analysis, Congress may have to develop legislation to protect industry from economic espionage. How these issues are decided may have a dramatic effect on the economic future of this country.

- - - -

This concludes my prepared statement. We would be pleased to answer any questions you may have.