United States General Accounting Office

GAO

Testimony

Before the Select Committee on Intelligence
United States Senate

For Release on Delivery
Expected at
10:30 a.m., EST
Wednesday,
February 28, 1996

ECONOMIC ESPIONAGE

Information on Threat From U.S. Allies

Statement for the Record by David E. Cooper, Associate Director, Defense Acquisitions Issues, National Security and
International Affairs Division

G A O
75 years
1921 - 1996

GAO/T-NSIAD-96-114

Mr. Chairman and Members of the Committee:

I am pleased to be able to provide this statement for the record. We recently completed a report on security arrangements used to protect sensitive information when foreign-owned U.S. companies work on classified Department of Defense contracts.[1] As part of this effort, we examined the threat of foreign espionage facing U.S. defense companies, a concern of today's hearing.

In brief, Mr. Chairman, we reported that, according to the Federal Bureau of Investigation and intelligence agencies, some close U.S. allies actively seek to obtain classified and technical information from the United States through unauthorized means. These agencies have determined that foreign intelligence activities directed at U.S. critical technologies pose a significant threat to national security.

Economic Espionage Efforts of Allies

U.S. intelligence agencies report a continuing economic espionage threat from certain U.S. allies. Our report discussed the espionage activities of five allies.

A goal common to most of these countries was the support of the country's defense industry. Countries seek U.S. defense technologies to incorporate into domestically produced systems. By obtaining the technology from the United States, a country can have cutting-edge weapon systems without the cost of research and development. The cutting-edge technologies not only provide superior weapon systems for a country's own use, but also make these products more marketable for exports.

Country a

According to a U.S. intelligence agency, the government of Country A conducts the most aggressive espionage operation against the United States of any U.S. ally. Classified military information and sensitive military technologies are high-priority targets for the intelligence agencies of this country. Country A seeks this information for three reasons: (1) to help the technological development of its own defense industrial base, (2) to sell or trade the information with other countries for economic reasons, and (3) to sell or trade the information with other countries to develop political alliances and alternative sources of arms. According to a

[1]Defense Industrial Security: Weaknesses in U.S. Security Arrangements With Foreign-Owned Defense Contractors (GAO/NSIAD-96-64, Feb. 20, 1996)

classified 1994 report produced by a U.S. government interagency working group on U.S. critical technology companies,[2] Country A routinely resorts to state-sponsored espionage using covert collection techniques to obtain sensitive U.S. economic information and technology. Agents of Country A collect a variety of classified and proprietary information through observation, elicitation, and theft.

The following are intelligence agency examples of Country A information collection efforts:

- An espionage operation run by the intelligence organization responsible for collecting scientific and technological information for Country A paid a U.S. government employee to obtain U.S. classified military intelligence documents.
- Several citizens of Country A were caught in the United States stealing sensitive technology used in manufacturing artillery gun tubes.
- Agents of Country A allegedly stole design plans for a classified reconnaissance system from a U.S. company and gave them to a defense contractor from Country A.
- A company from Country A is suspected of surreptitiously monitoring a DOD telecommunications system to obtain classified information for Country A intelligence.
- Citizens of Country A were investigated for allegations of passing advanced aerospace design technology to unauthorized scientists and researchers.
- Country A is suspected of targeting U.S. avionics, missile telemetry and testing data, and aircraft communication systems for intelligence operations.
- It has been determined that Country A targeted specialized software that is used to store data in friendly aircraft warning systems.
- Country A has targeted information on advanced materials and coatings for collection. A Country A government agency allegedly obtained information regarding a chemical finish used on missile reentry vehicles from a U.S. person.

Country B

According to intelligence agencies, in the 1960s, the government of Country B began an aggressive and massive espionage effort against the United States. The 1994 interagency report on U.S. critical technology companies pointed out that recent international developments have

[2]Report on U.S. Critical Technology Companies, Report to Congress on Foreign Acquisition of and Espionage Activities Against U.S. Critical Technology Companies (1994).

increased foreign intelligence collection efforts against U.S. economic interests. The lessening of East-West tensions in the late 1980s and early 1990s enabled Country B intelligence services to allocate greater resources to collect sensitive U.S. economic information and technology.

Methods used by Country B are updated versions of classic Cold War recruitment and technical operations. The Country B government organization that conducts these activities does not target U.S. national defense information such as war plans, but rather seeks U.S. technology. The motivation for these activities is the health of Country B's defense industrial base. Country B considers it vital to its national security to be self-sufficient in manufacturing arms. Since domestic consumption will not support its defense industries, Country B must export arms. Country B seeks U.S. defense technologies to incorporate into domestically produced systems. By stealing the technology from the United States, Country B can have cutting-edge weapon systems without the cost of research and development. The cutting-edge technologies not only provide superior weapon systems for Country B's own use, but also make these products more marketable for exports. It is believed that Country B espionage efforts against the U.S. defense industries will continue and may increase. Country B needs the cutting-edge technologies to compete with U.S. systems in the international arms market.

The following are intelligence agency examples of Country B information collection efforts:

- In the late 1980s, Country B's intelligence agency recruited agents at the European offices of three U.S. computer and electronics firms. The agents apparently were stealing unusually sensitive technical information for a struggling Country B company. This Country B company also owns a U.S. company performing classified contracts for DOD.
- Country B companies and government officials have been investigated for suspected efforts to acquire advanced abrasive technology and stealth-related coatings.
- Country B representatives have been investigated for targeting software that performs high-speed, real-time computational analysis that can be used in a missile attack system.
- Information was obtained that Country B targeted a number of U.S. defense companies and their missile and satellite technologies for espionage efforts. Companies of Country B have made efforts, some successful, to acquire targeted companies.

Country C

The motivation for Country C industrial espionage against the United States is much like that of Country B: Country C wants cutting-edge technologies to incorporate into weapon systems it produces. The technology would give Country C armed forces a quality weapon and would increase the weapon's export market potential. The Country C government intelligence organization has assisted Country C industry in obtaining defense technologies, but not as actively as Country B intelligence has for its industry. One example of Country C government assistance occurred in the late 1980s, when a Country C firm wanted to enter Strategic Defense Initiative work. At that time, the Country C intelligence organization assisted this firm in obtaining applicable technology.

Country D

The Country D government has no official foreign intelligence service. Private Country D companies are the intelligence gatherers. They have more of a presence throughout the world than the Country D government. However, according to the 1994 interagency report, the Country D government obtains much of the economic intelligence that Country D private-sector firms operating abroad collect for their own purposes. This occasionally includes classified foreign government documents and corporate proprietary data. Country D employees have been quite successful in developing and exploiting Americans who have access to classified and proprietary information.

The following are examples of information collection efforts of Country D:

- Firms from Country D have been investigated for targeting advanced propulsion technologies, from slush-hydrogen fuel to torpedo target motors, and attempting to export these items through intermediaries and specialty shipping companies in violation of export restrictions.
- Individuals from Country D have been investigated for allegedly passing advanced aerospace design technology to unauthorized scientists and researchers.
- Electronics firms from Country D directed information-gathering efforts at competing U.S. firms in order to increase the market share of Country D in the semiconductor field.

Country E

Intelligence community officials stated that they did not have indications that the intelligence service of Country E has targeted the United States or its defense industry for espionage efforts. However, according to the 1994

interagency report, in 1991 the intelligence service of this country was considering moving toward what it called "semi-overt" collection of foreign economic intelligence. At that time, Country E's intelligence service reportedly planned to increase the number of its senior officers in Washington to improve its semi-overt collection—probably referring to more intense elicitation from government and business contacts.

The main counterintelligence concern cited by one intelligence agency regarding Country E is not that its government may be targeting the United States with espionage efforts, but that any technology that does find its way into Country E will probably be diverted to countries to which the United States would not sell its defense technologies. The defense industry of this country is of particular concern in this regard.

It was reported that information diversions from Country E have serious implications for U.S. national security. Large-scale losses of technology were discovered in the early 1990s. Primary responsibility for industrial security resides in a small staff of the government of Country E. It was reported that this limited staff often loses when its regulatory concerns clash with business interests. The intelligence agency concluded that the additional time needed to eradicate the diversion systems will consequently limit the degree of technological security available for several years. The question suggested by this situation is, if technology from a U.S. defense contractor owned by interests of Country E is transferred to Country E, will this U.S. defense technology then be diverted to countries to which the United States would not sell?

Our report also discusses how the Department of Defense seeks to protect sensitive information and technologies at foreign-owned U.S. companies against such threats. It makes recommendations aimed at improving information security at firms operating under these security arrangements.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested