Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2001

This report was prepared by the Office of the National Counterintelligence Executive.

Reverse Blank

October 2001

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2001

Scope Note

This annual report reviews the threat from foreign economic collection and industrial espionage and is conducted in compliance with a Congressional mandate. Reporting throughout calendar year 2000 showed continued efforts by foreign governments, corporations, and individuals to acquire US proprietary economic information.

The Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359 requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the sixth *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, disseminated in September 2000 and covers intelligence reporting and other information from calendar year 2000.

The Authorization Act specifies that the annual report is to examine three aspects of the threat to US industry: the number and identity of the foreign governments believed to be conducting industrial espionage, the industrial sectors and types of information and technology targeted by such espionage, and the methods used to conduct espionage. To prepare this assessment, the Office of the National Counterintelligence Executive (NCIX) requested the assistance of the Intelligence Community (IC). The following government agencies provided individual assessments for this report:

- Air Force Office of Special Investigations (AFOSI).
- Central Intelligence Agency (CIA).
- Defense Intelligence Agency (DIA).
- Defense Security Service (DSS).
- Department of Energy (DOE).
- Department of State, including the Bureau of Intelligence and Research and the Bureau of Diplomatic Security.
- Federal Bureau of Investigation (FBI).
- Army Counterintelligence Center (ACIC).

- Naval Criminal Investigative Service (NCIS).
- National Reconnaissance Office (NRO).
- National Security Agency (NSA).
- US Customs Service.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2001

Key Findings

As the world's leading industrial power and leader in technology development, the United States continues to be a prime target of foreign economic collection and industrial espionage.

The United States pays a high financial price for economic espionage. The business community estimates that, in calendar year 2000, economic espionage cost from **$100-250 billion** in lost sales. The greatest losses to US companies involve information concerning manufacturing processes and research and development.

Increasing competition for limited global resources will intensify economic collection against the United States, including the theft of trade secrets and competitive business information.

Definitions

Economic Espionage. *There is no consensus within the US Government on the definition of economic espionage. For the purposes of this report, NCIX will use the US Attorney General's definition of economic espionage as "the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies." This definition excludes the collection of public domain and legally available information that constitutes a significant majority of economic collection. Aggressive intelligence collection that is entirely in the public domain and is legal may harm US industry, but it is not espionage. It, however, may help foreign intelligence services identify and fill information gaps that could be a precursor to economic espionage.*[a]

Industrial Espionage. *According to the Justice Department, industrial espionage is defined "as activity conducted by a foreign . . . government or by a foreign company with the direct assistance of a foreign government against a private US company for the sole purpose of acquiring commercial secrets." This definition does not extend to the activity of private entities conducted without foreign government involvement, nor does it pertain to lawful efforts to obtain commercially useful information, such as information available on the Internet. Although some open-collection efforts may be a precursor to clandestine collection, they do not constitute industrial espionage. Some countries have a long history of ties between government and industry; however, it is often difficult to ascertain whether espionage has been committed under foreign government sponsorship, a necessary requirement under the Economic Espionage Act, Title 18 U.S.C., Section 1831.*

Proprietary Information. *Another term used in this report is proprietary information, the definition of which is information not within the public domain and that which the owner has taken some measures to protect. Generally, such information concerns US business and economic resources, activities, research and development, policies, and critical technologies. Although it may be unclassified, the loss of this information could impede the ability of the United States to compete in the world marketplace and could have an adverse effect on the US economy, eventually weakening national security. Commonly referred to as "trade secrets," this information typically is protected under both state and federal laws.*

[a] *For a conviction under the Economic Espionage Act (EEA) of 1996 (title 18 U.S.C. Chapter 90), a person must convert a trade secret to an economic benefit in interstate commerce.*

Contents

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2001

Overview of the Threat to US National Security

The United States continues to be threatened by the theft of proprietary economic information and information on critical technologies. The risks to sensitive business information and advanced technologies continue to increase significantly as foreign governments—both former adversaries and allies—focus their espionage resources in ever-greater numbers on the private sector. They are seeking not only technological data but also financial and commercial information that will provide their companies with a competitive edge in the global economy.

Targeted US Defense Information and Technology

According to US defense industry reporting, targeting conducted by commercial and individual foreign collectors accounted for 60 percent of the total suspicious activities. Government-sponsored targeting—including military and other official government activity—accounted for 21 percent of suspicious activities. Targeting activities by government-affiliated entities—including institutes, laboratories, and universities—accounted for another 19 percent. Foreign companies whose work exclusively or predominantly supports government agencies were assessed as being government affiliated.

Collection Methods

There has been no visible change in foreign collection methods over the past year. Economic and industrial information collectors seldom use one method of collection. They combine collection techniques into a concerted effort that includes legal and illegal methods, and they continue to become more innovative in their tactics. Consistent with traditional espionage operations, significant foreign intelligence collection efforts are often conducted legally and openly. These collection efforts often serve as precursors to economic espionage:

- Open-source collection activities:
  - — Requests for information.
  - — Solicitation and marketing of services.
  - — Acquisition of technology and companies.
  - — Visits by foreign nationals to US facilities.
  - — Conferences.
  - — Internet activity (cyber attack and exploitation).
  - — Exploitation of joint ventures.

Requests for Information

Activities reported in this category include unsolicited requests received from known or unknown sources—usually foreign—for classified, sensitive but unclassified, export-controlled, or company proprietary information. According to the Defense Security Service (DSS), in 2000 these kinds of suspicious activities accounted for 41 percent of total reported collection efforts. Not surprisingly, there has been a dramatic rise in the use of the Internet for these kinds of collection activities. DSS reported that the use of the Internet by foreign entities collecting US technology and technical information accounted for 27 percent of all suspicious contacts.

The Internet provides a simple, low-cost, nonthreatening, risk-free means of worldwide access to US technology. E-mail and Web-chat exchanges are inconspicuous and can bypass traditional security safeguards, directly reaching the targeted individual.

Solicitation and Marketing of Foreign Services
One of the most popular tactics used to gain access to US research and development facilities is to have foreign scientists submit unsolicited employment applications. In 2000, facilities that were the targets of this kind of solicitation were working on such technologies as electro-optics, ballistics, and astrophysics. Other approaches included offers of software support, internships, and proposals to act as sales or purchasing agents. In addition, of growing importance is the greater use of foreign research facilities and software development companies located outside the United States to work on commercial projects related to protected programs. Any time direct control of a process or a product is relinquished, the technology associated with it is susceptible to possible exploitation.

Acquisition of Technology and Companies
Acquisitions were greatly on the rise in 2000. This is the latest manifestation of an increased trend to acquire sensitive technologies through purchase. According to DSS reporting, 88 percent of all reported suspicious acquisition activities involved third parties. Third parties are not the actual entities acquiring the technology but are the ultimate end users. Third-party acquisitions are often an indicator of a possible technology transfer or diversion because when the ultimate recipients are determined, they are often countries that are on embargoed lists for the acquired items. One method that is commonly used involves setting up a freight forwarder, that is, a cooperating US-based company that will provide the ultimate foreign recipient with a US address to subvert US export-control laws.

Exploitation of Visits to US Companies
During the past year, efforts continued by foreigners to exploit their visits to US facilities. Some examples of exploitation techniques include:

- Wandering around facilities unescorted, bringing unauthorized cameras and/or recording devices into cleared facilities, or pressing their hosts for additional accesses or information.

- Adding last minute and/or unannounced persons as part of the visit.

- Arriving unannounced and seeking access by asking to see an employee belonging to the same organization as the visitor.

- Hiding true agendas, for example, by trying to shift conversations to topics not agreed upon in advance.

- Misrepresenting a visitor's importance or technical competency to secure visit approval.

Conferences
International seminar audiences often include leading scientists and technical experts, who pose more of a threat than intelligence officers due to their level of technical understanding and ability to exploit immediately the intelligence they collect. The counterintelligence community reporting indicates that, during seminars, foreign entities attempt subtle approaches such as sitting next to a potential target and initiating casual conversation. This activity often serves as a starting point for later exploitation. Membership lists of international business and/or technical societies are increasingly used to identify potential US targets. One of the most common targeting techniques is to use collectors who have common cultural backgrounds with the target such as origin of birth, religion, or language.

Internet Activity (Cyber Attack and Exploitation)
This category addresses cyber attack and exploitation vice Internet-based requests for information. The majority of Internet endeavors are foreign probes searching for potential weaknesses in systems for exploitation. One example was a network attack that, over the period of a day, involved several hundred attempts to use multiple passwords to illegally obtain access to a cleared defense facility's network. Fortunately, the facility had an appropriate level of protection in place to repel this attack. This example reflects the extent to which intelligence collectors are attempting to use the Internet to gain access to sensitive or proprietary information. Given the considerable effort that is under way in the cyber attack and exploitation arenas, substantial resources will need to be allocated in the future to ensure adequate security countermeasures.

Exploitation of Joint Ventures/Research
Joint ventures place foreign personnel in close proximity to US personnel and technology and can thereby facilitate access to protected programs. This is of special concern when foreign employees are in place for long periods of time. In this scenario, there is always a danger that foreign employees will be more readily accepted as full partners, and the security vigilance of US colleagues may wane.

Some examples of suspicious activity in joint ventures/research include: foreign workers seeking access to areas or information outside the purview of their work agreement, enticing US companies to provide large quantities of technical data as part of the bidding process, and foreign organizations sending more representatives than reasonably necessary for particular projects.

Illegal Collection Activities
Foreigners seeking to acquire US proprietary economic and industrial information often engage in the following types of illegal activities:

- **Acquisition of export-controlled technologies.** The unlawful acquisition of export-controlled technologies by foreign collectors remains a considerable concern. Methods of operation employed to circumvent the export-control process include: using front companies within the United States and overseas, illegally transporting products to an undisclosed end user by utilizing false end-user certificates, and purchasing products that have been modified during the manufacturing process to meet export-controlled specifications.

- **Theft of trade secrets and critical technologies.** US businessmen traveling overseas are increasingly becoming targets of foreign collection activities. There are numerous examples of briefcases or laptop computers showing evidence of unauthorized access after being left unattended in hotel rooms. In addition, there is evidence of travelers being photographed during business meetings in foreign countries for future targeting.

- **Agent recruitment, US volunteers, and co-optees.** Foreign intelligence services and government-sponsored entities continue to utilize traditional clandestine espionage methods to collect US trade secrets and critical technologies. These methods include agent recruitment, US volunteers, and co-optees.

Appendix

Key Economic Espionage Cases Published in the Press

People's Republic of China

Case One
Two businessmen, one a Chinese national, who is the president of a Beijing-based firm, and the other a naturalized Canadian citizen, pleaded guilty to charges of illegally exporting fiber-optic gyroscopes to the PRC without the required State Department permits. Export of these gyroscopes to the PRC is prohibited. The two men bought the gyroscopes from a Massachusetts company and planned to export them to the PRC via a Canadian subsidiary of the Beijing-based firm. The gyroscopes can be used in missile and aircraft guidance systems, as well as smart bombs.

Case Two
Two naturalized US citizens were convicted of conspiring to illegally export weapons parts to their native China. They used their exporting company to purchase surplus US missile, aircraft, radar, and tank parts from the Defense Reutilization and Marketing Service and then ship them to the PRC. The exported items were on the US Munitions List that prohibited them from being shipped without a license from the State Department.

Case Three
Two Chinese scientists and a naturalized US citizen who was born in China were arrested for stealing product designs from a major US telecommunications firm and passing them to a Chinese Government–owned company in Beijing. Both Chinese scientists had received technical degrees from US universities before being employed by the US firm.

Case Four
A Chinese company based in Orlando, Florida, was charged with illegally exporting radiation-hardened integrated circuits to Chinese missile and satellite manufacturers in the PRC without the required Department of Commerce licenses. The affidavit prepared by the Department of Commerce described three illegal diversions of the missile microchips. According to weapons proliferation specialists, the microchips have military applications and could be used by the Chinese military to improve their long-range missile-targeting capabilities.

Case Five
A naturalized Chinese national was arrested for attempting to smuggle a defense-grade Radiance high-speed (HS) infrared camera to the PRC. Since the Radiance HS camera is on the US Munitions List, companies must file with the Department of State to legally export such items. The camera was destined for the Chinese State Ship Building Corporation, a state-owned conglomerate of 58 companies that is based in Beijing and Shanghai.

Pakistan

Case One
US Customs Service agents arrested two Pakistani brothers and charged them with conspiring to smuggle sophisticated cameras for military intelligence gathering to a Pakistani Government laboratory. One of the brothers was a naturalized US citizen, while the other, a Pakistani citizen, had recently completed requirements for a master's degree in engineering at a US university. A US aerospace company alerted the US Customs Service to the suspicious activities of the brothers after they attempted to purchase the cameras despite being denied an export license by the State Department.

Case Two
A British citizen pleaded guilty to violating the Arms Export Control Act by trying to ship night-vision goggles and blueprints for C-130 aircraft to Pakistan. He was acting on behalf of a firm located in Islamabad. The C-130 aircraft is used for a variety of military purposes, including troop transport, surveillance, and gunships.

Iran

A 20-month federal investigation culminated in the arrest by the US Customs Service of a naturalized Canadian from Iran and a Malaysian citizen for conspiring to illegally export aircraft parts for the F-14 Tomcat, F-5 Tiger, and F-4 Phantom to the Iranian air force. In addition, a naturalized US citizen from Iran pleaded guilty to violating the Arms Export Control Act by trying to smuggle F-14 parts into Iran.