Overseas Security Advisory Council - Global Security News & Reports

Economic Espionage Collection Methodologies

GLOBAL SECURITY CONCERNS

Worldwide 7 Jun 2007

The U.S. Department of State issued the following report on Economic Espionage Collection Methodologies:

Intelligence collectors seldom use one method in isolation to collect information from their target, but, rather, combine various methodologies into concerted collection programs. Although countries or corporations have been known to turn legitimate transactions or business relationships into clandestine collection opportunities, some of the methods listed are most often used for legitimate purposes. While their inclusion here is not intended to imply illegal activity, they are listed as potential elements of a broader, coordinated intelligence effort.

Traditional Methods

Traditional espionage methods primarily reserved for collecting national defense information are now being applied to collect economic and proprietary information. Traditional awareness training is most suitable for fulfilling these collection methods.

• *Classic Agent Recruitment* . An intelligence collector's best source is a trusted person inside a company or organization whom the collector can task to provide proprietary or classified information. A foreign collector's interest in employees is not necessarily commensurate with their rank in the company. Researchers, key business managers, and corporate executives can all be targets, but so can support employees such as secretaries, computer operators, technicians, and maintenance people. The latter frequently have good, if not the best, access to competitive information. In addition, their lower pay and rank may provide fertile ground for manipulation by an intelligence agency.

• *U.S. Volunteers*. The individuals most likely to improperly acquire a company's information are the company's own employees. Employees who resort to stealing information exhibit the same motivations and human frailties as the average thief or spy: illegal or excessive use of drugs or alcohol, money problems, personal stress, and just plain greed.

• *Surveillance and Surreptitious Entry* . Economic and industrial espionage may involve simply breaking into an office containing desired information. Companies have reported break-ins in which laptop computers or disks were stolen, even when there were easily obtainable, more valuable items in the same vicinity. These instances are not always reported, or reported as merely break-ins, without considering the possibility that the target was information rather than equipment.

Some countries convince hotel operators to provide intelligence collectors with access to

visitors' luggage or rooms. During these surreptitious break-ins, known colloquially as "bag ops," unattended luggage is searched for sensitive information, and any useful documents are copied or simply stolen.

• *Specialized Technical Operations* . This includes computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses. These activities account for the largest portion of economic and industrial information lost by U.S. corporations.

Because they are so easily accessed and intercepted, corporate telecommunications - particularly international telecommunications - provide a highly vulnerable and lucrative source for anyone interested in obtaining trade secrets or competitive information. Because of the increased usage of these links for bulk computer data transmission and electronic mail, intelligence collectors find telecommunications intercepts cost-effective. For example, foreign intelligence collectors intercept facsimile transmissions through government-owned telephone companies, and the stakes are large -- approximately half of all overseas telecommunications are facsimile transmissions. Innovative "hackers" connected to computers containing competitive information evade the controls and access companies' information. In addition, many American companies have begun using electronic data interchange, a system of transferring corporate bidding, invoice, and pricing data electronically overseas. Many foreign government and corporate intelligence collectors find this information invaluable.

• *Economic Disinformation* . Some governments also use disinformation campaigns to scare their domestic companies and potential clients away from dealing with U.S. companies. Press and government agencies frequently discuss foreign economic and industrial intelligence activities, often in vague, nonspecific terms. The issue has been used to paint foreign competitors or countries as aggressive and untrustworthy, even if the accuser has no tangible evidence of any collection activity. Some countries have widely publicized their efforts to set up information security mechanisms to protect against their competitors' penetration attempts, and frequently the United States is mentioned as the primary threat.

Other Economic Collection Methods

• *Tasking Foreign Students Studying in the United States* . Some foreign governments task foreign students specifically to acquire information on a variety of economic and technical subjects. In some instances, countries recruit students before they come to the United States to study and task them to send any technological information they acquire back to their home country. Others are approached after arriving and are recruited or pressured based upon a sense of loyalty or fear for their home country's government or intelligence service.

In some instances, at an intelligence collector's behest, foreign graduate students serve as assistants at no cost to professors doing research in a targeted field. The student then has access to the professor's research and learns the applications of the technology.

As an alternative to compulsory military service, one foreign government has an organized

program to send interns abroad, often with the specific task of collecting foreign business and technological information.

• *Tasking Foreign Employees of U.S. Firms and Agencies* . Foreign companies and governments sometimes recruit or task compatriot employees within a U.S. firm to steal proprietary information. Although similar to clandestine recruitment used traditionally by intelligence services, often no intelligence service is involved, only a competing company or non-intelligence government agency. The collector then passes the information directly to a foreign firm or the government for use in its R&D activities.

• *Debriefing of Foreign Visitors to the United States* . Some countries actively debrief their citizens after foreign travel, asking for any information acquired during their trips abroad. Sometimes these debriefing sessions are heavy-handed, with some foreign scientists describing them as offensive. In other countries, they are simply an accepted part of traveling abroad.

• *Recruitment of Émigrés, Ethnic Targeting* . Frequently, intelligence collectors find it effective to target persons of their own ethnic group. They particularly seek individuals working in U.S. military and R&D facilities who have access to proprietary and classified U.S. technology. Several countries have found repatriation of émigré and foreign ethnic scientists to be the most beneficial technology transfer methodology. One country, in particular, claims to have repatriated thousands of ethnic scientists back to their home country from the United States. Ethnic targeting includes attempts to recruit and task naturalized U.S. citizens and permanent resident aliens to assist in acquiring U.S. S&T information. Frequently, foreign intelligence collectors appeal to a person's patriotism and ethnic loyalty. Some countries collectors resort to threatening family members that continue to reside in their home country.

• *Elicitation During International Conferences and Trade Fairs* . Events - such as international conferences on high-tech topics, trade fairs, and air shows - attract many foreign scientists and engineers, providing foreign intelligence collectors with a concentrated group of specialists on a certain topic. Collectors target these individuals while they are abroad to gather any information the scientists or engineers may possess. Sometimes, depending on the foreign country and the specific circumstances, these elicitation efforts are heavy-handed and threatening, while other times they are subtle.

Foreign intelligence collectors sometimes attempt to recruit scientists by inviting them on expense-paid trips abroad for conferences or sabbaticals. The individuals are treated royally, and their advice is sought on areas of interest. When they return to the United States, collectors re-contact them and ask them to provide information on their areas of research.

• *Commercial Data Bases, Trade and Scientific Journals, Computer Bulletin Boards, Openly Available U.S. Government Data, Corporate Publications* . Many collectors take advantage of the vast amount of competitive information that is legally and openly available in the United States. Open-source information can provide personality profile data, data on new R&D and planned products, new manufacturing techniques, and competitors' strengths and weaknesses. Most collectors use this information for its own worth in their business

competition. However, some use openly available information as leads to refine and focus their clandestine collection and to identity individuals and organizations that possess desired information.

• *Clandestine Collection of Open-Source Materials* . Because they believe that they are closely monitored by U.S. Counterintelligence, some traditional intelligence services resort to clandestine methods to collect even open source materials. They have been known to use false names when accessing open-source data bases and at time ask that a legal and open relationship be kept confidential.

• *Foreign Government Use of Private-Sector Organizations, Front Companies, and Joint Ventures*. Some foreign governments exploit existing non-government affiliated organizations or create new ones - such as friendship societies, international exchange organizations, import-export companies, and other entities that have frequent contact with foreigners - to gather intelligence and to station intelligence collectors. They conceal government involvement in these organizations and present them as purely private entities in order to cover their intelligence operations. These organizations spot and assess potential foreign intelligence recruits with whom they have contact. Such organizations also lobby U.S. Government officials to change policies the foreign government considers unfavorable.

• *Corporate Mergers and Acquisitions* . Several countries use corporate mergers and acquisitions to acquire technology. The vast majority of these transactions are made for completely legitimate purposes. However, sometimes they are made specifically to allow a foreign company to acquire U.S.-origin technologies without spending their own resources on R&D.

According to a 1994 U.S. Government report entitled "Report on U.S. Critical Technology Companies," 984 foreign mergers and acquisitions of U.S. critical technology companies occurred between January 1, 1985 and October 1, 1993. All but a handful of these mergers and acquisitions were friendly, and four countries accounted for 60 percent of them. Of the total, 60 percent involved U.S. firms in advanced materials, computers - including software and peripherals - and bio-technology, areas of relative U.S. technical strength. The remaining deals involved U.S. firms in electronics and semiconductors, professional and scientific instrumentation, communications equipment, advanced manufacturing, and aircraft and spare parts.

• *Headhunting, Hiring Competitors' Employees* . Foreign companies typically hire knowledgeable employees of competing U.S. firms to do corresponding work for the foreign firm. At times, they do this specifically to gain inside technical information from the employee and use it against the competing U.S. firm.

• *Corporate Technology Agreements* . Some foreign companies use potential technology sharing agreements as conduits for receiving proprietary information. In such instances, foreign companies demand that, in order to negotiate an agreement, the U.S. company must divulge large amounts of information about its processes and products, sometimes much more than is justified by the project being negotiated. Often, the information requested is highly sensitive. In some of these cases, the foreign company either

terminates the deal after receipt of the information or refuses to negotiate further if denied the information.

• *Sponsorship of Research Activities in the United States* . Numerous foreign countries exploit a favorable research climate in the United States to sponsor research activities at U.S. universities and research centers. Generally, both the U.S. and the foreign country benefit from the finished research. At times, however, foreign governments or companies use the opportunity as a one-sided attempt only to collect research results and proprietary information at the U.S. facility. Foreign intelligence services also use these efforts as platforms to insert intelligence officers who act solely as information collectors.

• *Hiring Information Brokers, Consultants* . Information brokers scour the world for valuable proprietary data. What they cannot obtain legally or by guile, some information brokers purchase. The broker then verifies the data, puts it into a usable and easily accessible format, and delivers it to interested clients. The following advertisement published in the Asian Wall Street Journal in 1991 illustrates this activity:

"Do you have advanced/privileged information of any type of project/contract that is going to be carried out in your country? We hold commission/agency agreements with many large European companies and could introduce them to your project/contract. Any commission received would be shared with yourselves."

The ad was followed by a phone number in Western Europe.

Some countries frequently hire well-connected consultants to write reports on topics of interest and to lobby U.S. Government officials on the country's behalf. Often, the consultants are former high-ranking U.S. Government officials who maintain contacts with their former colleagues. They exploit these connections and contract relationships to acquire protected information and to gain access to other high-level officials who are currently holding positions of authority through whom they attempt to further acquire protected information.

• *Fulfillment of Classified U.S. Government Contracts and Exploitation of DOD-Sponsored Technology Sharing Agreements* . At times, classified U.S. Government contracts are awarded to companies that are partially or substantially controlled by a foreign government. Although U.S. Government security agencies closely monitor these contracts, they can still provide foreign governments unauthorized access to information. Traditional allies of the United States are most likely to use this method, since non-allies seldom are included in such contracts.

• *Tasking Liaison Officers at Government-to-Government Projects.* During joint R&D activities, foreign governments routinely request to have an onsite liaison officer to monitor progress and provide guidance. Several allied countries have taken advantage of these positions as cover for intelligence officers assigned with collecting as much information about the facility as possible. Using their close access to their U.S. counterparts conducting joint R&D, particularly in the defense arena, liaison officers have been caught removing documents that are clearly marked as restricted or classified.

Overseas Security Advisory Council • Bureau of Diplomatic Security
U.S. Department of State • Washington, D.C. 20522-2008
Telephone: 571-345-2223 • Facsimile: 571-345-2238
Contact OSAC Webmaster