# THREAT AWARENESS AND

# DEFENSIVE SECURITY BRIEFING

## Introduction

The following information is taken from the National Counterintelligence Center report "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage".

## The Foreign Intelligence Threat

The gathering of information by intelligence agents, especially in wartime, is an age-old strategy for gaining superiority over enemies. Intelligence officers—those individuals working for government intelligence services—are trained to serve their country by gathering information. Spies, on the other hand, betray their country by committing espionage. Preventing this kind of betrayal is the ultimate goal of the entire U.S. personnel security system.

While espionage has existed since countries began to battle, it was the events of the last few generations (the era of the Cold War) that concern us. During that period we had only one monolithic enemy, the Soviet Union. Our knowledge of Soviet Cold War espionage began with the defection of Igor Sergeievitch Gouzenko, a cipher clerk in the Soviet Embassy in Ottawa. In September 1945, he defected to Canada with documents that eventually led to the arrest of Klaus Fuchs and, from there, to the apprehension of the Rosenbergs and their accomplices. A series of arrests and trials in the early 1950s helped set the climate for an anti-Communist campaign to root out all Communist sympathizers in government and nongovernment areas alike. Since then, motivations for espionage have changed dramatically. Ideology was supplanted by financial greed and other motives such as disgruntlement, revenge, wanting to please others, wanting to spy simply for the thrill, or a combination of all these things.

Nobody knows exactly how many spy incidents have occurred since World War II because so many have been kept secret or have never even been prosecuted. The research of the Security Research Center (SRC) (formally known as Personnel Security Research Center [PERSEREC]) has documented at least 130 cases in the open literature. This classical form of espionage—the passing of classified information—still continues, though the recipients have changed since the end of the Cold War. In a recent informal PERSEREC study of espionage cases since 1991 (found in open sources) six cases were "old" Cold War cases where the Soviet Union or Russia was the recipient, but the remaining nine involved spies who worked for a variety of countries, some of which were U.S. allies.

## The New Threat

Classical espionage cases still occur, but now we are seeing an increase in a different kind of spying—an espionage based on not only the theft of classified information but also on theft of high-technology information, classified or unclassified. This economic espionage is not a new phenomenon; its frequency has increased greatly in recent years. Estimates of current yearly U.S. loss of proprietary business information now range between $20 billion and $100 billion. This loss, and the loss of other technological information, is especially detrimental to our economic

vitality and may, by extension, have deleterious effects on U.S. security interests, since economic and national security are so closely linked in our highly competitive new world.

By now everyone understands that the end of the Cold War brought massive changes in the global economic structure. An intensified struggle for international *economic* power has taken the place of military superiority. Currently, a host of foreign governments and individuals (present adversaries, former foes and traditional friends) are expending considerable resources in attempting to acquire our technological know-how through economic espionage. Economic espionage is the acquisition by foreign governments or corporations of U.S. high-technology information in order to enhance their countries' economic competitiveness. (Please note that this discussion is limited to espionage conducted by foreign governments against the U.S. Government or U.S. companies, defense-related or otherwise. We are not discussing intercorporate or industrial espionage within the United States [i.e., American companies spying against each other] although sometimes the methods used are similar.)

The FBI believes that nearly 100 countries are now running economic espionage operations against the United States. Targets are shifting away from the classified military information sought in the old Cold War days toward basic research and development processes. Such targets also include the technology and trade secrets of U.S. high-tech companies—everything from cost analyses, marketing plans, contract bids and proprietary software to the high-tech data itself. Any information or process—whether classified, unclassified or proprietary—that leads to cutting-edge technology is plainly in demand. Some products are bought (or stolen) in this country and then physically smuggled abroad. Often the technology is not a physical product; it may be a plan, formula or idea that can be transported on computer or fax machine, or simply carried away inside the minds of scientists.

As suggested above, the economic espionage threat is not confined to America's traditional adversaries. Allies can be just as interested in U.S. technological know-how as our traditional foes from the Cold War. Countries are aggressively targeting American firms at home and abroad for industrial secrets that are critical to U.S. economic security. American corporations are now facing several foreign competitors who, backed by their intelligence services, are trying to steal trade secrets and technical data on a massive scale.

Who are these new spies? How do they present themselves? They may be informal representatives of their countries or people paid by their countries to spy. They may be visiting the United States on scientific exchanges, business tours, or with on-site inspection teams. They may be trade representatives or liaison officers at their embassies here. Some may be foreign moles placed in American companies by their country's government, or students doing research in the United States who serve as informal conduits to their home governments. They may be foreign business people who can manipulate the communications systems of U.S. high-tech companies. They may also be Americans, disgruntled or greedy employees of U.S. companies, who, having volunteered or been recruited, are willing to sell classified, proprietary or high-tech information to other countries. (Fifty percent of attempts to misappropriate proprietary information involve U.S. employees or ex-employees.) Whoever they are, foreign or home-grown, they are generally well educated and technologically sophisticated, and certainly well able to navigate in high-tech waters.

Many U.S. high-tech industries have been targeted but, according to a recent government report,

the following areas are the most vulnerable: biotechnology, aerospace, telecommunications, computer software and hardware, advanced transportation and engine technology, advanced materials and coatings (including stealth technologies), energy research, defense and armaments technology, manufacturing processes, and semiconductors. Not yet classified proprietary business information is aggressively targeted. The industries listed above are of strategic interest to the United States because they contribute so greatly to leading-edge, critical technologies. A 1995 report by the National Counterintelligence Center adds that foreign collectors have also exhibited an interest in government and corporate financial and trade data. Clearly, this list does not cover every high-tech area that is being targeted, but it provides a sense of some of the areas that are vulnerable.

**The Methods of Espionage**

Economic espionage is often conducted by using basic business intelligence-gathering methods. The Internet and dozens of commercial databases are widely available, along with such sources as trade journals and company newsletters and annual reports. So much technical information is available in the United States in open sources that it hardly would seem necessary to resort to illegal means; in effect, much of science and technology in this country is here for the taking. There are vast repositories of technical information with the National Technical Information Service (NTIS) and the Defense Technical Information Center (DTIC). Foreigners can make direct requests to the Department of Defense and, of course, a great deal of information is published in academic and technical journals and in newspapers and trade publications, and thus available to anyone.

However, employees need to be alert when such activities as extracting information from executives of competing companies under the guise of job interviews, or hiring away an employee from a competitor just to acquire that person’s knowledge occur.

In a world becoming more and more interconnected, systems for exchanging information are clearly necessary for research and commerce to thrive. The United States invites foreign scientists to its research institutes and laboratories in programs designed to enhance knowledge through the cross-fertilization of ideas. And we enter into exchange agreements with other countries to foster research and development, provide security or technical assistance, and so forth. Less economically developed countries—both allies and foes—do take advantage of the openness of our system. Some caution and wariness are thus suggested in order to prevent the disclosure of too much information.

A major means for foreign governments to obtain information is by sending their representatives to the United States on fact-finding visits or for training. Participants in scientific meetings, trade delegations and trade shows can easily obtain useful information during their stays here. Other arrangements, such as visitor programs, cultural exchanges and military exchanges, are also used. One fruitful method is sending students and scholars to U.S. universities or government research laboratories where they are trained and also participate in research as guests of the U.S. Government. High-tech data, acquired by scientists participating in such programs, is easily transferred back to home countries through fax, telephone, the written word, and by memory.

Foreign governments or their representatives often attempt to acquire high-tech information by establishing joint venture companies with Americans. This allows them direct access to U.S.

know-how not always available in the public domain, especially if the companies conduct classified work. Other standard business practices in this general category include mergers, strategic alliances, licensing agreements, and corporate technology agreements. It must be noted, however, that joint ventures are often encouraged by the United States. For example, the Bureau of Export Administration in the U.S. Department of Commerce has programs to encourage such ventures with the newly independent states of the former Soviet Union, as a way to expand U.S. trade in those areas.

Another way of acquiring high-tech information is to purchase U.S. high-tech companies, preferably those with government contracts, or for foreigners to set up their own companies in the U.S. to collect information on certain technologies and to train their own personnel. Related to establishing companies in the U.S. is the commonly used device of creating front companies. These are companies set up to undertake "legitimate" business but used by the foreign government to further its own economic espionage purposes.

Often foreigners acquire proprietary information under the guise of market research, sending surveys from abroad to ferret out product information. Even personal telephone calls, letters and fax inquiries from abroad can elicit useful information. Callers may pretend to be someone other than who they are; in the parlance of the business intelligence fraternity this is known as pretext calling.

Some economic espionage cases resemble typical old-style espionage operations conducted with the full panoply of tradecraft. Indeed, the very words used to describe the roles of participants in an economic espionage crime are borrowed directly from the classic espionage lexicon: spies, moles, recruiters, defectors.

The "best" way to acquire information from an organization or company is—in classic spy style—to recruit a mole on the inside or to send one of your own people in on a ruse, posing as someone else. Another method is to blackmail vulnerable employees of U.S. companies or to recruit foreign nationals working in U.S. subsidiaries abroad. Not all spies have been recruited. Some, perhaps disgruntled or troubled, employees, past or present, of U.S. companies have stolen materials and then sold them to foreign companies—the *volunteer* of classic espionage.

Equally as unscrupulous, and also patently illegal, is the outright bribing of employees to steal plans, reports and other proprietary documents, or hiring so-called consultants to spy on competitors, a practice that can include bugging competitors' offices. Other methods include theft and smuggling of goods, theft of intellectual property, tampering with companies' electronics, bribery, and so forth.

**The Damage**

At the industry and company level, the compromise of industrial technology often translates into lost contracts, loss of trade secrets and loss of technology (in the billions) and loss of technological edge over our competitors. In this age of shrinking budgets and tighter control over expenses, economic espionage can be very profitable; the less money a company has to spend on research, the greater its profit margin.

**The Old Threat Still Lingers**

All this discussion of economic espionage does not mean that traditional, classical espionage has ceased. It only means that espionage has shifted to some degree, away from stealing classified information to a new interest in acquiring high-tech information that might be advantageous to a foreign country. Classical spy cases continue, the most famous case being Aldrich Ames, a veteran CIA intelligence officer who volunteered highly secret and sensitive CIA information to Soviet and Russian intelligence from 1985 to 1994. It is known that at least 11 agents lost their lives and that Ames gave the KGB tens of thousand of classified documents, in what will surely be the spy case of the century. On the heels of Ames came a second CIA case, Harold Nicholson, arrested at the end of 1996 on espionage charges that he had sold secrets to Moscow for 29 months. Nicholson was a CIA operations officer.

There have been several other cases recently, involving individuals who were caught before they could do any real harm. For example, John Charlton, a retired engineer, was arrested in May 1995 for trying to sell secret documents stolen from his company at the time of his retirement. Between July and September 1993 he tried to sell the information for $100,000 to an FBI agent posing as a representative of a foreign government. In April 1996 he was sentenced to two years in prison and fined $50,000.

Another case in 1996 concerns a Navy machinist mate who sold an undercover FBI agent top secret information on nuclear submarines. The Petty Officer 1st Class, an instructor at the Naval Nuclear Power School in Orlando, Florida, was charged after he was video taped turning over documents to an FBI agent posing as a Russian. The young instructor, unbeknownst to him, was dealing all the time with an FBI agent, not a foreigner. His trial is still pending.

In another recent and aborted attempt, a civilian Navy intelligence official, a naturalized American, was accused of spying for his native country in Asia after he was arrested by the FBI. This individual is charged with transferring classified information to an agent of a foreign government.

Losses caused by theft of U.S. military secrets can be massive. In times of crisis such losses can weaken and even destroy the country's national defense by alerting enemies of our military plans and new weaponry. Often the damage that results from the compromise of military secrets is impossible to repair. The information supplied to the Russians by John Walker, for example, enabled them to gain access to our weapons and sensory data, naval tactics, submarine and airborne training, military operations, and intelligence activities. In short, it permitted the Russians to measure the true capability and vulnerability of the U.S. Navy and to improve their own military positions dramatically.

**Indicators of Espionage**

Studies of traditional espionage cases have revealed a pattern of warning signs displayed by several of the spies in varying degrees. The most common indicators of an individual's espionage activity or potential vulnerability to espionage are mentioned below and should be a matter of concern to security and supervisory personnel.

Signs that an individual might be involved in espionage include attempts to gain access to classified information without a valid need-to-know or without the required security clearance. Other indicators might be unauthorized reproduction or removal of classified material from the

work area and secret destruction of documents. Unexplained affluence can be a possible sign of ongoing espionage if a legitimate source of increase income cannot be found. Sudden prosperity might be of particular concern when it follows a period of financial difficulties.

Foreign travel, on a regular basis and without sufficient explanation, might be another sign of espionage when individuals with access to classified information are involved. Job and career dissatisfaction or deep grudges against the company or the U.S. Government have also figured as predisposing elements in some cases.

**Facing the Challenge**

In summary, espionage against the United States, both economic and classical, continues to occur, and the threat it poses to U.S. national security and economic well-being is immense. Increasingly, economic espionage efforts directed against the United States come not only from present foes but also from friends and allies, all in search of U.S. high-tech and commercial secrets. With billions of dollars invested in research and development, the United States is a tempting target for friendly nations, former foes, and traditional adversaries alike.

The current challenge for security professionals is to make employees understand that, despite the vast political changes around the globe, foreign intelligence activities really do continue to be directed against the United States. Many people believe that there is no longer the danger of espionage. Many believe, for example, that it is no longer necessary to restrict the flow of scientific and technical information to our highly industrialized allies or to newly emerging democracies. However, experience has shown that the United States often gives away far more than it gets and that scientific "exchange" is more likely than not to be a one-way street. The cheapest way to gain access to economic and scientific information is to take what is freely given (by the U.S.) or to steal it. Employees of the U.S. Government and U.S. industry must be aware of this still-present danger and be able to recognize all warning signals. Moreover, they must understand their responsibilities to report any suspicions they may have of workmates or visitors so that the appropriate authorities can investigate the situation.