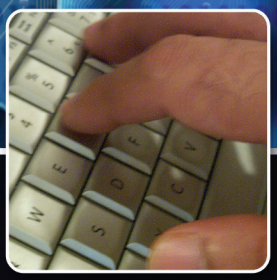
ANNUAL REPORT TO CONGRESS ON

FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2005



NCIX 2006-009
August 2006

August 2006

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage--2005

NCIX 2006-009

August 2006

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage--2005

This assessment was prepared by the Office of the National Counterintelligence Executive. Comments and queries are welcome and may be directed to the National Counterintelligence Officer for Economics, NCIX, on (703) 682-4500 or at www.ncixinfo@ncix.gov.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2005

Key Findings

Entities from a record number of countries—108—were involved in collection efforts against sensitive and protected US technologies in FY 2005, [1] according to evidence amassed by the Counterintelligence (CI) Community. A relatively small number of countries, though—including China and Russia—were the most aggressive and accounted for much of the targeting, just as they have since the CI Community first began systematically tracking foreign technology collection efforts in 1997.

Foreign collection efforts have hurt the United States in several ways. The technology losses have:

- Eroded the US military advantage by enabling foreign militaries to acquire sophisticated capabilities that might otherwise have taken years to develop.

- Undercut the US economy by making it possible for foreign firms to gain a competitive economic edge over US companies.

Private-sector players—foreign businessmen, scientists, engineers, students, and academics—were active collectors in FY 2005, although those who engaged in theft represented only a small fraction of total foreign experts in the United States. Moreover, evidence suggests that the vast majority of those who did attempt to steal technology or trade secrets did not initially come to the United States with that intent nor were they directed to do so by agents of foreign governments. Instead, after finding that they had access to information that was in great demand abroad, most engaged in illegal collection to satisfy their desire for profits, for academic or scientific acclaim, or out of a sense of patriotism to their home countries.

A number of factors have combined to facilitate private-sector technology theft. Globalization, while generating major gains for the US economy, has given foreigners unprecedented access to US firms and to sensitive technologies. There has also been a proliferation of devices that have made it easy for private-sector experts to illegally retrieve, store, and transfer massive amounts of information, including trade secrets and proprietary data; such devices are increasingly common in the workplace.

[1] From 1 October 2004 to 30 September 2005.

At the same time, the sophisticated information systems that create, store, process, and transmit sensitive information remain vulnerable to cyberexploitation.

Foreign government entities—including intelligence organizations and security services—have learned to capitalize on private-sector technology acquisitions. Some governments have established quasi-official organizations, either in the United States or in their home countries, to facilitate contact with overseas scientists, engineers, and businessmen. These organizations enable foreign government officials to directly gauge the level of access that various foreign experts have, or may gain, to sensitive US technology. The identified experts can be approached for sensitive information when they return to their home countries, thereby avoiding the need for meetings in the United States that could fall under the watchful eyes of the US law enforcement community.

Foreign government organizations also mounted their own targeting and collection operations in FY 2005. Official foreign collectors were observed:

- Targeting US firms for technology that would strengthen their foreign defense capabilities.

- Posting personnel at US military bases to collect classified information to bolster military modernization efforts.

- Employing commercial firms in the United States and in third countries to target and acquire US technology.

- Recruiting students, professors, scientists, and researchers to engage in technology collection.

In FY 2005, as usual, the cheapest, easiest, and least risky methods for acquiring sensitive technologies were the ones most heavily employed. Techniques that were used included:

- Making direct requests for classified, sensitive, or export-controlled information. In some cases, a single would-be foreign buyer sent out multiple requests to a variety of US companies, searching for a seller willing to ignore or bend export-licensing requirements.

- Forming ventures with US firms in the hope of placing collectors in proximity to sensitive technologies or else establishing foreign research

facilities and software development companies outside the United States to work on commercial projects related to protected programs.

- Offering technical services to US research facilities or cleared defense contractors in the hope of gaining access to protected technologies.

- Exploiting foreign visits to the United States and collecting at conventions and expositions.

- Relying on cybertools to collect sensitive US technology and economic information. Several foreign companies have become world leaders in the use of cybertools.

Again in FY 2005, foreign collectors targeted the entire range of items on the Militarily Critical Technology List (MCTL). The major collecting countries, in particular, attempted to vacuum up a wide variety of militarily critical technologies. Information technologies were again the most heavily targeted MCTL, accounting for almost 30 percent of suspicious incidents for all reporters. Other technologies that were heavily targeted included lasers and optics, aeronautics, sensors and armaments, and energetic materials. FY 2005 data showed a significant increase in the targeting of space systems technology.

During the next few years, the CI Community expects no slackening in demand for state-of-the-art US technology and production know-how. Continued fierce global economic competition will fuel commercial technology theft. At the same time, the demonstrated military benefits associated with advanced US technology will remain dominant drivers for illegal acquisitions of military and dual-use items.

As globalization continues to pressure US companies to move important technologies and even research and development facilities overseas, third-country venues may become increasingly important locations for US technology acquisition. Both the security and legal frameworks for protecting technologies abroad tend to be weaker than in the United States.

Other developments that the CI Community believes will facilitate the illegal outflow of US technology during the next few years are:

- The increased dependence of the US manufacturing and service sectors on foreign inputs, particularly software and hardware components, which opens the door to greater supply chain vulnerabilities.

- The increased presence in the workplace of devices like cell phones with digital photographic capability and Personal Digital Assistants with significant storage capability that can be employed for stealing technology.

- The continued expansion of international linkages among countries that will create global brokers skilled in moving technologies across borders and undercutting the ability of the US Government to control exports.

Contents

Scope Note

This is the llth annual report reviewing the threat to the United States from foreign economic collection and industrial espionage. The report seeks to characterize and assess efforts by foreign entities—government and private—to target or acquire critical US technologies, trade secrets, and sensitive financial or proprietary economic information. The loss of these could undermine US military capability, impede the ability of US firms to compete in the world marketplace, or have an adverse effect on the US economy, thereby weakening national security and eroding the current US technological lead.

The report is being submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359, which requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. It updates the 10th annual report published in April 2005 and includes data for FY 2005, the period 1 October 2004 through 30 September 2005. The information in this report also satisfies one of the requirements stipulated in the Defense Production Act of 1950, as amended, that the President provide quadrennial reports on whether foreign governments sponsor industrial espionage activities to obtain US critical technology assets.

As in previous years, the report deals with the acquisition of sensitive US technology—either classified or proprietary—by foreign entities, both government and private. The acquisitions take a variety of forms, including:

- **Economic espionage**, which is generally defined by Section 1831 of the Economic Espionage Act of 1996 (EAA) to be the theft of trade secrets in which the perpetrator acts intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent. Proving links between foreign governments and entities caught stealing US trade secrets is often impossible.

- **Industrial espionage or trade secret theft,** which is the acquisition of sensitive information that has independent economic value and that the owner has taken reasonable measures to protect, regardless of the perpetrator's country of origin or whether a foreign government agent

can be linked to the theft. The acquisition must be intended for the economic benefit of someone other than the owner. Sensitive information encompasses all types of financial, business, scientific, technical, economic , or engineering information. It includes patterns, plans, compilations, program devices, formulas, designs, prototypes, techniques, processes, programs, and codes, whether tangible or intangible and regardless of how the information is stored. Section 1832 of the EEA covers such violations.

- **Violations of export-control regulations**

  —*Transfer of dual-use equipment and technology:* Includes unauthorized acquisition of restricted US dual-use items—having both military and civil applications—by countries or persons that might apply such items to uses inimical to US interests. These items include goods and technology that might be related to the proliferation of weapons of mass destruction and their delivery means and those that could bolster the military and terrorism support capability of certain countries. The Department of Commerce's Bureau of Industry and Security administers the Export Administration Regulations and enforces violations of these rules.

  —*Transfer of defense items:* Includes unauthorized export of defense articles, defense services, and related technical data (collectively known as the U.S. Munitions List). These Munitions List items include US arms and implements of war. The State Department's Directorate of Defense Trade Controls administers the International Traffic in Arms Regulations and enforces violations of these rules. The State Department maintains a policy of denial for exports of any Munitions List item to proscribed countries, which could misuse or cause illegal proliferation of those items.

The paper highlights foreign efforts to target sensitive US technologies even when those efforts are legal. For example, it is not illegal for foreign entities to request classified or controlled information or technology, even though the actual export of that technology would violate US laws. The fact that such technologies are being targeted, however, is considered important information for this report. This paper does not cover violations of US copyright laws, such as the illegal plagiarism of videos, compact disks, or other literary or artistic works.

This assessment is a product of a cooperative effort across the CI Community. It was compiled by the Office of the National

Counterintelligence Executive on the basis of input from a broad cross-section of US Government entities. In particular, information compiled by the Defense Security Service, the Air Force Office of Special Investigations, and the Army Counterintelligence Center was instrumental in providing much of the detail for this Community assessment. The Federal Bureau of Investigation—the lead investigative agency for enforcing economic espionage statutes—provided significant information on economic espionage trends. In addition, the Department of Defense's Counterintelligence Field Activity and the Department of Energy added important data on foreign visitors to the United States, and the National Geospatial-Intelligence Agency provided input on foreign students.

A host of other organizations within the CI Community also made major contributions to and/or have coordinated on this report, including:

- US Immigration and Customs Enforcement (ICE).
- Central Intelligence Agency (CIA), including the Counterintelligence Center (CIC), the Open Source Center (OSC), the Information Operations Center (IOC), and several of CIA's geographic offices.
- Defense Intelligence Agency (DIA).
- Defense Threat Reduction Agency (DTRA).
- Defense Technology Security Administration (DTSA).
- Department of Commerce, Bureau of Industry and Security (BIS).
- Department of Energy (DOE).
- Department of Justice (DOJ).
- Department of State, including the Bureau of Intelligence and Research (State/INR) and the Bureau of Diplomatic Security (State/DS).
- National Reconnaissance Office (NRO).
- National Security Agency (NSA).
- Naval Criminal Investigative Service (NCIS).

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2005

One of the essential objectives of the Presidentially approved National Counterintelligence Strategy of the United States is to safeguard our vital national security secrets, critical assets, and technologies against theft, covert foreign diversion, or exploitation. This includes both helping to protect the sensitive technologies that are the backbone of our security and seeking to ensure a level economic playing field so that business and industry are not disadvantaged by foreign intelligence operations.

Amb. Eric J. Boswell
Former Acting National Counterintelligence Executive

The Threat to US Technologies

The Damaging Theft of US Technology and Trade Secrets

Foreign entities continued to aggressively target and acquire sensitive and protected US technologies in fiscal year 2005 (FY 2005).[2] Evidence amassed by the Counterintelligence (CI) Community showed a record number of countries—108—were involved in collection efforts. The Federal Bureau of Information (FBI) opened 89 economic espionage cases during the year and had 122 cases pending at yearend. In addition, the US Immigration and Customs Enforcement initiated more than 1,050 export investigations and conducted more than 2,400 export investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations, Export Administration Regulations, International Emergency Economic Powers Act, and the Trading With the Enemy Act. These investigations resulted in 101 arrests, 70 criminal indictments, and 85 criminal convictions. The Department of Commerce, Bureau of Industry and Security, initiated more than 1,300 export investigations resulting in 31 criminal convictions and the imposition of almost $8 million in criminal fines and $9 million in civil penalties.

The CI Community is unanimous in the view that this illegal outflow of technology imposed huge costs on the United States. A sample of the types of technologies lost during the year indicates the potential extent of damage.[3] Recent losses have hurt the United States by:

- Enabling foreign militaries to leapfrog technological hurdles and to acquire sophisticated capabilities that might have otherwise taken years to develop. A former Department of Defense (DoD) contractor provided China and a number of other countries with access to classified and export-controlled infrared signature suppression technologies developed for the B-2 Stealth Bomber. Such acquisitions would provide foreign militaries with an invaluable jump in developing stealth aircraft of their own or in countering the US advantage.

[2] From 1 October 2004 to 30 September 2005.

[3] Calculating a precise dollar figure for these losses would be difficult. Any such estimate must make fair market value estimates of the technologies lost by firms and the value of replacement technologies necessary to remain competitive. The figure must also consider factors such as lost sales as well as marketing and shipping costs. One of the challenges that makes calculating the cost of industrial espionage particularly difficult is that the technology losses often are not readily apparent. The only indication a US company may have that its research and development plans or its marketing strategies have been stolen is a shrinking or even a more slowly growing market share as foreign and domestic firms take advantage of price and product information to win customers. Likewise for national security secrets, often the only evidence of a loss of a key military technology is the emergence of a new or more sophisticated weapon or countermeasure in a foreign arsenal years later.

- Making it possible for foreign firms to gain a competitive economic edge over US competitors, thereby undermining the US economy. For example, in 2005, a major Japanese firm was fined more than $400 million after it was found guilty of stealing a US company's trade secrets and selling them to a competitor.

As in years past, entities from a relatively small number of countries accounted for the majority of foreign targeting of US technologies in FY 2005. China and Russia are two of the most aggressive collectors. The major collectors have been repeatedly identified targeting multiple US Government organizations and all types of technologies since at least 1997, when the CI Community first began systematically reporting on targeting efforts.

Globalization Expands Access to Sensitive Technologies

Foreign businessmen, scientists, engineers, students, and academics were major collectors of sensitive US technology in FY 2005. The openness of the US economy and the forces of globalization provide both opportunities and powerful natural incentives for this private-sector technology theft. The sheer number of visitors explains, in large part, why most of the opportunities devolved to the private sector. More than 30 million foreigners entered the United States on nonimmigrant visas in 2004, according to the most recent Department of Homeland Security's Office of Immigration statistics (see table 1). Most visitors came as tourists and had limited access to sensitive technologies. Almost 5 million, however, came on business visas, and many would have had access to sensitive US technologies or trade secrets. The number far exceeded the 350,000 official foreign visitors to the United States in 2004. US companies seeking to develop overseas markets sometimes employ first-generation immigrants who are bilingual and who maintain connections in their home countries. Such individuals, especially those with advanced degrees in scientific and technological fields, are well placed to broker illegal technology transfers from the United States.

The vast majority of these visitors—businessmen, scientists, and tourists—do not come here with the intent to collect sensitive technologies or economic information. Of the small percentage that eventually did steal US trade secrets, we doubt that foreign governments were directly involved in tasking these collectors (see text box). Instead, profits, patriotism to their home countries, and the desire to achieve academic or scientific acclaim appear to be the natural drivers—the so-called invisible hand behind most private-sector technology theft.[4] Indeed, most of those arrested for stealing US technology appear to have become involved in the theft after finding, serendipitously, that they had access to information that was in great demand in their home countries.

Globalization has intertwined US and foreign businesses in ways that have generated huge economic gains for both sides but that also have made it increasingly difficult to protect commercial and dual-use trade secrets. In 2004, the latest year for which data were available, foreign direct investment in the United States rose 8 percent—the fastest growth since a 32-percent increase in 2000—to

[4] Adam Smith originally coined the term "invisible hand" in his 1776 book *An Inquiry into the Nature and Causes of the Wealth of Nations.* The term was Smith's way of describing the mechanism by which he felt economic society operated. Smith noted that each individual in society strives to become wealthy "intending only his own gain" by providing what others in society value. Thus an "invisible hand" produces what is best for society even though the individual is driven only by self-interest. Nowadays, something much more general is meant by the expression. An invisible hand process is one in which the outcome to be explained is produced in a decentralized way, with no explicit agreements between the acting agents. The second essential component is that the process is not intentional. The agents' aims are neither coordinated nor identical with the actual outcome, which is a byproduct of those aims. The process is invisible because it works without the agents having knowledge of it.

Table 1
Nonimmigrants From Selected Countries Admitted to the United States, 2004

(Number of visitors)

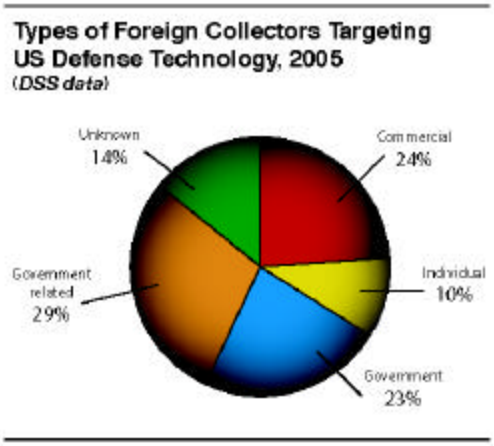
Rank	Country of Last Residence	Business	Pleasure	Other	All Classes
	All Countries	**4,593,124**	**22,802,907**	**3,385,299**	**30,781,330**
1	United Kingdom	606,398	4,042,056	132,561	4,781,015
2	Mexico [a]	443,802	3,779,304	206,178	4,429,284
3	Japan	381,281	3,648,711	178,248	4,208,240
4	Germany	301,361	1,139,036	78,095	1,518,492
5	France	187,769	832,883	51,735	1,072,387
6	China [b]	177,323	278,941	103,242	559,506
7	Korea	164,674	431,726	118,420	714,820
8	Brazil	108,711	336,596	67,685	512,992
9	Australia	107,787	458,139	30,980	596,906
10	Netherlands	105,969	386,966	16,023	508,958
11	Italy	103,942	486,541	33,347	623,830
12	Canada	97,960	346,641	139,953	584,554
13	India	88,011	185,854	168,463	442,328
14	Israel	74,679	218,104	24,103	316,886
15	Venezuela	68,771	262,658	31,273	362,702

[a] The increased use of Department of Homeland Security Form I-94 for the inspection of Mexican nationals helps explain the increased number of admissions after 1997.

[b] Includes People's Republic of China and Taiwan.

Source: Office of Immigration, *Yearbook of Immigration Statistics: 2004*.

How Much Private, How Much Government Directed?



Because of the complex nexus between public- and private-sector players in the theft of technology, it is virtually impossible to accurately gauge exactly how much collection can be attributed to the various players. Defense Security Service (DSS) data, however, provides one measure of the activity. The DSS data comes from reporting by cleared defense contractors. Because foreign state-sponsored organizations probably target US defense contractors more heavily than do foreign commercial entities, the DSS figures may show a larger government role than would similar statistics derived from US commercial firms. Even here, though, DSS data shows a significant portion of the activity comes from commercial enterprises or from private individuals.

$1,526 billion at the end of 2004.[5] A couple of the notable foreign acquisitions of US high-tech companies in the past few years included the purchase of fiber-optic network provider Global Crossing by Singapore Technologies Telemedia and the more recent takeover of IBM's personal computer (PC) business by China's computer giant Lenovo.[6]

Increasingly, foreign entities may not even need to come to the United States to access key US technologies. US firms increasingly feel compelled to move design specifications and even sensitive source code overseas in an effort to take advantage of foreign tax incentives or to shorten the supply cycle.[7] Just-in-time inventories and the speed necessary to bring new items to market to meet rapidly changing international demands also work to break down barriers to the outflow of sensitive technology. Once abroad, this information—previously considered too sensitive to share with foreign partners—becomes difficult to protect. In late 2004, for example, a US software manufacturer reported that portions of its source code and confidential design documents of one of its key products had been stolen from a recently opened research and development (R&D) center in Mumbai, India, according to press reports. The firm's security practices quickly uncovered the theft, but the organization had difficulty finding legal recourse to stop further dissemination of the information.

[5] Valued at historical cost—the book value of foreign direct investors' equity in, and outstanding loans to, their US affiliates.

[6] The United States has a mechanism in place to prevent foreign investment that is deemed to threaten US strategic interests. The Committee on Foreign Investments in the United States reviews such investments and can recommend that the President suspend or prohibit a foreign acquisition or, in the event that a takeover has already occurred, recommend he request the Attorney General to seek appropriate relief—including divestiture—in the district courts of the United States. Similarly, US federal laws require firms that have access to US classified information to be generally free from foreign ownership, control, or influence.

[7] In December 2004, for example, another major US firm announced its intent to open a $12 million research and development center in Tokyo, Japan. The new center will focus on developing Internet Protocol–based networking technologies. In late 2005, according to press reports, a major US chipmaker announced plans to spend $3.5 billion to build a new state-of-the-art chip-making plant in Israel.

This enmeshing of US and foreign firms is also creating supply-chain vulnerabilities. Foreign firms are increasingly becoming the primary or even sole providers of key information technology (IT) components, both hardware and software, for US industry. This dependence raises the possibility that components could be altered to allow clandestine access to IT systems and the trade secrets and technologies that they hold. The ability to insert altered IT components into US supply chains presents other threats to national security as well, such as creating opportunities for asymmetric warfare, espionage, and for degrading US critical national infrastructure.

The openness of the US economy has also given foreign individuals unprecedented access to high-tech US research facilities.

- Almost 30 percent of the science and engineering faculty employed at US universities and colleges are foreign born, according to National Science Foundation statistics.[8]

- Annual foreign student attendance at US institutes of higher education has averaged more than 570,000 since the beginning of the 2000 academic year, compared to an average of 460,000 students during the previous decade. More than 40 percent of PhDs awarded in science and engineering in the United States in 2004 went to foreign citizens; in physics and mathematics, the shares were around 55 percent.

Most of the foreign students and academics working in US research institutes are not involved with US technology theft. In fact, many significantly contribute to the advancement of research at their respective universities and institutes. However, the sheer size of the population and the access that some have to key R&D projects make it inevitable that this group will serve as an important funnel abroad for technologies.

At the same time that foreign access to sensitive US technologies is expanding, rapid advances in IT have vastly simplified the illegal retrieval, storage, and transfer of massive amounts of information, including trade secrets and proprietary data. Compact storage devices the size of a finger are now capable of handling up to five gigabytes of memory. Cell phones with digital photographic capability and the ability to wirelessly connect to the Internet are some of the other new facilitators in technology transfer. Sophisticated information systems that create, store, process, and transmit sensitive information are vulnerable to cyber exploitation. Many nations have formal programs for gathering our networked information, and foreign competitors are developing the capability to exploit those vulnerabilities.

The fact that the US technology is acquired by the private sector in no way slows its flow to foreign governments or inhibits its use in military applications. This transfer from the private to the public sector often happens voluntarily and seamlessly in countries like China and Russia, where there are hand-in-glove relationships between industry and government.[9] But even in most Asian and European countries, the CI Community sees continued evidence of cooperative information sharing between the public sector and the private firms that have acquired sensitive US technology.

[8] Several of the countries that send the most students to the United States are also among the top foreign collectors of US technology, and all experienced increases in enrollment during 2004-05.

[9] A Chinese Web site advertising a technology exhibit in April 2006 in Chongqing, China, highlights the emphasis Beijing places on facilitating the transfer of technology from civil to military uses. According to the Web site, the exhibit has three objectives: breaking down the barriers to sharing technology among industries, bureaucratic entities, and state and private sectors; facilitating coordinated development between the civilian hi-tech sector and the military; serving as a technology-exchange platform for civilian and military technologies.

Government Collectors Learn To Ride Private Coattails . . .

Although the private sector played an important role in collection last year, foreign governments were by no means out of the picture. In fact, there was ample evidence in FY 2005 that foreign intelligence services, defense establishments, and other government organizations remained aggressive in two ways. First, they became more effective in capitalizing on the increased private-sector collection activity underway, letting the invisible hand drive the collection process and then tapping the technology collected to meet official needs. Second, foreign government entities continued their own direct operations to collect technologies that commercial sources seemed unable to provide.

Foreign governments and intelligence organizations have created quasi-official organizations to enable them to capitalize on the private-sector theft that is underway. Indeed, the CI Community believes that foreign governments are major beneficiaries of the private-sector technology flow (see text box). To elicit sensitive information from those attending these quasi-official organizations, government officials may appeal to the professional egos of the private sector contacts, to their patriotism, or to their commercial sensibilities, by offering domestic business deals to accomplish the technology transfer. Coercion is also an option in countries like Russia and China, where security services still hold considerable sway over the private sector.

. . . But Foreign Government Organizations Also Directly Target US Technology

Although they have had significant success in capitalizing on the private-sector theft, foreign government organizations—including intelligence and security services—also mounted their own targeting and collection operations in FY 2005. Instances of official collection efforts were plentiful during the year.

The Problem of "Deemed Exports"

The "deemed export" rule of the Export Administration Regulations (EAR) applies to the release of "technology"—as defined in the EAR—to a foreign national in the United States. Such release is deemed to be an export to the country in which the foreign national holds citizenship status. Technology, in the context of EAR, means specific information required for the development, production, or use of a product. It may take the form of technical data or technical assistance. "Release" may occur in visual inspection by foreign nationals of US-origin equipment and facilities, oral exchanges of information in the United States or abroad, or in the application to situations abroad of personal knowledge or technical experience acquired in the United States. Naturalized US citizens and foreign nationals holding valid permanent resident status in the United States (green card holders) are not subject to the deemed export rule.

Although the CI Community believes that a significant amount of protected US technology leaves the country each year after being released to foreign nationals in the United States, so far, there has been only one case tried for violation of the deemed export law. In 2004, a US company, whose primary shareholder was a Chinese firm controlled by the People's Republic of China Government, failed to obtain export licenses for three Chinese nationals who worked at the company and were trained in manufacturing technology controlled by the EAR. The result was the transfer to China of knowledge concerning the manufacture of export-controlled products with direct military applications.

In our view, the reason so few cases have been prosecuted under the deemed export law is the difficulty in observing deemed exports. With no observable movement of goods, the transfer is virtually impossible to detect, let alone prosecute. The absence of prosecutions, in turn, may be a factor in lowering the awareness of the US scientific community to the extent of the problem.

Table 2 *(Number of visitors)*
Countries Sending the Most Foreign Visitors to DOE/NNSA Facilities, FY 2005

Rank	Country	All DOE/NNSA Facilities	Weapons Labs
	Total	**10,477**	**1,458**
1	China	4,011	404
2	India	2,202	300
3	Russia	2,150	403
4	Taiwan	459	85
5	Ukraine	348	31
6	Israel	336	76
7	France	256	47
8	Japan	231	25
9	Pakistan	174	44
10	South Korea	156	22
11	Kazakhstan	80	21
12	Iran	34	0

The steady flow of foreign officials and organizations to US military bases and laboratories in FY 2005 created opportunities for foreign intelligence efforts against US technologies. During FY 2005, delegations from several countries that are considered to be major collectors against US technology requested almost 900 visits to US military bases and more than 2,700 visits to DoD industries—a 35-percent increase from the previous year. During the same period, more than 9,000 foreign visitors from the same countries visited the Department of Energy (DOE) National Nuclear Security Administration (DOE/NNSA) facilities (see tables 2 and 3).

Foreign intelligence and security services also continued to clandestinely exploit a variety of other commercial collectors. For example, they:

- Continued to clandestinely employ commercial firms in technology collection activities. The large volume of genuine commercial activity serves to mask the activity of front companies and other intermediaries.

- May also be developing techniques for inserting collectors inside US companies to facilitate technology-acquisition efforts.

- On occasion, employed students, professors, scientists, and researchers in the technology collection effort.

Few Changes in Tools Used To Acquire Technology

In the FY 2004 *Annual Report*, we devoted considerable attention to detailing the major techniques used to target cleared defense contractors. Although those techniques vary during long periods of time—for example, with the advent of the Internet—there is little indication of sharp deviation from year to year. As a result, in this report for FY 2005, we provide only a brief summary of recent developments along with data for comparison purposes (see table 4).

Given that a significant portion of technology theft took place through commercial channels, it is not surprising that the cheapest, easiest, and least risky methods were the most heavily employed. As in previous years, **direct requests** were the most often used methods to acquire sensitive US technologies in FY 2005, far outnumbering any other approach, according to Defense Security Service (DSS), Air Force Office of Special Investigations (AFOSI), and Army Counterintelligence Center (ACIC) data. For the most part, these were requests for classified, sensitive, or export-controlled information that were not sought or encouraged by cleared contractors. Also included in this category were efforts by foreign entities to purchase US components or technologies.

Table 3
Requests for Visits to US Military Facilities and Department of Defense Industries[a]

FY 2004				FY 2005			
Country	Total Military and Industry	Military Facilities	DoD Industry	Country	Total Military and Industry	Military Facilities	DoD Industry
Germany	**2,389**	1,847	542	Germany	**2,896**	1399	1497
China	**72**	72	0	China	**97**	96	1
Taiwan	**286**	246	36	Taiwan	**2,585**	647	1,938
Colombia	**64**	64	0	Colombia	**2,546**	2,546	0
Japan	**1,076**	953	123	Japan	**2,284**	2,120	164
India	**68**	65	3	India	**485**	457	28
Israel	**1,83**	1,086	197	Israel	**1,419**	896	523
Egypt	**146**	122	24	Egypt	**1,346**	1,146	200
France	**649**	552	97	France	**823**	633	190
Russia	**19**	19	0	Russia	**114**	111	3
All Countries	**14,276**	5,954	1,158	All Countries	**22,916**	11,548	4,690

[a]CIFA Cornerstone data.

Note: Recorded in the foreign visitors database. A single request may have multiple visitors.

In some cases, a single would-be foreign buyer was observed sending multiple requests to a variety of US companies, probably in search of a seller willing to ignore export-licensing requirements. Since most requests were made using e-mail or telephone solicitation, search costs were virtually zero.

The more costly **exploitation of relationships** was a much less frequently used method of operation in FY 2005. This technique involved foreign firms forming ventures with US firms in the hope of placing collectors in proximity to sensitive technologies or else establishing foreign research facilities and software development companies outside the United States to work on commercial projects related to protected programs. AFOSI data showed a sharp decline in the use of this technique in FY 2005, while DSS data showed the figure constant but at only 5 percent of all suspicious incidents.

In the **solicitation of marketing services**, foreign entities offered their technical services to US research

Table 4
Methods of Operation—Comparing ACIC, AFOSI, and DSS Data

(Percent share of total)

DSS	FY 2005	FY 2004	AFOSI	FY 2005	FY 2004	ACIC	FY 2005
Direct request [a]	68	68	Direct request [a]	53	66	Direct request [a]	69
Exploitation of relationships	5	5	Joint ventures	9	15		
Solicitation of marketing services	10	13	Solicitation and seeking employment [b]	13	6	Solicitation of business or services	2
Foreign visits to United States and targeting at conventions, expos, and seminars	10	8	Foreign visitors and targeting at conferences [c]	26	13	Official visits and targeting at conferences or exhibitions	10
Suspicious Internet activity	5	3				Computer network intrusion, exploitation of unclassified Website	6
Other	3	2				Request to participate in research/scientific exchange	4
						Elicitation through liaison	6
						Unknown	3

[a] The Direct request category used here combines two categories broken out by DSS and AFOSI and three categories broken out by ACIC. Their specificity is based on the amount of detail that the foreign entities ask for in making their requests. For this paper, that specificity was considered unnecessary.

[b] Combines the Solicitation and Seeking employment categories in OSI data to make the data more comparable with DSS.

[c] Combines Foreign visits and Targeting at conventions, and so forth, categories.

facilities or to cleared defense contractors in the hope of gaining access to protected technologies. The FY 2005 AFOSI and DSS data presented a conflicting picture of the trends in the use of this method. AFOSI data showed stepped-up use of the solicitation of marketing services in FY 2005, while DSS data—which looked at all cleared defense contractors—showed the opposite. Although no clear conclusions about this trend can be drawn from the data, the fact that roughly 10 percent of all suspicious incidents for DSS and AFOSI relied on this approach was evidence of its continued viability as a tool for extracting technology.

Two other related approaches that remained in favor by those attempting to attract US technologies in FY 2005 were **exploitation of foreign visits** to the United States and **targeting at conventions and expositions**. The large number of foreign visitors each year from the major collecting nations indicates,

in our view, that these visits continued to yield useful information for collectors. Conventions, expositions, and seminars offered rich collection and targeting opportunities for foreign entities because they directly linked foreign experts with US specialists, programs, and technologies. Furthermore, these venues gave foreign specialists the opportunity to compare and contrast the various technologies and to ask technical questions to fill intelligence gaps. On the basis of DSS and ACIC data, collection at these venues accounted for around 10 percent of all suspicious incidents in FY 2005. Because of the prominence of international air shows in the AFOSI data, this tool accounted for 14 percent of suspicious incidents in FY 2004 and almost twice that share in FY 2005.

The Internet—Coming Into Its Own as a Tool for Technology Collection

The CI Community believes that the Internet will be a tool increasingly relied on to help acquire sensitive US technologies. Threats come from both state and nonstate actors. Of major concern is the fact that the nations best poised to use cybertools to access US technologies are also the countries that traditionally have been the most aggressive collectors in the United States.

No one is certain how much technology and sensitive proprietary information are lost annually to cybertheft. Detection of intrusions is difficult. Moreover, a recent private US survey indicated that, even when intrusions are detected, more than half of the impacted firms do not report the breach for fear of tarnishing their public image. In addition, the Internet has given foreign interests an easy, inexpensive, and anonymous way to spot, assess, and target US firms and individuals who may be willing to ignore or short-circuit export restrictions on sensitive US technologies.

A recent FBI survey provided additional weight to the observation that Internet espionage may be on the rise. According to the study, nearly nine out of 10 US businesses suffered from a computer virus, spyware, or other online attack in 2004 or 2005 despite widespread use of security software. The study concluded that viruses, spyware, computer theft, and other computer-related crimes cost US businesses $67 billion a year, according to an online press report. Detecting the origins of such attacks—even determining for certain whether they originate outside the United States—is difficult, since the probes can be routed through multiple foreign countries. And the real concern for the CI Community is how many such attacks may have gone undetected.

Cyberespionage Crossing International Boundaries

One of the most interesting recent cases of Internet espionage demonstrated the international nature of the problem. In early 2005, a British programmer sold customized copies of his spy software to three Israeli private investigation firms. Those firms, in turn, worked for a number of blue-chip Isreali firms, which allegedly used the software to spy on dozens of their international competitors, including at least one major high-tech firm. The software tempted victims into installing it by posing as a package of confidential documents delivered via e-mail. Once installed, the software recorded every keystroke and collected business documents and e-mails on a victim's personal computer and transmitted information to a server computer registered in London.

We believe that foreign governments, including intelligence services, also increasingly use the Internet as a tool for collecting a wide variety of information, including targeting information on US experts and the technologies with which they deal. There is no question that targeting is taking place but determining the specific source of the attack is difficult (see text box).

All Technologies Targeted

As has been the case in previous years, collectors targeted the entire range of items on the Militarily Critical Technology List (MCTL) in FY 2005 (see table 5). Biomedical technology and weapon effects

Table 5
US Militarily Critical Technologies Targeted in FY 2005[a]

(Percent of total incidents)

DSS Data			AFOSI Data				ACIC Data	
	FY2005	FY2004		FY2005		FY2005		FY2005
Information technology	22	21	Information technology	11	Information systems	15	Information technology	4
							Telecommunications	3
			Information security and information wartare	18			Communications and data links	21
Lasers and optics	11	8					Lasers, optics, supporting technology	10
Aeronautics	10	12	Aeronautics	15	Aeronautics	7	Aeronautics	4
Sensors	9	13	Sensors	6	Sensors and lasers	11	Sensors	5
Armaments and energetic materials	9	10	Armaments and energetic materials	17	Armaments and energetic materials	11	Armaments and energetic materials	16
Electronics	7	11	Electronics	3	Electronics	11		
Space systems	6	3	Space systems	12	Space systems	7		
Marine systems	5	2	Marine systems	2	Marine systems	5		
Materials and processing	4	3	Materials and processing	5	Materials	9	Materials and processing	3
Signature-control technology	4	5					Signature-control technology	3
Chemical technology	3	3					Chemical systems	4
Biological technology	3	2						
Positioning, navigation, and time technology	3	2	Positioning, navigation, and time technology	3	Guidance	6		
Manufacturing and fabrication	2	2	Manufacturing and fabrication	4	Manufacturing	7		
Energy systems	1	2	Energy systems	1	Power systems	3		
Nuclear technology	1	0	Nuclear, chemical sytems, and biotechnology	2	Nuclear, biological, and chemical systems	5		
Directed-energy and kinetic-energy systems	1	0	Directed-energy and kinetic-energy systems	3	Directed-kinetic energy	5		
Weapons effects	0	0						
Biomedical technology	0	1						
Ground systems technology	0	1					Ground systems technology	12
							Defensive protection systems	3
							Imaging and remote sensing	4
							Soldier systems technologies	8

[a]Categories differ because originators either modify or use different versions of the standard militarily critical technologies list.

were only lightly targeted, according to all reporters. Each of the major collecting countries targeted most militarily critical technologies during the year. China, for example, targeted all but the three least targeted categories, according to DSS statistics, while Russia targeted 14 of the 20 categories.

Comparing the DSS, AFOSI, and ACIC data is difficult because the three organizations do not categorize the technologies in the same way. In addition, this is the first year in which ACIC data was reported, making trend analysis problematic. Nevertheless, it is possible to draw a few broad conclusions on the basis of the data. For example, as was the case in FY 2004, the 2005 data shows that IT-related technologies were again the most heavily targeted items on the MCTL, accounting for almost 30 percent of suspicious incidents for all reporters.[10] The other technologies that were heavily targeted in FY 2004—lasers and optics, aeronautics, sensors and armaments, and energetic materials—were again near the top of the collection list in FY 2005 for all of the organizations reporting suspicious incidents.

Both AFOSI and DSS data showed a significant increase in the targeting of space systems technology, a category not shown in ACIC data. The National Reconnaissance Office concurs with those findings and agrees that this trend has been underway for several years and will most likely become more pronounced as a number of state and nonstate actors seek to achieve parity with the United States on space technologies or to gain insight into the vulnerabilities of US space systems. The CI Community believes that more than 30 countries targeted US space-related technology or information, though a small number of core countries accounted for around three-fourths of all known and suspect collection efforts since 1997. China by itself accounted for almost half the attempts.

[10] The DSS data breaks out IT as a separate category. For AFOSI, the IT-related category includes both "Information Technology" and "Information Security and Information Warfare." For the ACIC data, the IT-related category includes, "Information Technology," "Telecommunications," and "Communications and Data Links."

The Road Ahead

The road ahead is a challenging one when it comes to protecting sensitive US technologies from foreign theft. There will be no slackening in demand for state-of-the-art US technology and production know-how. Globalization is shining an increasingly bright light on the potential gains associated with technology acquisition. At the same time, the openness of the US economy to both trade and labor flows continues to make the United States a near ideal location for illicit technology acquisition.

China will continue to absorb vast amounts of US technology, though it is also pushing hard for indigenous development of many advanced technologies. As its civilian and military sectors become more sophisticated, demand for more advanced technology will concomitantly rise. Then too, its access to sensitive US technologies is likely to improve in the years ahead. The number of scientists, engineers, and academics working in the United States from China shows no signs of abating. As the number of US students working in the hard sciences levels off, Chinese experts are likely to make up an even larger share of the US and global technology workforces. It is likely, moreover, that the informal organizations that have been set up in the United States to help Beijing track the access of these experts will be refined in the years ahead, further facilitating the flow of technology abroad.

At the same time, improving economic conditions in China and elsewhere mean that a larger share of experts studying and working overseas probably will return to work in their homelands. When they do, they will take with them their US educations, their accumulated scientific and commercial expertise, and—in some instances—trade secrets and protected technologies as well. Ironically, the United States, which has long benefited from its ability to attract some of the best and brightest minds from around the world, could experience a significant brain drain of its own during the next few years.

The demand for US technology will most likely not level off in the other major targeting countries. If anything, the appetites for technology will increase. On the commercial side, globalization will continue to serve as a driver for technology theft. Current market forces—including the demand for globally integrated manufacturing processes and for shorter production cycles—require that competing firms acquire the latest technologies either through direct purchase or using surreptitious means.

Similarly, the military benefits associated with acquisition of US technology will remain a dominant driver for a number of countries, including both Russia and China. The applications of nanotechnology in the military arena, the continued importance of lasers and sensors and armaments and energetic materials in maintaining military superiority all ensure continued demand for the latest military and dual-use technologies.

Third-country venues may also become increasingly important locations for acquisition of US technology. There is little doubt that Chinese and Russian companies have acquired US technology from third countries in both Asia and elsewhere. As the two countries' military and economic relations improve globally, both will have increased collection opportunities.

At the same time that the forces of globalization prod firms toward legal and illegal technology acquisition, they will also continue to facilitate that acquisition. The shift of US R&D facilities overseas appears to be accelerating as US firms attempt to take advantage of the large, cheap, and increasingly sophisticated foreign engineering and scientific communities. Microsoft will invest $1.7 billion dollars in India during the next four years, according to press reports, making India a major hub of Microsoft's research, product and application development, services, and technical support. Japan and China are likely to be two other major beneficiaries of this flow. Governments in these countries encourage foreign R&D investment by offering a range of preferential policies that include tax rebates, construction loans, access to modern facilities, and other incentives. They also use the lure of their large potential market as leverage to encourage technology transfer and R&D investment from abroad. Protecting technologies in these environments will continue to prove difficult. Although we expect gradual improvements in both security awareness and in the legal infrastructure protecting US patents and copyright in places like China and India, the speed at which technology moves overseas will probably continue to outpace the protections.

Other factors are combining to make it more difficult to protect US technologies:

- Cybertheft appears to be on the rise. As quickly as new protections evolve, fresh vulnerabilities are discovered, leaving firms vulnerable to technology theft. The creation of international supply chains—where foreign firms become the major providers of key software and hardware components—opens the door to even greater possible vulnerabilities.

- Devices that can be used for stealing technology are becoming increasingly commonplace within the workforce and are becoming significantly more powerful. Cell phones with digital photographic capability and Personal Digital Assistants with significant storage capability are available for data collection by those who gain even serendipitous access to corporate trade secrets or sensitive technologies.

Looking further down the road, it seems likely that, as profits continue to drive technology theft, markets will develop to move technology to the highest global bidder. At present, ethnic Chinese and Russian middlemen generally funnel US technologies toward their home countries; the entrepreneurs of the future may work as global merchants. The global linkages are made even more probable as the Internet removes the need for personal interaction in the marketing of goods abroad. In such an environment, nonstate players, including terrorist organizations, might find it even easier than now to acquire sensitive US technology.

Appendix

Examples of Foreign Technology Acquisition Efforts—Listed By Suspected End-User Country

Selected technology acquisition efforts in FY 2005:

- In October 2004, a naturalized US citizen and a Chinese citizen were sentenced to three years probation for false statements in connection with illegally exporting to China 25 low-noise amplifier chips that have applications in the US Hellfire missile. According to the indictment, the defendants falsely labeled the amplifier chips in export documents as "transistors" worth some $20. One of the individuals was a former employee of a major US defense contractor, and the other worked at a US research institute that designed software for military and warfare simulations.

- In November 2004, a New Jersey company was charged with attempted violation of the Iranian embargo in connection with an effort to export oil-burner nozzles to Germany, knowing that the devices would subsequently be illegally diverted to Iran.

- In November 2004, a federal judged fined a US aircraft parts supplier for illegally exporting components for the HAWK missile, the F-4 Phantom fighter jet, and the F-5 Phantom/Tiger fighter jet to China. The conviction was the 11th to result from a 5-year undercover US Immigration and Customs Enforcement investigation that targeted aircraft parts suppliers that sold defense articles over the Internet to foreign buyers without obtaining the required US export licenses or complying with the arms embargoes.

- In December 2004, a US citizen pleaded guilty to conspiracy to violate the Arms Export Control Act after purchasing from US vendors sensitive US military items, including components for HAWK missiles, military radars, and F-4 Phantom fighter jet aircraft for export to Israel. The individual knowingly failed to obtain the required export license. The individual has previously exported items via Israel to Iran. Israeli authorities that cooperated in the investigation do not believe the final destination of the shipments was Israel.

- In early 2005, a Singapore company on multiple occasions shipped US export-controlled items, including GPS components and radiofrequency power meters, to Iran Electronics Industries, according to press.

- In early 2005, the FBI arrested two employees of a US auto parts manufacturer on charges that they leaked trade secrets to a Chinese firm, according to press reporting. The Chinese company, Chongqing Huafa Industry Co., used the information to manufacture metal connecting rods and undercut the US manufacturer's prices.

- In January 2005, a Japanese national pleaded guilty in federal court to conspiracy to violate the Arms Export Control Act after attempting to purchase and illegally export military laser sights for M-16 and M-5 rifles.

- In February 2005, a UK citizen was indicted for violating the US embargo on Iran after allegedly attempting to illegally export an experimental, single-engine aircraft from the United States to Iran via the United Kingdom. The aircraft was intercepted in the United Kingdom. The individual,

who also allegedly exported electrical components from the United States to Iran via Austria on four occasions between 2000 and 2004, was arrested in Warsaw, Poland, by Polish authorities acting on a US arrest warrant.

- In February 2005, a US citizen pleaded guilty to illegally exporting sensitive night-vision lenses to Iran.

- In February 2005, managers of two United Arab Emirates (UAE)–based companies were charged with conspiring to illegally export goods to Iran via the UAE. The indictment alleges that the defendants shipped computer goods from a Texas company to an entity in Iran affiliated with that nation's ballistic missile program. It also alleges that they illegally exported a satellite communication system and other goods to Iran.

- In March 2005, a federal grand jury indicted the sales director of a US company with attempting to illegally export sensitive US technology to Iran in violation of the US embargo. According to the indictment, the individual attempted to export a machine that measures the tensile strength of steel and related software technologies.

- In March 2005, a US company pleaded guilty to exporting digital oscilloscopes to Israel without a license. The items were capable of being utilized in development of weapons of mass destruction and in missile delivery fields.

- In October 2005, an engineer working for a cleared defense contractor attempted to transfer US Navy Quiet Electric Drive (QED) technology to China, according to press reports. The engineer transferred QED information to a compact disk with the assistance of his wife and then delivered the disk to his brother. The brother encrypted the QED information and was arrested at the airport as he prepared to leave the United States for China with the data.


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
E PLURIBUS UNUM
UNITED STATES OF AMERICA


NATIONAL COUNTERINTELLIGENCE EXECUTIVE
UNITED STATES OF AMERICA