

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1998



This report was prepared by the National Counterintelligence Center.

Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 1998	2. REPORT TYPE N/A	3. DATES COVERED -	
4. TITLE AND SUBTITLE Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1998		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Office of the National Counterintelligence Executive (ONCIX) CS5 Room 300 Washington, DC 20505		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited			
13. SUPPLEMENTARY NOTES The original document contains color images.			
14. ABSTRACT			
15. SUBJECT TERMS			
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	
			SAR
			16
			19a. NAME OF RESPONSIBLE PERSON

Table of Contents

Key Findings	1
Background	1
Overview of the Threat	2
Legal Collection Versus Espionage	3
The Cost of Economic Espionage	4
Effects of the Economic Espionage Act	4
Origin of the Threat	6
Targeted Information and Technology	6
Collection Methods	8
Espionage and Other Illegal Collection Methods	9
Legal Collection Methods	9
Appendix - Case Summaries	11
Other Theft of Trade Secrets	13
Footnotes	14

Key Findings

- Despite the adoption of the Economic Espionage Act of 1996, many foreign countries, including some traditional US allies, continue their attempts to acquire US trade secret information and critical technologies for military and commercial application, through both legal and illegal means.
- Updated information, as reported by the US Intelligence Community, reaffirms the findings of the 1997 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage to include the origin of the threat, collection targets, and methods of operation.
- Analysis of updated information indicates that eight countries are most actively targeting US proprietary economic information, trade secrets, and critical technologies. In an effort to more effectively qualify the threat, four of the 12 most active collectors listed in the 1997 Annual Report were taken off the 1998 Priority Country List.
- Collection efforts continue to be driven by military force modernization, economic competition, and commercial modernization using technologies with dual-use applications.
- Clandestine collection efforts continue; however, consistent with traditional espionage operations, a significant majority to foreign intelligence collection is initially conducted through legal and open means and may be a precursor to economic espionage.

Background

The *Intelligence Authorization Act for Fiscal Year 1995*, Section 809(b) requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the third *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, which was released in June 1997.

The Intelligence Authorization Act further specifies three aspects of the threat to US industry to be reported and any trends in that threat to include (1) the number and identity of the foreign governments conducting foreign industrial espionage; (2) the industrial sectors and types of information and technology targeted by such espionage; and (3) the methods used to conduct such espionage.

In coordinating a community-based response to the above requirement, the National Counterintelligence Center (NACIC) requested the assistance of the following 12 agencies:

- Air Force Office of Special Investigations (AFOSI).
- Central Intelligence Agency (CIA).
- Defense Intelligence Agency (DIA).
- Defense Security Service (DSS).
- Department of Commerce.
- US Customs.
- Department of Energy (DOE).
- Department of State.
- Federal Bureau of Investigation (FBI).
- National Security Agency (NSA).
- Naval Criminal Investigative Service (NCIS).
- US Army

Ten of the above agencies responded to the request for information. Of the 10 participating agencies, three had no new information to report. The remaining seven agencies provided incidents and trends relating to the continuing foreign economic collection against the United States.

Overview of the Threat

Strong US capabilities in a wide variety of cutting edge, technical, and scientific fields, and the open nature of the United States continue to make the United States the top target of foreign countries engaged in economic intelligence collection and espionage. Similarly, the development and production of trade secret information is an integral part of US trade, commerce, and business, and the security of trade secrets is essential to maintaining the health and competitiveness of critical segments of the US economy.

For the most part, foreign collectors do not distinguish between military technology, civilian technology, proprietary information, and trade secrets - they simply collect what they find to be of value.

Increasing economic competition has redefined the context for espionage as nations link their national security to their economic security. Intelligence services are expanding from their primary focus on military secrets to include the collection of economic intelligence. The United States is particularly vulnerable to the changing focus of foreign collection since American corporations and research centers rely heavily on communications systems, computer networks, and electronic equipment to process and store information. The espionage threat is particularly troubling when the capabilities and experience of a foreign intelligence service support a US corporation's foreign competitor.

Economic crimes have a serious impact on a wide variety of US industries and businesses and therefore upon the economic well-being of the United States. Foreign governments and major foreign industrial sectors play a prominent role in their nation's business intelligence collection efforts. They actively target US persons, firms, industries, and the US Government to steal advanced critical technologies, trade secrets, proprietary information, and the results of research and development initiatives in support of their nation's commercial priorities and economic security agenda.

There have been progressive changes in three areas of foreign collection efforts targeting US interests:

- *Intelligence activity.* Intelligence collection activity is not limited to intelligence personnel. Increasingly, foreign-sponsored, non-intelligence personnel - to include foreign industry representatives, students, researchers, scientists, and foreign national "insiders" working in US firms - engage in clandestine activity that is harmful to the security and economic well-being of the United States.
- *Intelligence environment.* Significant advances in technology have allowed businesses and financial institutions to become prey of new age of criminals. The intelligence environment now includes the growing importance of maintaining the integrity of the United States' information infrastructure. At the same time, the growing use of computer networks and telecommunications for commerce and the storage and transmittal of sensitive information provides increased opportunities for technical collection.
- *Intelligence methodology.* Many traditional and nontraditional adversaries are technologically sophisticated and have modified their intelligence methodologies to use advanced technologies to collect US trade secrets and proprietary information.

Legal Collection Versus Espionage

There are no agreed-upon definitions of economic or industrial espionage. The US Attorney General defines economic espionage as "*the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies.*" This definition excludes the collection of open and legally available information that constitutes a significant majority of economic collection. Aggressive intelligence collection that is entirely open and legal may harm US industry but is not espionage. However, it can help foreign intelligence service identify information gaps and in some cases may be precursor to economic espionage.

The statute that mandates this report defines industrial espionage as "*industrial espionage conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private US company and aimed at obtaining commercial*

secrets." This definition does not extend to activities of private entities without foreign government involvement, nor does it pertain to lawful efforts to obtain commercially useful information, for example, through the Internet. While some of these legal activities may be a precursor to clandestine collection, it does not constitute industrial espionage. Some countries have long tradition of ties between government and industry; however, often it is not easy to determine what is foreign government - sponsored espionage - a necessary requirement under the Economic Espionage Act (Title 18 U.S.C., Section 1831).

The Cost of Economic Espionage

It is difficult to assess the dollar loss as a result of economic espionage and the theft of trade secrets. The US Intelligence Community has not systematically evaluated the costs. The American Society for Industrial Security (ASIS) conducted an intellectual property loss survey of Fortune 1,000 companies and 300 fastest growing companies. Despite an overall 12-percent response rate, responding companies reported \$44 billion in known and suspected losses over a 17-month period during 1996-97.

⁽¹⁾ The vast majority of these losses were in the suspected category.

Pacific Northwest National Laboratory, under contract by the FBI, has developed a methodology to objectively assess and determine the scope of economic loss resulting from the theft of intellectual property. This Economic Loss Model was first applied to the facts of a case involving the theft of intellectual property from a US corporation by a foreign competitor who, as a result of the theft, captured the market.

⁽²⁾ Using this tool, the misappropriation of intellectual property in this case resulted in over \$600 million in lost sales, the direct loss of 2,600 full-time jobs, and a resulting loss of 9,542 jobs for the economy as a whole over a 14-year time frame.

Analysis also determined that the US trade balance was negatively impacted by \$714 million and lost tax revenues totaled \$129 million. The Economic Loss Model will continue to be used on a case-by-case basis and may be used for court purposes to produce unbiased and independent loss estimates.

Effects of the Economic Espionage Act

Since the enactment of the Economic Espionage Act of 1996, US law enforcement has taken advantage of the changed legal structure to fill many gaps and inadequacies that formerly existed in federal law. Important partnerships have been formed between

members of the US Intelligence Community, the law enforcement community and US industry, allowing for prompt detection and successful investigative efforts.

Five cases have been, or are currently being prosecuted under the Economic Espionage Act. US companies that have been the targets of trade secret theft under the Act include Gillette Company, Pittsburgh Plate Glass (PPG), Bristol Myers Squibb, Avery Dennison Corporation, and Joy Mining Machinery. In each case, a significant economic loss was prevented. To date, four individuals, involved in three cases, have pled guilty to Title 18 United States Code (U.S.C.), Section 1832 - theft of trade secrets.

⁽³⁾ However, no direct foreign government involvement has been proved in any of these cases. The other two cases involve the indictment of foreign national and one foreign business. In addition, an outstanding warrant presently exists for one Taiwan person. Prosecutions are still pending in these cases and investigation continues to fully determine the extent of foreign government involvement.

Each indictment and prosecution is a strong example of close cooperation between the US Federal Government and US industry. In furtherance of this cooperation, the FBI has undertaken a number of initiatives. The FBI's National Security Division sponsored a series of six regional Economic Espionage Conferences. These conferences brought together elements of US industry and Federal Government criminal and intelligence sectors that play a role in economic espionage matters. The FBI's Awareness of National Security Issues and Response Program (ANSIR) is designed to develop a nationwide communication network among corporate security professionals, law enforcement, and others on a variety of national security matters, to include economic espionage. In addition, the FBI is currently working with industry to develop an online system to facilitate the timely sharing of information concerning incident reports, threat profiles, and referrals between industry and the FBI. The FBI has also initiated efforts to include operative language from the Economic Espionage Act into the Federal Acquisition Regulation (FAR). The FAR provides uniform policies and procedures for acquisitions by executive agencies of the Federal Government.

The Department of Defense Counterintelligence Technology Protection Working Group was formed through joint efforts of DoD service CI agencies and the Counterintelligence Directorate, Office of the Secretary of Defense (OSD). The Working Group's purpose is to foster interagency cooperation to identify, coordinate, and facilitate the sharing of counterintelligence information and activities that support technology protection and critical technologies. The forum facilitates the exchange of information on foreign government intentions, collection capabilities, and operations targeting US critical technologies, systems and subsystems. The group has attendees from all DoD elements, OSD, FBI, NSA, National Reconnaissance Office, NACIC, and other US Government agencies.

Origin of the Threat

A number of foreign countries, to include some traditional US allies, continue their collection efforts against the United States. This year, eight countries have been identified as nations most actively involved in the collection of US proprietary economic and industrial information.

⁽⁴⁾ These countries do not reflect the entire picture of targeting against US interests - only the most serious threat.

The 1997 *Annual Report* identified 12 countries, in no ranking order, that were believed to be the most active collectors of US proprietary information and critical technologies. The four countries that have been omitted from this year's list have not ceased their collection efforts entirely but are believed to pose a diminished threat to US interests.

A threat to US economic and industrial interests entails both intent and capability. All countries on this year's Priority Country List have the intent and capability to engage in economic collection and economic espionage. Hostile intent involves a willingness to effectively conduct economic espionage against the United States and the capacity to do so. An effective foreign collection program focuses on technology and information that can be used by a country's indigenous commercial and defense industries. In addition, a close relationship between government and business exists among many of the most active economic collector countries - a factor that helps to establish targeting priorities and promote effective dissemination of information. In addition, to have a sufficient negative effect on US industry, a foreign country must have the capability to exploit stolen technology and a base for profiting from it, such as a large economy, an advanced industrial sector, or a third-country buyer.

Targeted Information and Technology

Foreign collection efforts continue to be driven by military force modernization, economic competition, and commercial modernization using technologies with dual-use applications. Targeting dual-use technology provides foreign collectors with a high return on investment and a low probability that the United States will detect any diversion from its stated end use. A majority of collected information is restricted, sensitive and/or proprietary and its loss is detrimental to US economic interests. A smaller portion of collected information is classified in nature.

According to the DSS, US defense industry reporting of suspicious activity during 1997 revealed that foreign government and commercially sponsored entities continued to target weapon components, developing technologies, and technical information more intensely than complete weapon systems and military equipment. Less developed countries seek older technologies that cost less but still improve their military capabilities. More

developed nations appear to seek more advanced technical information to copy or counter US military systems. A review of reported incidents of suspected targeting against critical technologies in 1997 has reaffirmed that all 18 categories of the DoD's Military Critical Technology List (MCTL) continue to be the subject of foreign interest for military and/or economic exploitation. The majority of MCTL categories are dual-use and include:

- Aeronautics Systems.
- Armaments and Energetic Materials.
- Chemical and Biological Systems.
- Directed and Kinetic Energy Systems.
- Electronics.
- Ground Systems.
- Guidance, Navigation, and Vehicle Control.
- Information Systems.
- Information Warfare.
- Manufacturing and Fabrication.
- Marine Systems.
- Materials.
- Nuclear Systems.
- Power Systems.
- Sensors and Lasers.
- Signature Control.
- Space Systems.
- Weapons Effects and Countermeasures.

Of the 18 technology categories listed on the MCTL, the DSS observed that the top five most sought-after technologies were (in order): Information Systems, Aeronautic Systems, Sensors and Lasers, Electronics, Armaments and Energetic Materials. In the past, DSS has emphasized only the top three sought-after MCTL categories; however, current reporting has changed only slightly from 1996 when sensor and laser technology surpassed aeronautics systems as the secondmost sought-after technology.

Under the five primary technology categories, several more specific areas of foreign interest in 1997 included:

Information Systems:

- Information security systems.
- Software/hardware.
- Transmission systems.
- Modeling and simulation.
- Command, control, communications, computers, and intelligence (C4I).
- Intelligence systems.

Aeronautics Systems:

- Fixed-wing aircraft.
- Gas turbine engines.
- Unmanned aerial vehicles (UAV).
- Heads-up display.
- Aircraft stealth.
- Crew interface.

Sensors and Lasers:

- Focal plane array/infrared.
- Radar.
- Imagery.
- Electro-optic/night-vision devices.
- Acoustic.

Electronics:

- Microelectronics.
- Materials/components.
- Optoelectronics.
- Fabrication equipment.

Armaments and Energetic Materials:

- Advanced artillery munitions.
- Surface-to-air, antiship, and air-to-air missiles.

Collection Methods

There has been no visible change in foreign collection methods. Practitioners of both economic and industrial collection seldom use one method of collection. Instead, they combine a number of collection techniques in a concerted effort that combines legal and illegal, traditional, and more innovative methods. Foreign individuals, businesses, government entities, and intelligence-affiliated personnel conducted collection activity during 1997. These foreign interests were not always government sponsored and demonstrated various levels of suspicious activity.

Consistent with traditional espionage operations, a significant majority of foreign intelligence collection is initially conducted through legal and open means and may be a precursor to economic espionage. Foreign intelligence services and companies rely predominately on HUMINT collection when operating against US targets in the United States and abroad. Foreign collectors most likely avoid technical collection inside the United States because of the legal risks as well as the costs. However, most modern

foreign intelligence and security services are capable of monitoring telephone, facsimile, and computer transmissions within their own country.

Espionage and Other Illegal Collection Methods

Investigations during 1997 indicate that foreign intelligence services and other government-sponsored entities continue to employ traditional clandestine espionage methods to obtain US trade secrets, critical technologies, and even open-source information. These methods include agent recruitment, US volunteers and co-optees, surreptitious entry, theft, and computer intrusions. According to the FBI, there has been a significant increase in its pending computer intrusion cases.

Legal Collection Methods

In addition to traditional espionage and other illegal activities, foreign governments, entities, and agents utilize various legal collection methods to target US economic and proprietary information that may be open source, proprietary, restricted, or even classified. As such, these methods do not necessarily involve illicit or illegal activity. Some of these legal activities may be a precursor to clandestine or illegal collection; however, they do not of themselves constitute evidence of illegal activity. Legal collection methods can include joint ventures, foreign students, scientific exchanges, Internet access, unsolicited requests for information, cultural targeting, mergers and acquisitions, and visits to US facilities.

US defense industry reporting of suspicious activity confirms that throughout 1997, a number of methods were used to collect defense-related information and technologies. Despite the legitimate nature of these collection practices, they may be an important element in a broader, directed intelligence-collection effort. The following collection methods were associated with potential collection efforts in 1997:

- Unsolicited requests for information.
- Exploitation of foreign US visits.
- Exploitation of joint ventures and research.
- Targeting visitors at international conventions, seminars, and exhibits.
- Acquisition of US technology and/or US companies.
- Solicitation and marketing of services.
- Foreign employees in a cleared facility.
- Targeting former US company employees.

According to US defense industry reporting to the DSS, the following five collection methods (in order) were most frequently associated with foreign activity in 1997.

Unsolicited Requests.

Since DSS began keeping statistics in 1995, reporting of unsolicited foreign requests for information has tripled. The requests have originated via e-mail, telephone, facsimile, and mail, and have come from foreign companies, individuals, government officials, and organizations. The use of the Internet has become the vehicle of choice for unsolicited requests as it provides an international, low cost, and anonymous medium to contact cleared contractor employees. In 1997, DSS saw a resurgence in the reporting of unsolicited requests for information by restricted countries.⁽⁵⁾

Visits to US Facilities.

Visitors continued to request information beyond the scope of approved discussions, broker appointments at additional companies or subsidiaries on short notice, and photograph sensitive production lines. Also reported with more frequency were the collection efforts by visiting foreign personnel involved in multinational training efforts. These visitors requested restricted and/or controlled technologies from their US counterparts.

According to a 1997 General Accounting Office report, thousands of scientists, researchers, and officials from Russia and China have gained access to the three US nuclear laboratories without security background checks. The report cited DOE labs - Lawrence Livermore, Los Alamos, and Sandia - for lax security. Some of the individuals allowed access to labs were later shown to have suspected foreign intelligence connections. The report focused on visits from 1994 - 1996 by citizens of 22 countries on DOE's "sensitive" country list.

⁽⁶⁾ A total of 5,472 visitors from those 22 countries came to DOE labs. Only 892 visitors, or 16 percent, were given background checks. Visitors from these sensitive countries gained access to areas where work can include technologies under government-export restriction, unclassified but sensitive information, and valuable equipment. Although DOE agreed with the report's recommendations and is taking extensive steps to improve security, the Department challenged the notion that background checks ensure airtight security.

Joint Ventures and Research.

As with foreign national visits, joint efforts place foreign personnel in proximity to US personnel and afford potential access to S&T programs and information. A number of reports involved cleared US personnel being targeted while engaged in joint ventures overseas. There are further indicators that front companies may be using this method of operation as well.

International Conventions, Seminars, and Exhibits.

During such events, US participants reported possible telephone monitoring and hotel room intrusions. In addition, US technical experts have received invitations to share their knowledge in international forums. While many of these requests are benign, others are an effort to press US experts for restricted, proprietary, and even classified information.

Solicitation and Marketing of Services.

Consistent with past reporting, foreign individuals with technical backgrounds offered their services to cleared commercial and government research facilities, academic institutions, and defense companies. A new trend in 1997 involved foreign nationals who fabricated past work histories in an attempt to gain employment with cleared companies in unclassified positions. In addition, foreign software manufacturers solicited products to cleared US companies that had been embedded with spawned processes and multithreaded tasks.

Appendix - Case Summaries

Economic Espionage Act 1996
(Title 18 U.S.C., 1832)

Daniel and Patrick Worthing

Patrick Worthing and his brother Daniel were arrested by the FBI on 7 December 1996, after agreeing to sell Pittsburgh Plate Glass Industries (PPG) information for \$1,000 to an FBI Special Agent posing as a representative of Owen-Corning. The FBI received information from PPG that an individual was attempting to sell company trade secrets to representatives of Owens-Corning Corporation, a primary PPG competitor. Both subjects were charged under Title 18 U.S.C., Section 1832 (Theft of Trade Secrets). On 18 April 1997, because of his minimal involvement, Daniel Worthing was sentenced to six months of home confinement, five years probation, and 100 hours of community service. In June 1997, Patrick Worthing, who pled guilty to the charges against him, was sentenced to 15 months in jail and three years probation.

Hsu Kai-Lo and Chester H. Ho

On 14 June 1997, Hsu Kai-Lo and Chester H. Ho (naturalized US citizens) were arrested by the FBI for attempting to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb (BMS) Company. Hsu and Ho were employees of the Yuen Foong Paper Manufacturing Company of Taiwan. On 19 July 1997, Hsu, Ho, and Jessica Chou (a Taiwan citizen who was actively involved in the attempted theft) were indicted on 11 counts. Two of the 11 counts were violations of Title 18 U.S.C., Section 1832 (Theft of Trade Secrets). Chou remains in Taiwan. Taiwan has publicly stated that it will not help the FBI bring Chou to justice in the United States. This case is in the pretrial stages. The US Department of Justice (DOJ) has appealed a trial judge's ruling on a key part of the Economic Espionage Act (Title 18 U.S.C., Section 1835) regarding protective orders for trade secrets.

This case represents an attempted theft of valuable trade secrets that could have had significant impact on the US economic position in the worldwide pharmaceutical marketplace. If the Taiwan firm - Yuen Foong Paper Company - had obtained the synthetic Taxol formula, BMS would have lost approximately \$200 million a year in revenue from the world market. Over the 10-year period this translates to a potential loss of \$2 billion.

Pin Yen Yang, Hwei Chen Yang, and Four Pillars Company

On 5 September 1997, Pin Yen Yang and his daughter Hwei Chen Yang (a.k.a. Sally Yang) were arrested on several charges, including Title 18 U.S.C., Section 1832 (Theft of Trade Secrets). Also charged is Four Pillars Company, which has offices in Taiwan and is a registered agent in El Campo, Texas. It is alleged that Four Pillars Company, Pin Yang (Chairman of Four Pillars), Hwei Chen Yang, and Dr. Ten Hong Lee were involved in a conspiracy to illegally transfer sensitive, valuable trade secrets and other proprietary information from the Avery Dennison Corporation, Pasadena, California, to Four Pillars in Taiwan. ⁽⁷⁾

Dr. Lee, a Taiwan native and US citizen, had been an Avery Dennison employee since 1986 at the company's Concord, Ohio, facility. Dr. Lee allegedly received between \$150,000 and \$160,000 from Four Pillars/Pin Yen Yang for his involvement in the illegal transfer of Avery Dennison's proprietary manufacturing information and research data over a period of approximately eight years. On 1 October 1997, a Federal Grand Jury returned a 21-count indictment charging Four Pillars, Pin Yen Yang, and Sally Yang with attempted theft of trade secrets, mail fraud, wire fraud, money laundering, and receipt of stolen property. They are awaiting trial. On 1 October 1997, Dr. Lee pled guilty to one count of wire fraud in exchange for his full cooperation in the US Government's case against the accused. Economic losses to Avery Dennison are estimated at \$50-60 million.

Steven Louis Davis

On 23 January 1998, Steven Louis Davis pled guilty to federal charges that he stole and disclosed trade secrets concerning a new shaving system developed by the Gillette Company. Davis was employed by Wright Industries, a subcontractor of Gillette Company, which had been hired to assist in the development of the new shaving system. In February and March 1997, Davis made disclosures of technical drawings to Gillette's competitors Warner-Lambert Co., Bic, and American Safety Razor Co. The disclosures were made by facsimile and electronic mail. Although the FBI is aware that Davis reached out to one foreign-owned company (Bic), it is unclear if he was successful in disseminating trade secrets overseas. Davis was arrested on 3 October 1997 and was indicted on counts of Title 18, U.S.C., Section 1343 (Wire Fraud) and Title 18 U.S.C., Section 1832 (Theft of Trade Secrets). On 17 April 1998, Davis was sentenced to two years and three months in federal prison.

John Fulton

This investigation was based on information received from Joy Mining Machinery, a global coal mining company that manufactures and repairs technical components for longwall shearers (equipment that mechanically shears coal from the face of an underground coal wall). John Fulton approached a Joy employee in an attempt to purchase schematics for part of the longwall shearer system. Fulton, a former Joy employee, was currently operating United Mining Cable, a Joy competitor. The Joy employee became a cooperating witness in the case.

The cooperating witness made consensually monitored conversations in which Fulton offered to pay any amount of money for information pertaining to the chock interface unit of the longwall shearer. On 21 November 1997, Fulton paid the cooperating witness \$1,500 for blueprints and a technical binder both of which were Joy proprietary items. Fulton was arrested by the FBI after the exchange and was charged with unlawfully attempting to obtain trade secrets (Title 18 U.S.C., Section 1832).

On 14 April 1998, Fulton pled guilty to one count of theft of trade secrets. He will be sentenced in September 1998.

Other Theft of Trade Secrets

Harold Worden

Harold Worden, a 28-year employee of Eastman Kodak Corporation, established his own consulting firm upon retirement. Worden subsequently hired many former Kodak employees and stole a considerable amount of Kodak trade secret and proprietary information that he later attempted to sell to Kodak rivals including corporations in the PRC. Worden pled guilty to one felony count of Title 18 U.S.C., Section 2314 (Interstate Transportation of Stolen Property). The *Economic Espionage Act of 1996* was not yet signed into law. Worden was sentenced to one-year imprisonment, three months of home confinement with a monitoring bracelet, three years of supervised probation, and a \$30,000 fine.

John Hebel

This investigation involved unauthorized intrusion into a voice-mail system by a disgruntled former employee. The victim was Standard Duplicating Machines Corporation (Standard), whose main competitor was the US affiliate, Duplo Manufacturing Corporation of Japan (Duplo). John Hebel was employed by Standard as a field sales manager from 1990 to 1992 when he was terminated. Hebel was subsequently hired by Duplo. Through an unsolicited phone call from a customer, Standard discovered that while employed at Duplo, Hebel accessed Standard's electronic phone messaging system and used the information in Duplo's benefit to compete against Standard. On 6 November 1996, Hebel was charged with one count of violating Title 18 U.S.C., Section 1343 (Wire Fraud). On 14 March 1997, Hebel was sentenced to two years

probation. In addition, a civil suit was brought against Duplo by Standard with a final settlement closed to \$1 million.

Footnotes

(1) It must be noted that this figure represents both domestic industrial theft and foreign economic espionage. In fact, only a small percentage of the ASIS reported dollar loss is a result of foreign competitors, foreign intelligence services, or foreign government-sponsored entities.

(2) Pacific Northwest National Laboratory conducted their analysis independent of US company auditors.

(3) Daniel and Patrick Worthing attempted to sell Pittsburgh Plate Glass information to an FBI undercover agent posing as a representative of Owens-Corning. Steven Davis stole and disclosed Gillette Company trade secrets to several Gillette competitors. John Fulton attempted to purchase proprietary, technical information from a cooperating witness employed at Joy Mining Machinery. All four have pled guilty to theft of trade secrets. See appendix for further case details.

(4) Participating CI agencies provided NACIC with compilations of incidents and trends that appeared to involve the targeting of US economic and industrial information during the past year. NACIC, as coordinator, compiled a master list of countries assessed to be most aggressively collecting against US interests. Because of each CI agency's differing mission, investigative responsibilities, and reporting criteria, one agency's list of foreign collectors could differ from that of another. NACIC's analytic effort in compiling a master list sought to ensure the integrity of submitted data and consistency with the assessment criteria.

(5) Restricted countries are those that normally do not do business with the United States or have embargoes placed on them.

(6) DOE's Sensitive Country List includes Algeria, Armenia, Azerbaijan, Belarus, China, Cuba, Georgia, India, Iran, Iraq, Israel, Kazakhstan, Kyrgyzstan, Libya, Moldova, Pakistan, Russia, Syria, Taiwan, Turkmenistan, Ukraine, and Uzbekistan.

(7) Avery Dennison Corporation is one of the largest manufacturers of adhesive products with more than 16,000 employees worldwide.