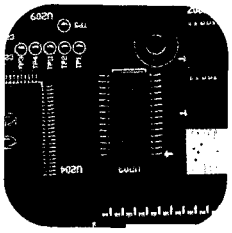
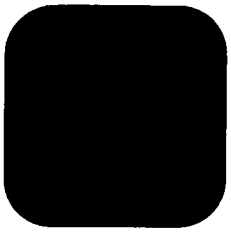


(U) Economic Espionage

"Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor. . . the companies are training the armies and the unemployed are the casualties."
BERNARD ESAMBERT

(U) Economic espionage has always been a factor in relations between competitor nations. For example, in 1811 an American merchant, Francis Cabot Lowell, toured Scotland and England, ostensibly for "reasons of health," and in the process either memorized or purloined enough information concerning British textile mills to return to Boston and build a copy of the Cartwright loom. That particular tightly guarded device had revolutionized British textile production, and it subsequently helped Lowell build a complex of mills that propelled the U.S. into its own industrial revolution.[72]

(U) As the 21st Century begins, the lines of espionage are becoming less and less clearly defined. Because nations are now linking their national security with economic security, the spy of today may not be after the composition of a new warhead, because that is no longer a lucrative market. He may instead be collecting the scientific and technological data that goes into making a computer chip for a high-tech automobile, or the formula of a new cancer drug. In the words of Bernard Esambert, President of France's Pasteur Institute, "Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor...the companies are training the armies and the unemployed are the casualties."[73]

(U) Economic espionage often is not targeted at the "crown jewels" of U.S. technological supremacy. Instead, much of the sought-after information and technology is dated military-related or infrastructure-supportive material that is no longer classi-

fied but has both military and civilian applications. Although unclassified, information of interest usually is subject to control through government regulations.[74]

(U) Costs of Economic Espionage

(U) There has been a growing recognition of the cost of economic espionage. For example, in a 1999 American Society for Industrial Security survey of 1,000 U.S. companies, there were 579 reported losses of proprietary information. Loss of intellectual property totaled $45 billion. By 2001, this figure had risen to an estimated $59 billion. The average company responding reported 2.45 incidents, with the average loss per incident at over $500,000. Most of the incidents took place in high technology or service companies, with reported losses of intellectual property up sharply in 2001. Manufacturers reported fewer incidents—a total of 96—but suffered an average loss of nearly $50 million per incident.[75] According to a 1998 report to Congress on espionage, the actual figure may go as high as $300 billion.[76] The U.S. Chamber of Commerce estimates that losses today continue at roughly $2 billion a month.[77] Most U.S. companies do not have effective mechanisms for safeguarding their proprietary information, nor do they have consistent and effective mechanisms for determining the value of such information.

(U) These figures look less abstract if one applies what is known as the "economic loss model," developed by the Pacific Northwest National Laboratory. This model, applied to a single FBI case of economic espionage showed these results:

- (U) The foreign competitor captured the market
- (U) The U.S. business lost $600 million in sales
- (U) 2,600 full-time were jobs lost
- (U) 9,542 jobs were lost to the U.S. economy as a whole over 14 years
- (U) U.S. trade balance was negatively impacted by (U) $714 million
- (U) Lost tax revenues amounted to $129 million[78]

(U) Emerging Policy

(U) Although economic espionage has always been a part of the commercial landscape, it is only recently that it has been identified as a national problem at which U.S. intelligence resources should be deployed. This policy shift has taken place because over the past 40 years the U.S. has undergone a gradual paradigm shift concerning the general intelligence threat to the country. Prior to 1980, for example, the FBI defined the intelligence threat to the United States in terms of "the presence of hostile

intelligence services and their diplomatic establishments in the United States." A country was deemed to be "hostile" if it met certain classified national-security criteria.[79]

(U) All this changed in 1981, however, when the French government provided U.S. authorities information from a Soviet source code-named "FAREWELL." In reality, FAREWELL was Vladimir Vetrov, a KGB intelligence officer with a senior analytical post in Directorate T, which was responsible for collecting strategic, military, and industrial technology from the West. Vetrov eventually provided the French with more than 3,000 documents detailing Soviet operations, which were more successful and much larger in scope than anyone had suspected.[80] Vetrov's reporting provided important documentation of the following:

Vetrov eventually provided the French with more than 3,000 documents detailing Soviet operations, which were more successful and much larger in scope than anyone had suspected.

- (U) The State Committee on Science and Technology determined what information must be collected and developed tasking for Line X, the operational unit which carried out the bulk of the collection objectives. Line X, however, was not the only entity to receive tasking from this committee. The GRU, the Soviet Academy of Sciences, and the State Committee for External Relations were assigned this collection mission, as well.[81]

- (U) It was not intelligence operatives trained to act like scientists who carried out the collection objectives; rather, it was the task of actual scientists who had been trained as collectors to gather the information. This meant that actual scientists could evaluate and decide on the spot if the information they had access to bore any relevance to the collection objectives with which they were tasked, and also if the information was worth the collection effort.[82]

- (U) The U.S. foreign policy of engagement with the Soviet Union provided broad access for these collectors and opened many new avenues for exploitation, few of which escaped Soviet intelligence. Beginning in 1972, delegations of Soviet specialists arrived in the U.S. in droves to visit companies and laboratories around the country.[83] Further, the Soviet Union was quickly acquiring information for about 1% the cost of what the West spent in developing it over many years.[84]

(U) Vetrov's reporting later was confirmed and amplified by Vasili Mitrokhin, a former KGB officer who, over more than a decade, hand-copied and archived a wealth of information from Soviet intelligence files. According to Mitrokhin, during the mid-1970s, the KGB made unprecedented use of the Soviet scientific community in intelligence operations. For example, the KGB's Directorate T succeeded in developing approximately 90 agent-recruiters, 900 agents, and 350 trusted contacts among the ranks of Soviet scientists. Of these, 77 agents and 44 trusted contacts reported on Western high technology. The intelligence role of the Soviet scientists was to talent-spot Western scientists in areas of intelligence interest, approach them on a personal or institutional level for cooperation, and collect information from them.[85]

(U) The intelligence treasure trove from FAREWELL was a factor in the FBI's 1985 shift in its view of the intelligence threat to the United States away from intelligence-service presence to a definition that focused on activities directed by intelligence services against the U.S., regardless of where those activities occurred or what country initiated them.[86]

(U) In the early 1990s, the winding down of the Cold War caused the FBI to again reassess the overall intelligence threat to the U.S. This time, the FBI developed a strategy that focused on the targets of intelligence activities, such as proprietary technology, data, and employees.[87] This shift took place at about the same time that the extensive direct involvement of France's intelligence services in economic espionage against the U.S. became public knowledge.

(U) In October 1996, the Economic Espionage and Protection of Proprietary Economic Information Act was signed. The new law had two primary elements not previously covered by U.S. law.

- (U) First, it allowed U.S. national intelligence resources to be used on more foreign intelligence organization activities, and not only when they targeted classified government information and programs. In particular, the Economic Espionage Act allowed U.S. agencies to investigate cases where a foreign intelligence service, applying traditional methodologies, mounted an intelligence attack against a U.S. company to gather proprietary information to support the commercial interests of a foreign company.

- (U) Second, the law extended the definition of "goods, wares or merchandise" protected by Federal anti-theft statutes to include the "proprietary economic information" of a company. This permitted Federal investigation and prosecution in the event that the information was used in interstate commerce.

(U) The Outsider Threat

(U) Most organizations conceptualize the main threat to their operations security as coming from outside the organization. In the realm of economic espionage, the main "outsider" threats come from company-to-company attacks launched by economic competitors, attempts to purloin critical intelligence through duping unwitting employees of the organization, and even through the direct involvement of foreign intelligence services.

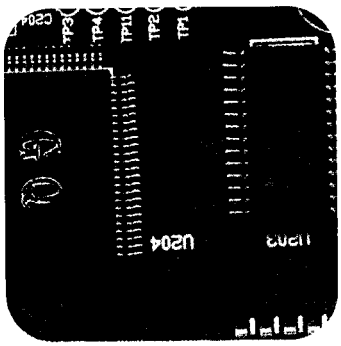
(U) Foreign or Domestic Competitors

(U) Competitor companies have been responsible for many instances of economic espionage against their U.S. counterparts. A frequent scenario is one in which an employee leaves his company and goes to work for the competitor, taking proprietary information with him. The following is a representative sample of competitor-company economic espionage against a variety of U.S. technologies:

(U) *Automotive Glass Manufacturing Process*

(U) In late 1973, John Akfirat, a research engineer in the Glass Division of Ford Motor Company was discovered to be in negotiation with a Portuguese automotive glass manufacturer in competition with Ford. Akfirat was to be paid $250,000 for delivering the proprietary information, and he would also be hired by the company at a good salary. Ford had licensed the revolutionary glassmaking process from its British inventor for $1.25 million and substantial royalties. The Portuguese competitor could have used the critical information to capture the European auto glass market from Ford, which calculated its potential loss at $2.79 million. Akfirat was convicted and received 60 days in jail and a $10,000 fine. Shortly after his release from jail in 1974, Akfirat got a job at another glass company, and he and his new boss began to travel frequently to Romania to talk with officials there about the proprietary glass manufacturing process. By 1978, he and his boss had exported specialized glass-manufacturing equipment to Romania, in the process making false statements in the export documents required. In 1983, Akfirat was again arrested for ongoing fraud against Ford. He admitted to meeting with Romanian officials as part of a scheme for constructing a plant there which would use the process Akfirat had learned from Ford and to providing the Romanians with computer hardware and software. This time Akfirat was convicted and sentenced to four months of community service, two years probation, and a $1,000 fine. His boss was not prosecuted, but the company did have to pay monetary damages both to Ford and the British company that invented the manufacturing process.[88]

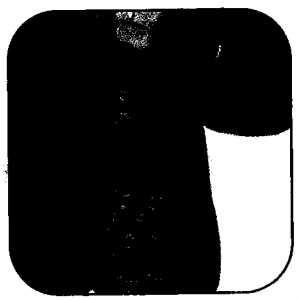
(U) *Computer Chip Designs*



(U) In 1979, PRC nationals opened a computer chip manufacturing plant in California named Chipex, Inc. Chipex supposedly was a joint venture with a Hong Kong firm, but in actuality the Hong Kong company was itself a subsidiary of a PRC electronics company. The ostensible purpose of the plant was to manufacture chips from designs provided by U.S. companies, while at the same time training PRC nationals on how to use the manufacturing equipment. In reality, however, Chipex also was illegally copying its customers' proprietary designs and sending them to its parent corporation in China. U.S. Customs Service and the Commerce Department raided Chipex in 1982 and shut it down. The subsequent investigation determined that the PRC's San Francisco Consulate provided support and guidance to Chipex's operations, and several PRC students were used in duplicating the proprietary U.S. designs.[89]

(U) *Microwave Tube Design Drawings*

(U) In 1989, Ssangyong, a large South Korean conglomerate, purchased a U.S. microwave technology company, M Square Microtec, Inc. M Square was participating in a microwave technology joint venture with Litton Systems, which held U.S. defense contracts. Litton soon discovered that M Square had stolen some of its proprietary radar and microwave tube design drawings and passed them on to Ssangyong. Litton notified the FBI about the situation, but the intangible nature of its loss precluded criminal investigation. Litton Systems pursued the matter through civil litigation, and in the process, uncovered Ssangyong documents detailing its strategy to undercut Litton's prices, which had to reflect research costs. In 1995, Litton Systems was awarded a summary judgment of $65 million against Ssangyong.[90]



(U) *Organic Fertilizer*

(U) In late 1994, three representatives of a South Korean firm visiting the laboratory of Rubicon/Pacific Trading Group to view a sales presentation of its new organic fertilizer were observed dipping their ties in a solution of the product. The three visitors then pulled out cameras and fanned out in different directions, photographing everything in sight. Rubicon's new fertilizer was more productive, environmentally friendlier, and cheaper than its main alternative and had a potentially huge market, especially in Asia. Rubicon later had problems trying to interest South Korean farmers' associations in using the fertilizer.[91]

(U) *Cancer Drugs*

(U) In June 1997, Hsu Kai-lo and Chester H. Ho (naturalized U.S. 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 Company. Hsu and Ho were employees of

Adhesives Formulas

(U) An employee of FIELCO Industries received a phone call from a Mexican national offering the employee up to $10,000 for information on the formulas for his company's state-of-the-art adhesives. The employee notified his supervisors of the approach, and they called in U.S. law enforcement authorities. The caller subsequently mailed the employee $2,000 in cash and asked to be faxed some of the information. The facsimile number provided matched that of one of FIELCO's customer companies in Mexico. When the caller flew to the U.S. to pay the employee the balance of the bribe money, he was arrested. FIELCO estimated that the formula information would have cost the company $1 million annually in sales.[241]

the Yuen Foong Paper Manufacturing Company of Taiwan. Jessica Chou, a Taiwan citizen actively involved in the attempted theft, was also indicted. Taiwan publicly stated that it would not help the U.S. extradite Chou for trial in the U.S. If the Taiwan firm had obtained the synthetic Taxol formula, Bristol-Myers Squibb would have lost approximately $200 million a year in revenue from the world market.[92]

(U) *Coal Mining Technology*

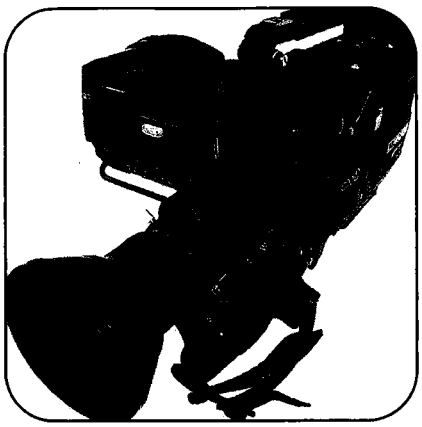
(U) In mid-1997, John Fulton, a former employee of Joy Mining Machinery, Inc., and at the time the operator of a Joy competitor, United Mining Cable, approached a Joy employee in an attempt to purchase schematics for part of the coal-shearing system used by Joy. Joy Mining Machinery is a global coal mining company that manufactures and repairs technical components of equipment that mechanically shears coal from the face of an underground coal wall. The Joy employee became a cooperating witness in the case and participated in consensually monitored conversations. Fulton offered to pay any amount of money for information pertaining to the chock interface unit of the coal-shearing technology. In 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.[93]

(U) Through Unwitting Accomplices

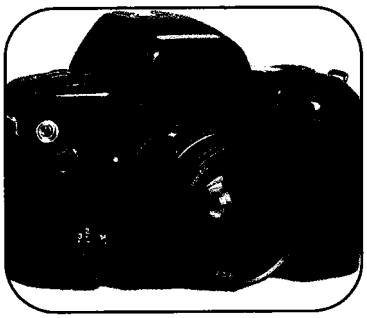
(U) Sometimes collectors of economic intelligence try to brazen their way into opportunities in which they can collect critical information. Another ploy is to create situations in which the employees of a targeted facility can be induced to give their proprietary information away, in the mistaken belief that the individuals requesting the information have been properly authorized to receive it. Examples of this type include the following:

- (U) A Japanese collector called the president of a major U.S. biotechnology firm, knowing the president was out of town. The Japanese businessman assured the secretary he spoke to that the company president had already given his approval for her to provide several sheets of data on a technical compound.

The secretary refused to provide the information, and her boss later confirmed that he had not given authorization for anyone to receive the data. [94]



- (U) A Japanese TV crew requested and obtained permission to visit a U.S. firm to film a documentary on cancer research. While filming the video, the crew asked many questions, collected information, and sought access to sensitive areas. Before long it became apparent the visitors had much more technical understanding of the industry than would be expected from a professional television crew. Company officials had the visitors escorted from the facility.[95]



- (U) Japanese scientific visitors to one facility wandered into restricted areas and began taking pictures. When confronted, they apologized profusely and blamed their lack of English language skills for not being able to read the posted signs denying them access. At later social gatherings, however, the Japanese scientists were observed conversing with their counterparts in fluent English.[96]

- (U) French engineers, with the support of the French Embassy in Washington, misrepresented themselves as customers of Dow Corning and sought to obtain information regarding the coating used in the stealth aircraft to evade radar detection.[97]

- (U) A business education professor from India who taught a night class at a Maryland college required each of her students to write a term paper on the company where they worked. One student advised the FBI that her paper had been returned by the professor three times, with the professor on each occasion asking for more detailed information. Eventually, the professor's interest in the student's company extended to directing her to provide sensitive, possibly proprietary data.[98]

(U) From Foreign Intelligence Services

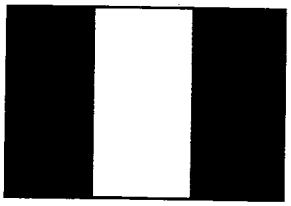
(U) Intelligence services are, by definition, specialists in the techniques of collecting "secret" information. When they apply their specialized skills against individual commercial targets, they can provide a potent combination of resources and special skills. It has been extensively documented that France has used this approach against the U.S. for many years.

(U) First, the memoirs of Count Alexandre de Marenches, director of France's external intelligence service from 1970-1981, recount that an agent in the U.S. Government provided information about an upcoming currency devaluation that allowed the Bank of France to reap enormous profits in international currency markets. De Marenches's successor, Pierre Marion, admitted in news interviews that he initiated an economic espionage program against U.S. businesses to keep France internationally competitive. Marion mentioned that IBM, Corning Glass, and Texas Instruments had been specific targets of the French intelligence service. Marion explained that, "It would not be normal for us to spy on the United States in political matters or military matters, but in the economic and technical spheres we are competitors; we are not allies." Marion was succeeded by Charles Silberzahn, who also confirmed publicly that economic espionage had replaced political intelligence as a priority for France, and that theft of information about large corporations was a long-term French government policy. In a 1996 interview on a German television program, Silberzahn observed that in France "the state is not just responsible for lawmaking, it is in business as well."[99]

"It would not be normal for us to spy on the United States in political matters or military matters, but in the economic and technical spheres we are competitors; we are not allies."

Pierre Marion, Former Director of France's Eternal Intelligence Service

(U) Examples of economic espionage operations against the U.S. directed and controlled by foreign intelligence services or other foreign government entities include the following:



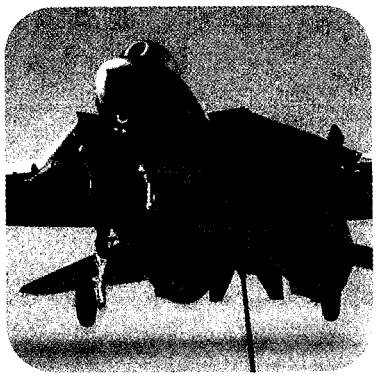
- (U) Beginning in 1969, the French intelligence service recruited several French nationals in the France-based offices of IBM, Corning Glass, and Texas Instruments. These agents were tasked to collect information on marketing plans, product specifications, and travel itineraries of executives. French intelligence passed the information along to competing companies in France, including Machines Bull. In 1993, when Bull sued Texas Instruments over patent infringement on a computer chip, Texas Instruments discovered that Bull had originally stolen the design from them through an agent who worked for Texas Instruments for 13 years. After two years of litigation, the two companies settled out of court, on undisclosed terms.[100]

- (U) In 1973, ranking scientists and managers of the Soviet computer and electronics industries obtained a visa for the specific purpose of visiting the Uranus Liquid Crystal Watch Company of Minneola, Long Island. This was definitely a very odd choice

Well-Dressed Trashmen

(U) In May 1991, a private security guard in an exclusive residential area of Houston, Texas, noticed two well-dressed men tossing into their van plastic bags of garbage taken from behind the home of an executive for a U.S. defense contractor. The guard notified the FBI, and investigation later identified the van as belonging to the French consul general in Houston. When FBI agents quizzed the French diplomat about his actions, he claimed that he had been looking for bags of grass clippings to fill in a hole dug in his back yard.[242]

of destination for such a delegation, but three days before the delegation's arrival the Soviets requested an expansion of the itinerary to include nearly all leading U.S. computer and semiconductor firms. The reason for the abrupt change in plans was that the Soviets had studied U.S. regulations and procedures and discovered that, if they made a last-minute change of itinerary, the U.S. Defense Department would not have time to object. This allowed the delegation to observe the latest critical technology.



- (U) In 1985, a U.S. aerospace company bidding to sell jet fighter aircraft to India lost a $2 billion contract to a French aerospace company after the French intelligence service became aware of the U.S. company's best and final offer during negotiations and then passed the information along to a French competitor.

- (U) In the spring of 1986, Recon Optical was in the midst of a $45 million contract with Israel to manufacture advanced airborne photographic surveillance equipment. The terms of the contract allowed three Israeli Air Force officers to be stationed at Recon to monitor progress of the project. After a lengthy dispute with Israel over the financial terms of the contract, Recon decided to close work down and asked the three Israeli officers to leave. The officers attempted to leave the premises with boxes of Recon data labeled as their personal belongings. These were confiscated, and examination of their contents revealed that the

officers had for months been sending proprietary Recon information to a competitor company back in Israel. Recon sued the government of Israel, and an arbitrator awarded the American company $3 million in damages.[101]

(U) The Insider Threat

(U) Most people visualize espionage as a secret agent managing to sneak into a facility, defeat its guards and locks, and then spirit away secret documents or equipment. In reality, the most common threat comes from an employee inside the facility who approaches an outsider to sell his organization's secrets. Three surveys conducted between 1988 and 1994 by the American Society for Industrial Security determined that approximately 75 percent of all reported incidents of economic espionage were attributable to employees or former employees with access to sensitive information. The figure for losses attributable to vendors, consultants, joint venture partners, and subcontractors was at that time just 15 percent, but by 1999 a similar survey identified on-site contractor employees and original equipment manufacturers as the main source of concern for U.S. companies.[102]

Seventy-five percent of all reported incidents of economic espionage were attributable to employees or former employees with access to sensitive information.

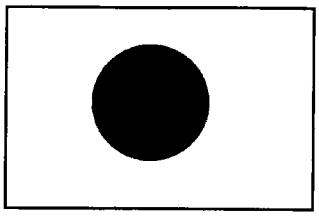
(U) In cases involving national security, between 1975 and 2000 the United States charged 140 individuals with espionage. Of these, 80 were U.S. citizens with a security clearance, 35 were U.S. citizens or resident aliens with no security clearance, and the remaining 25 were foreign nationals. By a more than three-to-one margin, the cases involved one person acting without co-conspirators. In about two thirds of the cases, the arrests were made only after there had been damage to U.S. national security.[103]

(U) Moles and espionage entrepreneurs are two types of insiders who can wreak havoc through economic espionage. These cases are particularly difficult for OPSEC managers, since an insider with access to his organization's critical information would also know the critical needs of competitors or adversaries. Moreover, he is likely to be familiar with his organization's security systems and safeguards and be in a good position to defeat or circumvent them.

(U) Moles

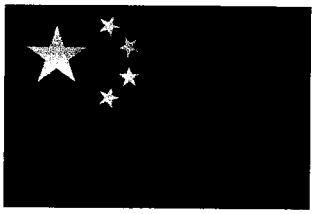
(U) A "mole" is an employee sent by an outside entity to work for a competitor or recruited after he already is inside the targeted organization. The mole tunnels his way into a position of access to the organization's critical information, and then passes the data back to his outside clients.

- (U) From 1977 to 1986, agents operating from the Japanese consulate in San Francisco obtained vast amounts of information from a middle-level researcher at Fairchild Semiconductors,



Inc. The employee provided them computer disks containing as many as 160,000 pages of confidential research results and corporate plans. The Fairchild mole was never conclusively identified and was apparently able to leave Fairchild with enough extra money to retire soon thereafter. Fairchild was so weakened by the mole's efforts that, in 1986, it required government assistance to fight off a Fujitsu Corporation bid to purchase 80 percent of the company.[104]

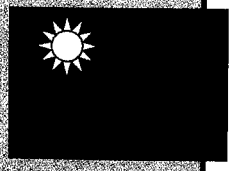
- (U) In 1981, a French software engineer was convicted on two counts of felony theft involving the intellectual property of his employer, Renaissance Software Systems, Inc. At the time, he was receiving a stipend from the French government for reporting on his work at Renaissance.[105]



- (U) In 1994, Yao Mindong, a PRC national in a five-month engineer training program at a Motorola Company facility in Albuquerque, New Mexico, made a sudden, unannounced departure from the workplace several days early. Just before his departure, Yao visited the plant's computer facility and printed out some materials to take back with him. Motorola officials had no way of determining what data Yao printed out, but they were concerned because it had taken the company 50 man-years to develop the project Yao had been working on. Motorola valued its potential loss from the incident at $5 million.[106]

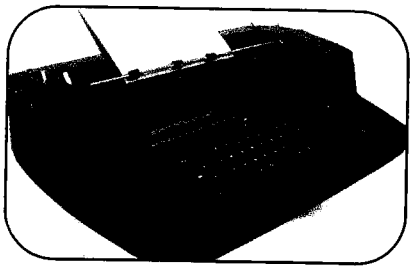
Avery-Dennison Case

(U) In September 1997, Dr. Ten Hong Lee, Pin Yen Yang, and his daughter Sally Hwei Chen Yang were arrested for theft of trade secrets from the Avery-Dennison Corporation, Pasadena, California. Four Pillars Enterprises, Ltd, which has offices in Texas and Taiwan, was also charged. Lee, a Taiwan native and U.S. citizen, had been an Avery-Dennison employee since 1986 at the company's Concord, Ohio, facility. Over a period of approximately eight years, he received between $150,000 and $160,000 for providing Four Pillars and the Yangs with secrets about adhesives used in products such as self-stick postage stamps, name labels, diaper tape and battery labels. Both Yangs were fined, and Pin Yen Yang was also sentenced to home confinement. Four Pillars was assessed the maximum statutory fine, $5 million. The estimated damage to Avery-Dennison was $50-60 million.[243]



(U) Espionage Entrepreneurs

(U) An "espionage entrepreneur" is an employee who obtains access to critical information and then tries to use the information as an inducement to a competitor company to hire him for a better job or simply tries to sell his secrets outright to one or more buyers. They are most commonly discovered when an approach is reported by one of the potential buyers of the critical information. Here are some examples of critical intelligence compromised by information entrepreneurs:



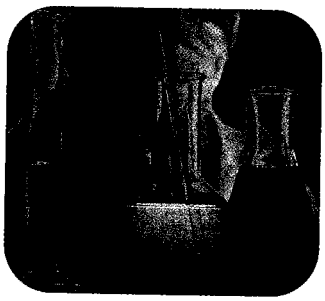
(U) *Electronic Typewriter Trade Secrets*

(U) In the summer of 1979, Orion Briel, a disgruntled employee at Exxon's QYX division, resigned his job and sent a letter to a vice president of IBM's Office Products Division, offering to steal proprietary Exxon documents, including designs for new products, research and development plans, and marketing strategies. QYX at the time had captured nearly 25 percent of the computerized typewriter market, a field once dominated by IBM. Briel asked for $100,000. IBM reported the approach to the FBI. The potential loss to Exxon was $500 million.[107]

(U) *Telecommunications Computer Applications*

(U) In 1986, Ronald Hoffman, a U.S. scientist working on space technology computer research for Science Applications International Corporation (SAIC) attempted to persuade SAIC to sell information to Japan developed for the Strategic Defense Initiative but with commercial telecommunications and weather-satellite applications. Japan was years behind the U.S. in this area, but SAIC declined to pursue the matter, since the information was both classified and restricted from export. Hoffman thereupon formed his own research and export company, Plume Technology, as a sideline activity and contacted various Japanese firms to offer his services. Over the next four years, he sold SAIC technology to four Japanese companies. Ronald Hoffman was arrested in 1990 and convicted of selling classified information. No legal action was taken against his Japanese customers, who subsequently gained a significant competitive advantage in the space industry.[108]

(U) *Genetically Engineered Pharmaceuticals*



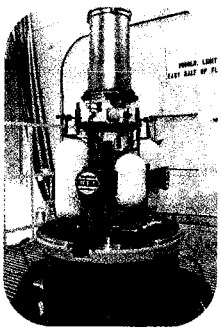
(U) In early 1990, a former research scientist with Merck and Company and Schering-Plough Company and an accomplice who ran a research laboratory let it be known that they had some extremely valuable pharmaceutical trade secrets to sell. Their offer was to provide details of the manufacturing process for two genetically engineered pharmaceuticals: Ivermectin, a leading antiparasitic drug with worldwide livestock usage, and Interferon, which is used as an anticancer and antiviral drug. Their offer attracted the attention of the FBI, and later that year both were arrested immediately after selling their critical information on one of the drug

fermentation processes to an undercover agent, who paid the two $1.5 million in cash and bonds. The companies involved advised that over $750 million had been spent developing the two drugs. Since there was no Economic Espionage Act at the time, the case was prosecuted under applicable fraud statutes.[109]

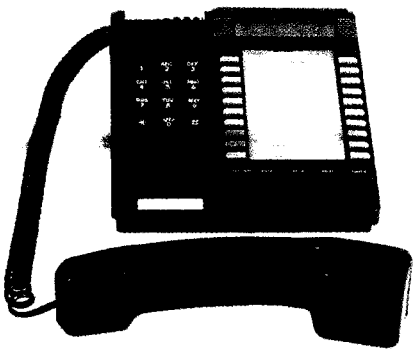
(U) *Tomahawk Missile Bid Information*

(U) In 1993, the U.S. Navy decided to have a sole vendor, either Hughes Aircraft or McDonnell-Douglas Missile Systems Company, manufacture its Tomahawk cruise missiles; and this caused an intense competition between the two companies. In November of that year, a former Hughes employee approached a senior manager at McDonnell-Douglas and offered to sell the specifics of the Hughes bid and pricing information for $70,000. The manager alerted the FBI. A month later, the espionage entrepreneur and the current Hughes employee who was the source of his information were arrested by the FBI and the Naval Criminal Investigative Service after they agreed to sell the proprietary information to undercover agents.[110]

(U) *Copier Technology*



(U) In late 1996, Harold Worden, a 28-year employee of Eastman Kodak Corporation, retired and established his own consulting firm. Worden thereupon 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 China. Worden's illegal activities were documented in an investigation using a double-agent operation, and he was arrested and pled guilty. Worden was sentenced to one-year imprisonment and a $30,000 fine.[111]



(U) *Voice-Mail Intelligence*

(U) In November 1996, John Hebel was arrested and charged with wire fraud. Hebel had been employed by Standard Duplicating Machines Corporation as a field sales manager from 1990 to 1992, when he was terminated. Hebel subsequently found employment at the U.S. affiliate of Duplo Manufacturing Corporation of Japan. Through an unsolicited phone call from a customer, Standard discovered that, while employed at Duplo, Hebel had accessed Standard's electronic phone messaging system and used the information to Duplo's benefit to compete against Standard. In March 1997, Hebel was sentenced to two years' probation. In addition, a civil suit was brought against Duplo by Standard,

with a final settlement close to $1 million.[112]

(U) *Glass Technology*

(U) In December 1996, Patrick Worthing and his brother, Daniel, were arrested by the FBI, after agreeing to sell PPG Industries (Pittsburgh Plate Glass) information for $1,000 to an FBI special agent posing as a representative of Owens-Corning, a primary PPG competitor. Patrick Worthing had misappropriated diskettes, blueprints and other types of confidential research information from PPG, which he tried to sell to Owens-Corning. However, Owens-Corning alerted PPG, who subsequently informed the FBI that an individual was attempting to sell company trade secrets to representatives of Owens-Corning Corporation.[113]

(U) *Razor Blade Design Information*

(U) In February and March 1997, Steven Louis Davis stole and disclosed trade secrets concerning a new shaving system developed by the Gillette Company. Davis was a process control engineer employed by a subcontractor of Gillette Company. Using several pseudonyms, Davis sent facsimiles and electronic mail containing confidential technical drawings to Gillette's competitors Warner-Lambert Co., Bic, and American Safety Razor Co. Davis, in soliciting further interest, claimed that he had 600 megabytes of Gillette's product drawings, equipment drawings, and assembly drawings relating to Gillette's next generation of razor systems. Davis was arrested in October 1997. Subsequent FBI investigation was not able to establish to what extent he had disseminated trade secrets overseas. After pleading guilty, he was sentenced to two years and three months in Federal prison and $1.2 million in restitution.[114]

(U) *Computer source code*

(U) In a recent case, Cadence Design Systems, Inc., was attempting to recover $1.2 billion from former employees alleged to have stolen intellectual property to build up the product line of a competitor. Evidence collected during the execution of a search warrant included electronic footprints which show that one employee E-mailed six megabytes of computer source code to a private account before quitting Cadence and joining the rival company. Before long, the competitor company began marketing a product similar to Cadence's, and theirs contained the same source code, including the same typographical errors as in the Cadence product. In the words of a senior vice president of Cadence, "That source code is the central nervous system for every other product and service we put out. It took hundreds and hundreds of engineering hours and years to develop." A criminal

case is pending against the rival company.[115]

(U) Developing a Countermeasures Strategy

(U) One of the problems that U.S. companies who have been the victims of economic espionage face is that they often feel constrained to keep their losses secret. In fact, the General Accounting Office-the investigative arm of the U.S. Congress-had to abandon its plan to study the extent and impact of foreign government spying on U.S. companies when it became clear that firms had little desire to discuss the matter.

(U) U.S. firms have been reluctant to speak out about their experiences with economic espionage for a number of practical reasons. For one thing, if a firm makes its loss known, it may suffer public embarrassment and become known as a company that can't keep its secrets. Some companies that have reported successful attacks on their critical information have seen their stock prices drop, their employee morale plummet, and their corporate partners pull out of deals for fear their own critical information may be compromised. Also, when the economic espionage has come from a foreign country, the U.S. company that names names runs the additional risk of losing future contracts there. Finally, criminal and civil penalties imposed on individuals and organizations engaged in economic espionage are small compared to the potentially huge gains possible.

(U) The case of Recon Optical is an instructive example of some of the problems that U.S. companies can face, even after they have "successfully" fended off an economic espionage operation. Although Recon was awarded a reported $3 million by an arbitration panel, the figure did not cover the company's legal expenses in waging a four-year lawsuit against Israel. The Israeli contract had been the company's largest, and its management was tied down in the legal process. The action depleted all the company's cash, and when it tried to bid for contracts in two huge new Pentagon reconnaissance programs, its prices had to reflect its low cash reserves and thus could be beat by competitors. The company's sales dropped 40 percent, and it was forced to lay off 800 of its 1,100-member workforce. Only the emergency military needs of the Gulf War kept Recon Optical from going under completely.[116]

Recon's sales dropped 40 percent, and it was forced to lay off 800 of its 1,100-member workforce.

(U) Economic Espionage Indicators

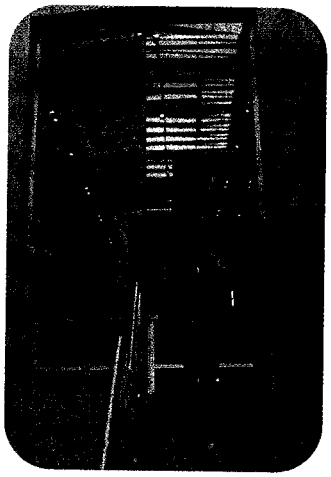
(U) Given the realities that U.S. organizations face, many may try to handle OPSEC requirements without outside assistance. The following is a partial list and discussion of indicators that a given company may be under economic espionage attack.

(U) Outsider Threat Indicators

(U) *Unsolicited requests for information*

(U) Such requests frequently involve faxing, mailing, E-mailing, or phoning to indi-

viduals rather than corporate marketing departments. The requests may involve surveys or questionnaires and are frequently sent over the Internet. Marketing surveys can elicit sensitive technological and business information. With this method, it is important to consider who is the end user of the information and who is completing the survey. Increasing use of the Internet provides a method of bypassing organizational security systems for collection purposes. Internet access to a company's bulletin board, homepage, and employees provides a collector many avenues to broaden collection efforts. Additional indicators include communications in which the recipient has never met the sender; the requestor identifies himself as a consultant or student; the requestor insinuates the company he works for is "classified;" and the requester advises the recipient not to worry about security concerns.[117]



(U) *Inappropriate Conduct During Visit*

(U) Visitors are an obvious vector for loss of critical information. One economic espionage indicator is an attempt to arrange an alternative mechanism such as proposing a commercial visit shortly after an official visit has been denied by the host organization. Another situation involves foreign visitors accompanied by a diplomat who attempts to conceal the visitors' identities or official positions during the visit. Yet another is the existence of hidden agendas: the visitors arrive to discuss program "X" but do everything to discuss and meet with personnel who work with program "Y." Last-minute and unannounced persons being added to the visiting party is also a reason for heightened concern. The questions asked by the visitors also may be an indicator of an economic espionage interest on their part, especially if they ask them during a briefing outside the scope of the approved visit, hoping to get a courteous or spontaneous response.[118]

(U) *Suspicious Work Offers*

(U) Sometimes foreign scientists and engineers will offer their services to research facilities, academic institutions, and defense contractors. This may be an attempt to place a foreign national inside the facility as a "mole" to collect on a desired technology. There are further reasons for concern if the foreign applicant has a scientific background in a specialty for which his country has been identified as having a collection requirement, if the technology the prospective employee wants to work with is proprietary or export-controlled, if the applicant's salary and expenses are to be paid by a foreign government or a corporation associated with the government, or if the prospective employee offers to work under a knowledgeable individual for a lengthy time for free. Another tactic is for one side to overstaff a joint-venture operation, using its excess employees to gather loose information from their business partners.[119]

(U) *Invitations to International Exhibitions, Conventions, and Seminars*

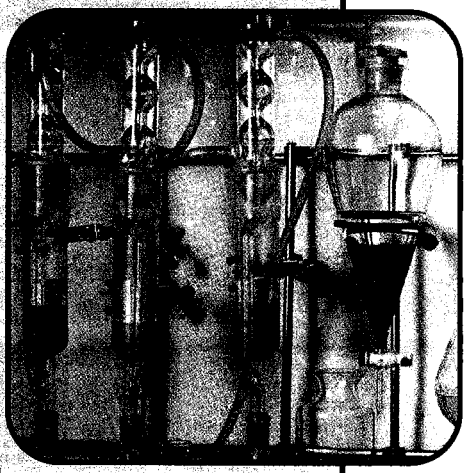
(U) It is not necessary for critical information collectors to devise ways to get into a

(U//FOUO) Here are the steps a security consultant recently used to compromise the current research projects of a large chemicals company.

1. (U//FOUO) The consultant used the Internet and newspaper files to familiarize himself with news reports of current projects and with past incidents of "industrial espionage" against the company. He wanted to find out what had worked and what had not.

2. (U//FOUO) Hired as a temporary employee in a low-level position, the insider went to a nearby restaurant that had a fishbowl with business cards in it for a weekly free lunch drawing and fished out a company card. He had a local print shop duplicate the card in his name, with the title, "Supervisor of Information Security."

3. (U//FOUO) Noting that the company used a passcard for some computer systems, the employee forged his supervisor's name to a memo ordering a special access card for himself in his assumed information-security role.



4. (U//FOUO) The insider called on a senior researcher on one of the projects he had read about in the newspaper and gave her his new business card. He interviewed the researcher about what information in the project could be considered sensitive and asked for suggestions on how to improve security. The researcher suggested he contact the team leader, which he did, mentioning the referral from the researcher. The team leader identified the portion of the project considered most valuable and gave the insider the names of all the people working on the project, so he could interview them about data-storage security. Using the same technique, the insider interviewed several other employees until he found one who admitted he had not backed up his key files. Under the guise of "walking through" the backup process with the employee, the insider had the employee mark his files as "shared." Later he downloaded the files from his own office computer.

5. (U//FOUO) Looking for a critical document on the project, the insider accessed an unprotected computer file with research meeting minutes on it. One document identified the location of the document and the User ID and password needed to open it. Using the same password, the insider accessed several other summary documents with details of two other critical projects the company was working on.

(U//FOUO) Had he chosen to, the security consultant could have left at the end of the day and not returned. He had compromised three projects of potential multi-million dollar value to the company's competitors.[245]

U.S. facility if they can induce the facility to send its knowledgeable staff members to locations and situations where there is little or no protection for them. This is a particular OPSEC problem for organizations in which foreign travel is highly prized by staff members. If the invitation is to send representatives for a specific topic, whom the organization selects to attend may itself identify future targets for foreign collectors and economic competitors. Indicators that economic espionage may be involved in such situations are: if the organizing country or organization has tried unsuccessfully to visit the invited facility, if the travel or accommodations are offered expense-paid, if a summary of the conference speaking topic is requested far in advance of the foreign meeting, if attendees wear false or incomplete conference name tags, or if there is excessive or suspicious filming or photography at the conference.[120]

(U) *Proposals for Joint Ventures or Joint Research Projects*

(U) It is not necessary for a foreign collector or an economic competitor to steal critical intelligence from an organization if the organization can be persuaded to give the information away. Proposals for mutually profitable cooperative enterprises are one means of collecting critical information that would otherwise be difficult to obtain. Requests for unrestricted access to the organization's local area network or its physical plant may be indicators of economic espionage. Sometimes companies are induced to provide large amounts of technical data as part of the bidding process, only to have the contract canceled, or the proposed technology sharing agreements may be one-sided. Other indicators of the impending loss of critical information are the venture partner's sending more people than necessary to staff the project, or the venture partner's staff members singling out individual employees to provide information outside the scope of the agreement.[121]

(U) Insider Threat Indicators

(U) *Hiring Ex-Employees*

(U) An ex-employee who now works for a competitor can be a good source of critical company intelligence for the competitor, not just because of the intellectual property the ex-employee may already know, but also because of the ex-employee's ability to find out recent information. In this regard, it can be critical to keep track of which former employees now work for competitor companies and which former employees still maintain social or professional contact with current staff members. Of particular concern is the employee who has a job history of alternating working between one company and one of its competitors.[122]

(U) *Foreign Ethnic Targeting of Employees*

(U//FOUO) Sometimes, foreign countries and their commercial entities attempt to

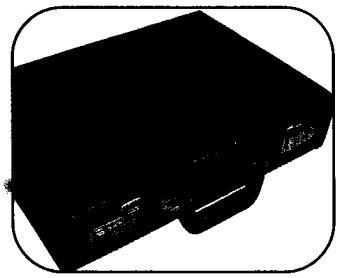
exploit cultural ties with company employees to exploit them for collection of critical information. Sometimes, an employee will receive unsolicited mailings or greeting cards from foreign embassy personnel. In other cases, an employee may be invited to travel to the country of his ancestry to give a lecture or receive an award. This may be an especially ominous development if the travel is also to be expense-paid. Alternatively, foreign delegations may arrive without an interpreter and ask the company to provide an employee who speaks their language. The visitors may then single out the employee for extra socializing and may invite him to pay a reciprocal visit to their country.[123]

(U) *A "Too-Good" Employee*

(U) Sometimes individual characteristics that are most valued in an employee may, taken together, give reason to fear possible economic espionage from him. These indicators include extra initiative, such as volunteering for special work or project assignments offering different or higher access; repeatedly volunteering to work nights or weekends, especially when few other employees are present; refusing promotion to a higher-paying job with less access to proprietary information; etc.

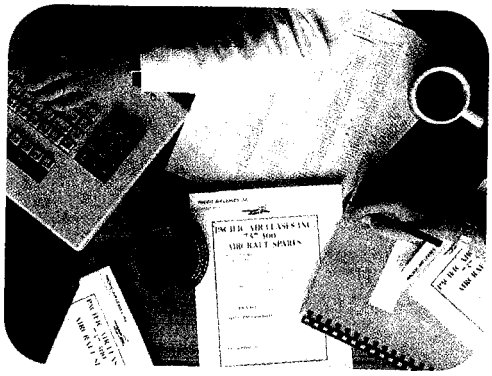
(U) Work Assignments and Access Indicators

- (U) Any attempt to obtain classified, sensitive, or trade secret information without a genuine "need to know" that information
- (U) Unauthorized removal of classified, sensitive, or trade secret information from a work area
- (U) Placing classified, sensitive, or trade secret information in desks or briefcases for no apparent reason



- (U) Unusual use of, requests for, classified, sensitive, or trade secret information
- (U) Using a copier machine in other offices to reproduce classified, sensitive, or trade secret information when a copier machine is available in that person's office
- (U) Repeated or unusual or unnecessary overtime
- (U) Sudden deterioration in work performance or a change in attitude of a person with access to classified, sensitive, or trade secret information
- (U) Borrowing or making notes of classified, sensitive, or trade secret information not associated with assigned work
- (U) Attempting to obtain witness signatures on a classified or sensitive

document destruction form where the destruction was not actually observed by the witness



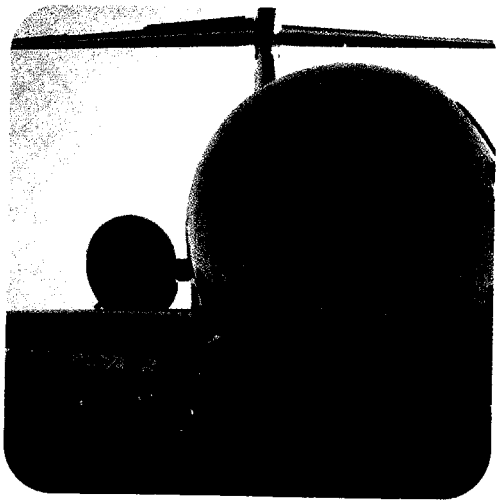
- (U) Bringing a camera or recording device into an area where classified, sensitive, or trade secret information is used, especially new cellular phones with digital imaging and transmission capability
- (U) Excessive unauthorized use of a classified or sensitive computer system at work.[131]

(U) Financial Indicators

- (U) Sudden purchase of high-value items such as real estate, automobiles or vacations for which no logical source of income exists
- (U) Flashing of expensive purchases or large sums of cash, especially after returning from leave
- (U) Extensive or regular gambling losses or financial indebtedness
- (U) Sudden repayment of large loans
- (U) Purchase of expensive miniature cameras and related equipment
- (U) Purchase of quality international or ham radio-band communications equipment by other than a known hobbyist[124]

(U) Leave and Travel Indicators

- (U) Short domestic or overseas trips for no apparent purpose
- (U) Recurring or quick weekend trips not associated with recreation or family
- (U) Trips that cost out of proportion to the short time spent at the locations
- (U) Upon return, the traveler has a hard time describing the location visited
- (U) Personal or family travel to current or former Communist countries



- (U) Inquiries about passport or visa requirements for current or former Communist countries
- (U) Travel on current or former Communist Bloc aircraft or cruise liners
- (U) Mention of problems with border-crossing, visa or police in former or current Communist countries[125]

(U) Social and Family Indicators

- (U) Relatives or friends live in or maintain connections to current or former Communist countries
- (U) Relatives or friends visit from current or former Communist countries
- (U) Relatives or friends in current or former Communist countries request assistance
- (U) Use of illegal drugs[126]