Economic Espionage: Security Missions Redefined

Edwin Fraumann, Federal Bureau of Investigation

In the post Cold War era increasing international economic competition has redefined the context for espionage as nations link their national security to their economic security. Proprietary economic information meant to be secret is stolen with losses estimated anywhere between $24 and 100 billion. In this climate of distrust, intelligence services are expanding from their primary focus on military secrets to collecting economic secrets, i.e., to conducting economic espionage. Since cessation of the Cold War, the most virulent offenders have been former military allies of the United States.

Economic espionage poses a real threat to America's economic future, yet outside of the intelligence community, few know about it. The author attempts to close this information gap by defining economic espionage, and by discussing the methods used to obtain trade secrets from U.S. corporations. He also provides an overview of legislation used in fighting economic espionage and the impact of the Economic Espionage Act of 1996, which is aimed at strengthening efforts at preventing it.

Opinions expressed in this article are those of the author and do not necessarily represent official positions of the F.B.I.

Introduction

Throughout history, espionage has generally been viewed as an activity conducted by spies to obtain the military secrets of an enemy. Some of the most successful and well-known examples of espionage include England's use of spies to uncover the military information that helped to defeat the Spanish Armada in 1588; the use of spies by the Allies during World War II to defeat the Axis powers; and the Soviet Union's use of spies to steal atomic bomb secrets from their former allies, the United States and Britain.

In the post Cold War era, however, increasing international economic competition has redefined the context for espionage as nations link their national security to their economic security. Spying conducted by intelligence services is expanding from its primary focus on military secrets to collecting economic secrets, i.e., to conducting economic espionage.

The United States is particularly vulnerable to the changing focus of international espionage agencies since so many American corporations and research centers rely heavily on communications systems, computer networks, and electronic equipment to process and to store information. Over 50 countries have covertly tried to obtain advanced technologies from United States industries (U.S. Senate, 1996a). In 1995, the annual cost of economic espionage to corporate America was conservatively estimated to be at least $50 billion. If intellectual property theft and unrestricted technology transfer are included, the estimate rises up to $240 billion (Perry, 1995, 3).

A wide range of federal statutes provide the authority for activities that counter economic espionage. These activities are undertaken by at least nine federal agencies, including the FBI, which has the dominant role. However, given the extent of the problem, it was obvious that existing initiatives had not been effective in preventing the theft of economic secrets. In recognition of the growing threat of economic espionage and the inability of existing legislation to deal with it, the Economic Espionage Act of 1996 (18 U.S.C. secs. 1831-1839) was signed into law on October 11, 1996, creating a new federal crime—the theft of trade secrets.

Although the problem of economic espionage had become extensive and was the subject of debate in Congress, few people outside of those fighting it and those affected by it were aware of its scope and impact.

The Department of Justice now has sweeping authority to prosecute the theft of trade secrets in the United States. The act, intended to crack down on economic espionage by foreign and domestic competitors, makes it illegal to steal a competitor's "proprietary" economic information and imposes stiff new penalties for these thefts. Section 1831 of the act addresses economic espionage provisions and agents of foreign powers. Section 1832 of the act makes it a federal crime for any person to convert a trade secret to his own benefit or the benefit of others knowing that the offense will injure the owner of the trade secret.

Although the problem of economic espionage had become extensive and was the subject of debate in Congress, few people outside of those fighting it and those affected by it were aware of its scope and impact. This article attempts to close this information gap by providing a working definition of economic espionage and trade secrets, describing the methods that are used to obtain trade secrets from American corporations and research centers, and summarizing the technological capabilities of selected countries to conduct economic espionage against the United States. The article also addresses public-sector initiatives in the United States to protect its economic interests.

Economic Espionage: What Are We Talking About?

According to the FBI, "'economic espionage' means foreign-power sponsored or coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons for the purpose of unlawfully obtaining proprietary economic information" (FBI, 1995, 2). In Section 1839 of the Economic Espionage Act of 1996 "trade secret" is defined to mean "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."

Foreign intelligence services that seek out America's trade secrets can damage national and corporate interests much more readily than can traditional "industrial espionage" whereby one company attempts through legal and illegal methods to learn the trade secrets of another. A recent survey of 173 nations found that 57 were actively running operations to obtain proprietary economic information and technologies from U.S. corporations, and that some 100 countries spent a portion of their gross national product on collecting proprietary economic information (Richter, 1995, 8). Ironically, a number of these countries, including Germany, Japan, South Korea, and France, developed their modern intelligence services with assistance from the U.S. intelligence community. Additional resources are also expended by many countries in order to collect nonproprietary information through accessing environments not protected or classified.

Conducting Economic Espionage

Many spy agencies around the world are adapting classic spy techniques from military and political espionage endeavors to conduct economic espionage. Agencies use a number of "intrusive" methods to obtain classified proprietary economic information relating to trade secrets. A country's intelligence service will also, at certain times, use what can be described as "nonintrusive" methods to obtain nonproprietary information. These methods might involve monitoring the marketing surveys of a company or an organization, soliciting disclosures by employees, and researching published materials that can be processed into information useful to spy agencies.

Intrusive Methods

The methods listed below constitute the intrusive methods most widely used to collect proprietary information involving trade secrets.

Electronic Access of Protected Environments

- Eavesdropping through wiretapping, bugging offices, or capturing cellular telephone conversations.
- Penetrating a computer system through hacking into the network, hard drive, or software.

Physical Access of Protected Environments

- Using direct illegal observation and surreptitious photography.
- Using surveillance and reconnaissance.
- Trespassing on a competitor's property.
- Stealing proprietary information contained in drawings and documents or on floppy disks and CD ROMs.

Access to Personnel Working in Protected Environments

- Utilizing the services of a prostitute for blackmail purposes.
- Using a "swallow" (good looking woman) or a "raven" (good looking man) to form a close personal relationship with an employee having knowledge of trade secrets.
- Hiring a competitor's employee who has the specific knowledge desired.
- Bribing a supplier or employee.
- Planting an agent or "mole" on the competitor, whose true identity is hidden and whose true task is to compromise key employees, tap into the computer databases, and intercept all communications with the goal of ferreting out confidential research, technologies, and information.
- Conducting false employment interviews with competitor's employees who have knowledge of trade secrets.

Nonintrusive Methods

The use of nonintrusive methods to gather nonproprietary information from open source environments can also serve to increase economic competitiveness. These methods are not consid-

ered espionage as such. Nevertheless, the processing of data, collecting information, and forming it into intelligence for distribution is a service that thousands of analysts at intelligence agencies perform. Nonintrusive methods can supply data and information that are used to formulate intelligence-based decisions through researching published materials, seeking out disclosures made by employees, obtaining market surveys and reports, and analyzing competitors' products.

Economic Espionage Activities

Unfortunately, and not surprisingly, publicly available information is limited concerning the economic espionage activities of most countries. However, sufficient evidence for a select group of countries provides some insight into how intelligence agencies have adapted to the economic arena.

France

Although the French may view the United States as a political and military ally most of the time, this friendship extends only to those two areas, and certainly not to the areas of technology and economics. France uses its intelligence services to engage in a variety of intrusive methods to conduct economic espionage and to provide intelligence to various French governmental agencies, which in turn determine which French companies should receive it.

Both the Directorate General of the External, which is France's equivalent of the CIA, and the Directorate of Surveillance and Terrorism, its equivalent of the FBI, play a major role in conducting economic espionage. Surveillance and Terrorism monitors personnel and communications inside France, including telephone conversations and faxes, and even began in the early 1970s to bug Air France flights from New York to Paris. It has also been known to conduct "bag" operations in hotels whereby it surreptitiously opens suitcases and uses bribes and prostitutes to compromise employees who can supply information or provide access (Schweizer, 1993).

France prides itself on having one of the world's strictest laws on the abuse of personal data, but its intelligence services are not held accountable to these same personal protection laws. Two special units of the Directorate of General Information, which report to the Ministry of the Interior, gather domestic intelligence for the government, specifically collecting information on foreigners in France and on French employees working for foreign firms. The Directorate General of the External and the Directorate of General Information continually match up information from their databases regarding foreign companies and personnel. When a particular target is identified, individuals are sometimes placed in "deep cover" within a foreign firm without revealing their true allegiance (Schweizer, 1993, 110-111; Madsen, 1993, 423).

Japan

To the Japanese, objectivity and insight can be obtained only when they are based on access to the correct information, without which effective and profitable decisions are not possible. The Japanese word for information, *joho*, means having a purpose and a method (Baumard, 1994, 35). In the United States information is seen more as a commodity. Economic espionage in Japan is very sophisticated and diverse; its mission is to make Japan even more prosperous and competitive.

Prior to World War II, Japan had a very effective military espionage apparatus, which was dismantled when the peace treaty ending the war prohibited the re-establishment of a Japanese intelligence agency. Many Japanese intelligence officers found employment in Japanese trading companies. To this day Japan does not have an intelligence agency to conduct economic espionage, but relies instead on its trade ministries to collect economic information through mostly nonintrusive methods.

During the 1950s the Japanese government began subsidizing the worldwide travel of up to 10,000 Japanese businessmen each year to gather foreign technological information. It has recently been estimated that 80 percent of all Japanese intelligence assets have been directed toward gathering information about the United States and to a lesser degree, Europe (Richter, 1995, 8). Not only is economic espionage performed externally, it is performed internally as well. The domestic Public Security Investigation Agency is charged with conducting "bag job" operations against targeted American business executives.

Much of Japan's economic success is attributable to the coordination of its economic espionage through the Japan External Trade Organization (JETRO), with offices in 59 countries, and the Ministry of International Trade and Industry (MITI). John D. Shea, president of Technology Analysis Group, Incorporated, of San Jose, puts it this way, "It's very similar to the way the CIA is set up.... The Japanese have people gathering data and sending it back to a central clearing operation run by MITI and JETRO"(Schweizer, 1993, 80-84). Intelligence gathering at MITI is conducted by a variety of sections, such as the General Affairs sections of the Secretariat of the International Trade Policy Bureau, which is responsible for foreign trade policies and procedures and works with affected companies when collecting intelligence.

> More than a hundred Japanese companies...paid up to $100,000 a year in 1990 for annual membership in ILPs [industrial liaison programs] that provided members with pre-published papers, ready access to university laboratories, a chance to acquire exclusive rights to patents held by the university, and help in overcoming technological problems in developing their products (Tolchin and Tolchin, 1992, 220).

In the laboratories of such American universities as Stanford for instance, Japanese corporations have endowed six permanent chairs and one visiting professorship, devoted either to business or engineering pursuits. Half of the foreign companies that participate in the Industrial Liaison Program at the Massachusetts Institute of Technology are Japanese, and more than a third of the endowed corporate chairs there are sponsored by Japanese companies. These 19 chairs represent $20 million to MIT (Combs and Moorhead, 1992, 25). This involvement certainly allows for the use of many nonintrusive methods for information collection, while at the same time quite possibly providing access to trade secrets as well.

Although Japan relies primarily on nonintrusive methods, it has used intrusive methods as well. In 1981 Hitachi was offered IBM's secret plans for the new 3381 computer by a computer consultant

on behalf of a former IBM scientist. In 1982 a Hitachi agent was arrested in the act of buying this information. In all there were twelve defendants in the subsequent lawsuit, but the case never even came up for trial. It was settled out of court (Schweizer, 1993).

Germany

The Germans have been very active and quite successful in the field of economic espionage through the utilization of a top secret computer facility outside Frankfurt, which has allowed the Federal Intelligence Service to enter both data networks and databases of companies and governments around the world. This computer espionage operation, code named Project RAHAB, involves the systematic entry into computer databases. It has accessed computer systems throughout the United States and the world, targeting electronics, optics, avionics, chemistry, computers, and telecommunications (Madsen, 1993, 421).

Israel

Economic, scientific, and technological intelligence gathering in Israel is traditionally placed under counterintelligence, the Israeli Defense Force Intelligence Branch or the Israeli Central Institute for Intelligence and Special Duties. These agencies have been successful at obtaining information beneficial to Israeli state-owned industries, particularly for those in aerospace, chemicals, and electronics.

China

The Chinese External Liaison Department uses intrusive methods such as monitoring data communications and computers and actively eavesdrops on digital links within China. The Chinese government often use their visiting students and professors in non-intrusive methods to penetrate American corporate and academic laboratories and report their findings to Chinese authorities.

Russia

The new Russian Federation has divided the once powerful KGB into two separate agencies. The Ministry of Security is now responsible for domestic security and law enforcement while the Foreign Intelligence Service is responsible for gathering foreign intelligence. The National Center for Automated Data Exchanges at the Institute of Automated Systems in Moscow, using intrusive methods, monitors Soviet computer users and foreign data networks and databases to obtain any proprietary information or intellectual property it can. Intrusive methods for conducting economic espionage in protected environments include electronic access, physical access, and gaining access to personnel.

An example of economic espionage carried out via the computer occurred from 1986 to 1989 when a group of contract hackers employed by the KGB accessed countless computer systems and networks from terminals outside the United States. This group of hackers, based in West Germany, was run by a KGB officer based in East Berlin, with the objective of penetrating sensitive computer systems around the world. The hackers were paid both in cash and drugs for information obtained from the U.S. military, from scientific R&D organizations, and from universities. Upon penetrating the computer system at the Lawrence Berkeley Laboratory in California, the group used it as the host to access the Advanced Research Projects Agency Network/Military Network, which in turn allowed the group to penetrate 450 other computers (Madsen, 1993, 417).

South Korea

South Korean methods for pursuing economic espionage include aggressively accessing closed source environments through the use of electronic access, physical access, and access to personnel for obtaining proprietary information. South Korean intelligence agents are extremely active in collecting political, economic, and technological secrets. For its size South Korea possesses one of the world's most successful intelligence organizations. Its National Security Planning Agency boasts of possessing technically proficient agents, enormous financial resources, and well-organized informers who are paid large sums for helping collect proprietary information. Overseas, members of the intelligence service are usually posted to the South Korean embassy as part of the diplomatic staff, but often they are assigned to Korea's industrial conglomerates, such as Hyundi, Samsung, and the Lucky Group (Schweizer, 1993, 186-187).

Economic Espionage Across Countries

Although economic espionage methods differ among countries, in many instances the technological capabilities of a nation's intelligence agency can be categorized based on its level of advancement in electronic eavesdropping and computer intelligence gathering. The following table categorizes levels of sophistication of selected countries based on two criteria: (1) having technological capabilities and (2) having personnel with expertise in conducting electronic eavesdropping and computer intelligence gathering.

Tier 1 countries have the technological and the intelligence abilities to conduct electronic eavesdropping and possess the expertise to use computer intelligence gathering. Tier 2 countries possess first-rate intelligence gathering organizations but lack the resources to utilize sophisticated computers and data intelligence gathering. The intelligence agencies of Tier 3 countries will soon have high technology capabilities.

The Role of Federal Agencies in Protecting U.S. Interests

The FBI has instituted a program called the Awareness of National Security Issues and Response, which allows the bureau to interface with the private sector concerning the issues that arise when attempting to safeguard proprietary information. During fiscal years 1993 and 1994, the FBI briefed nearly a quarter of a million personnel in almost 20,000 companies and also held briefings at academic institutions, laboratories, and state and local governments.

In 1995 over 700 foreign counterintelligence investigations were pending involving economic espionage. This is a dramatic

Table 1
Classification Levels of Countries having Electronic Eavesdropping and Computer Intelligence Gathering:

Tier 1	Tier 2	Tier 3
France	Russia	Iraq
Japan	India	Libya
Germany	Ukraine	
Israel	Columbia	
China	S. Korea	

Source: Madsen, 1993

increase over the 400 cases investigated during 1994. This increase is primarily attributable to recent changes in the FBI's foreign counterintelligence program, resources, and initiatives. It also demonstrates the size of the problem (FBI, 1995).

The FBI is the primary counterintelligence agency in the United States and as such, investigates both foreign intelligence and criminal activities. The establishment of the National Security Threat List in February 1992 focuses the FBI on prohibiting foreign intelligence agencies from stealing critical technologies and proprietary information. Presumptive primacy over economic espionage lies with the FBI, but the state department's Overseas Security Advisory Council, the U.S. Customs Service, and other agencies such as the Defense Intelligence Agency, the Department of Commerce, and the Department of Defense, are also involved in fighting economic espionage (see Table 2).

The Central Intelligence Agency (CIA) provides information to the FBI for use in the Awareness of National Security Issues and Response program, and it briefs U.S. corporate officials concerning foreign intelligence threats. The CIA also plans and implements an array of activities under the auspices of the National Counterintelligence Center's new interagency Awareness Working Group, designed to inform and assist U.S. companies that are actual or potential targets of economic espionage.

The state department's Overseas Security Advisory Council is a joint venture with U.S. business interests. The council interacts with business interests to address overseas security problems of mutual concern, including foreign economic threats.

The U.S. Customs Service is the primary border enforcement agency. It is also responsible for the enforcement of trade sanctions and embargoes against designated countries, strategic trade issues, and protection of intellectual property rights.

Table 2
Involvement of Federal Agencies in Combating Economic Espionage

Agency and Agency responsibilities	
CIA (Central Intelligence Agency)	Selected US persons and companies overseas
DIA (Defense Intelligence Agency)	DoD contractors
DIS (Defense Investigative Service)	DoD contractors
DoD/ASPP (Department of Defense)	DoD Acquisition Systems Protection Program
DoDSI (Department of Defense Security Institute)	Briefings and *Security Awareness Bulletin;* Military Services Contractors working on service R&D programs, special access programs, and military systems and acquisition programs
DOE (Department of Energy)	DOE contractors, US corporations involved in cooperative research and development agreements (CRADA)
FBI (Federal Bureau of Investigation)	All US industry
NACIC (National Counterintelligence Center)	Selected US industry
NASA (National Aeronautics and Space Administration)	NASA contractors
NSA (National Security Agency)	NSA contractors
USDS/DS/OSAC (State Department)	Member companies

Source: Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, July, 1995.

Statutory Protection Against Economic Espionage

Before the Economic Espionage Act of 1996 was instituted to protect U.S. trade secrets, efforts of law enforcement and intelligence agencies to prevent economic espionage were predicated upon a number of existing federal statutes. Table 3 lists the major statutes. However, even with so many acts and statutes addressing so many different types of violations, existing law enforcement efforts failed to protect proprietary information sufficiently. They lacked focus specific enough and punitive action strong enough to seriously counter economic espionage. Also missing was a clear focus on economic espionage involving national security and internal security violations. Existing federal laws were inadequate to protect against new high-tech theft of intellectual property rights.

It was clear that more explicit legislation was needed to give government agencies a clearer purpose and mission for addressing economic espionage and for increasing enforcement and sentencing procedures. The Economic Espionage Act of 1996 now makes the theft of trade secrets a federal criminal offense and empowers federal government agencies to investigate and enforce broad mandates involving criminal activities, forfeiture, civil proceedings, extraterritoriality, construction with other laws, preservation of confidentiality, and law enforcement activities. This new legislation not only authorizes new guidelines, fines, and terms of imprisonment for the violation of trade secrets but also deals with issues of

Table 3
Federal Statutes Relating to Economic Espionage

The Espionage Act of 1917: Meant for use in a military struggle.
The National Security Act of 1947: Established the CIA.
The Interstate Transportation of Stolen Property Act: Intended to thwart the transportation of stolen property across state lines in automobiles.
The Mail Fraud statute: Used if a theft scheme involves the use of the mail.
The Fraud by Wire statute: Requires an intent to defraud as well as the use of wire, radio, or television.
The Copyright Act of 1980: Covers software applications.
The Trade Secrets Act: Penalizes improper disclosure of technologies.
The Computer Fraud and Abuse Act of 1984: Makes it a crime to gain unauthorized access to federal computers
The Computer Fraud and Abuse Act of 1986: Provides penalties for activities in connection with computers and computer access devices.
The Counterintelligence and Security Enhancements Act of 1994: Deals with gathering, transmitting, or delivering defense information to aid a foreign government.

compliance. The act directs the court to take the necessary and appropriate action to preserve the confidentiality of information involved and amends the wiretap statute to authorize the interception of communications in order to protect U.S. trade secrets.

Private Sector Initiatives to Counter Economic Espionage

The United States government is increasing its role in preventing economic espionage. How is corporate America to respond? Even with government's involvement in monitoring national security issues, most organizations do not receive enough guidance and information on what they can do to protect their proprietary information and what constitutes compliance in order to make their proprietary assets into trade secrets as defined by The Economic Espionage Act of 1996.

Organizations may fail to recognize the severity of the problem. As a consequence, they may fail to take the necessary steps to avoid being a victim of economic espionage. On the other hand, management expertise in defending an organization's proprietary assets, and allocating adequate resources to do so can create an environment that focuses on the problem and identifies possible solutions.

The American Society for Industrial Security advocates the creation of a public-private information network that would allow U.S. corporations to share their espionage experiences anonymously, thus allowing for a national dialogue about critical business issues. Such a dialogue is necessary in order for security professionals and government agencies to accurately assess the nation's security issues (Stack, 1995). The FBI's implementation of the Awareness of National Security Issues and Response program is one attempt at addressing the issue of how best to make private industry aware of the wide-reaching implications of the new economic espionage legislation.

Conclusion

Economic espionage is the emerging activity for intelligence agencies around the world. "The resulting security environment presents a new set of threats to our national security, and presents challenges to existing security, intelligence, counterintelligence and law enforcement structures and missions" (U.S. House, 1996). Foreign countries are using their spy services to steal proprietary economic information in the form of trade secrets from U.S. companies, which are primary targets. Not only are intrusive methods used such as eavesdropping, computer hacking, and bribery, so too are nonintrusive methods used such as employing visiting students and professors to seek out information and search out open source environments that might contain trade secrets incorrectly labeled.

With losses in the United States from economic espionage estimated at anywhere from $50 billion to $240 billion, it was obvious that existing laws were not adequate to address the problem. The Economic Espionage Act of 1996 is an attempt by Congress to address the issues surrounding the theft of proprietary secrets through acts of economic espionage, even though the agencies that will participate and the full scope of their jurisdictions and duties in implementing the act have yet to be sorted out.

The FBI initiated the Economic Counterintelligence Program in late 1994 to detect and counteract activities sponsored by foreign powers against U.S. economic interests. The Economic Espionage Act of 1996 resolved many inadequacies of past statutes by specifically proscribing the various acts defined under economic espionage and addressing the national security aspect of this crime. Under the Awareness of National Security and Response program, the FBI has begun acquainting U.S. corporations with the threat of economic espionage. Limiting economic espionage will require not only increased law enforcement, but also cooperation and coordination between various government agencies and the private sector.

It is equally important for corporations and individuals to protect against becoming victims of economic espionage. As computers, electronic mail, faxes, and videoconferencing become more accepted ways of storing and communicating trade secrets, such protection becomes even more critical for preventing economic espionage. Increased international economic competition in this post Cold War era will continue to place foreign intelligence agencies in the position of conducting economic espionage to further their countries' welfare. There are no friends or allies in this international spy game.

◆ ◆ ◆

Edwin Fraumann is a special agent with the Federal Bureau of Investigation and has taught as an adjunct assistant professor in the Public Administration Department at John Jay College of Criminal Justice in New York City. He holds degrees from the University of Michigan and New York University, and has a doctorate in education from Columbia University.

References

Baumard, Phillippe (1994). "From Noticing to Making Sense: Using Intelligence to Develop Strategy." *International Journal of Intelligence and Counterintelligence* 7 (Spring): 29-73.

Combs, Richard E., and John D. Moorhead (1992). *The Competitive Intelligence Handbook.* London: Scarecrow Press.

Federal Bureau of Investigation (1995). "Economic Espionage and Protection of Proprietary Economic Information Act of 1996." Federal Bureau of Investigation Proposal, Washington, DC, 4 December.

Madsen, Wayne (1993). "Intelligence Agency Threats to Computer Security." *International Journal of Intelligence and Counterintelligence* 6(Winter): 413-445.

Perry, Sam (1995). "Economic Espionage and Corporate Responsibility." *Criminal Justice International* 11(2): 3.

Richter, James A. (1995). "Clandestine Encounters: The New Wave of Industrial Espionage." Ann Arbor, MI: Strategic Development Staff, National Center for Manufacturing Sciences.

Stack, Michael (1995). "Security Organization Offers Industry Local, National and International Resources and Counterespionage Guidance," Ann Arbor, MI: National Center for Manufacturing Sciences.

Schweizer, Peter (1993). *Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets.* New York: Atlantic Monthly Press.

Tolchin, Martin, and Susan J. Tolchin (1992). *Selling Our Security: The Erosion of America's Assets.* New York: Alfred A. Knopf.

U.S. House (1996). Committee on the Judiciary. Subcommittee on Crime. *Hearings on Economic Espionage.* 104th Cong., 2d sess.

U.S. Senate (1996a). *To prohibit economic espionage, to provide for the protection of United States vital proprietary economic information, and for other purposes.* 104th Cong., 2d sess. S. 1556. (2/1/96):104-359.

_____(1996b). *Intelligence Authorization Act for Fiscal Year 1997.* 104th Cong., 2d sess. S. 1718. (4/30/96): 10626-10635.