THE FEDERAL GOVERNMENT'S WAR ON ECONOMIC ESPIONAGE

DARREN S. TUCKER*

In economics, we are competitors, not allies.
— Pierre Marion, former French Intelligence Director.
They're robbing us blind.
— Raymond Rocca, former Central Intelligence Agency Deputy Director of Counterintelligence.

1. INTRODUCTION

During the Cold War, both intelligence[1] and counterintelligence[2] focused on military and political targets.[3] A typical case

---

* J.D. Candidate, 1998, University of Pennsylvania Law School; B.A., 1995, College of William and Mary. Special thanks to Robert A. Rizzi and Jonathan Fredman for commenting on a previous draft and Edwin O'Connor and his team of Associate Editors for their editing assistance. I dedicate this Comment to my grandmother, Betty, my parents, Tom and Audrey, my sister, Megan, and my fiancée, Anne.

[1] Intelligence is categorized as strategic or tactical. *See* UNITED STATES INTELLIGENCE: AN ENCYCLOPEDIA at xi (Bruce W. Watson et al. eds., 1990). Strategic intelligence is "information on events, threats, and individuals that create major problems for the federal government." *Id.* Tactical intelligence is (1) information used to assess military threats against the U.S. armed forces and (2) covert and clandestine operations used to collect information or to influence events. *See id.*

[2] Counterintelligence is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personal, physical, document or communications security programs." Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1982), *reprinted in* 50 U.S.C. § 401 (1997). Counterintelligence "may include tracking suspected foreign intelligence operatives, passing on deceptive information to foreign spies, and working with indigenous industries to prevent infiltration by foreign intelligence services." Timothy D. Foley, *The Role of the CIA in Economic and Technological Intelligence*, 18 FLETCHER F. WORLD AFF. Winter/Spring 1994, at 135, 141-42.

[3] *See Economic Espionage: Joint Hearing Before the Select Subcomm. on Intelligence of the U.S. Senate and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary of the U.S. Senate*, 104th Cong., 2d Sess. 45

of espionage involved an American scientist selling military technology to the Soviet Union or an Eastern European nation.[4] Since the end of the Cold War, foreign intelligence services have increasingly devoted their resources to stealing U.S. technology.[5] Now a prototypical example of espionage involves an employee selling company secrets to a foreign government, which in turn passes the information to a company based in that country.

Nations have increasingly viewed economic and technological strength as the keys to their power and influence.[6] Trade talks, for example, have replaced arms control as the most difficult form of diplomacy.[7] Intelligence services, facing lean budgets following the dissolution of the Soviet Union, are eager to adopt new roles in order to survive.[8] Government agencies involved in finance, trade and influential industries now have a growing role in surreptitious data collection.[9]

Perhaps most surprising about this disturbing trend is that the perpetrators are often long-time United States allies.[10] These countries steal U.S. economic and technological information despite their ideological similarity to and friendly diplomatic and cultural relations with the United States. Taking advantage of their access to U.S. information, many U.S. allies have obtained

---

(1996) (statement of Louis Freeh, Director, Federal Bureau of Investigation) [hereinafter Freeh]; Edwin Fraumann, *Economic Espionage: Security Missions Redefined*, 57 PUB. ADMIN. REV. 303, 303 (1997).

[4] *See* Thomas J. Jackamo, III, Note, *From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention*, 32 VA. J. INT'L L. 929, 942 (1992).

[5] *See* 142 CONG. REC. S12,208 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

[6] *See* Freeh, *supra* note 3, at 45 ("In today's world, a country's power and stature are increasingly measured by its economic and industrial capacity."); Representative Dan Glickman, *Intelligence After the Cold War*, 3 KAN. J.L. & PUB. POL'Y 142, 144 (1994) ("With the end of the Cold War, Americans accept today more than ever the premise that economic strength defines national security.").

[7] *See* Peter Schweizer, *The Growth of Economic Espionage: America Is Target Number One*, FOREIGN AFF., Jan./Feb. 1996, at 9, 13 [hereinafter *The Growth of Economic Espionage*].

[8] *See id.* at 13.

[9] *See* Freeh, *supra* note 3, at 45-46.

[10] *See Economic Espionage: Joint Hearing Before the Select Subcomm. on Intelligence of the U.S. Senate and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary of the U.S. Senate*, 104th Cong., 2d Sess. 17 (1996) (statement of David E. Cooper).

valuable confidential information with more success than the United States' traditional enemies.[11] Ironically, the U.S. intelligence community often trained and supplied the very services now spying on the United States.[12]

Even during the Cold War, countries that were formally allied with the United States spied on U.S. corporations.[13] Some U.S. allies adopted a "two-track" approach, under which they worked with the United States against the Soviet Union while pilfering trade secrets from U.S. corporations.[14] In fact, "[t]he practice of economic spying by allied intelligence services was an open secret amongst many FBI and CIA professionals during the Cold War."[15] The U.S. government did not consider espionage from friendly countries to be a serious national security concern during the Cold War.[16] The U.S. intelligence community kept economic espionage by our friends secret to ensure that allied intelligence services continued to spy on the Soviet Union.[17] Victimized U.S. companies rarely revealed the theft of their confidential information.[18] Thus, few people outside of the counterintelligence community were aware that many U.S. allies stole information from U.S. corporations.

This Comment examines economic espionage activities against the United States and how the U.S. government has recently moved to counter foreign governments stealing U.S. trade secrets. Section Two of this comment explains what is meant by the term economic espionage and contrasts it with industrial espionage. Section Three looks at which countries attempt to steal U.S. corporate secrets and what types of information they seek. Section Four examines the losses U.S. industry suffers as a result of economic espionage. Section Five details the methods that foreign intelligence services use to acquire trade secrets from U.S.

---

[11] *See* Freeh, *supra* note 3, at 46.

[12] *See* PETER SCHWEIZER, FRIENDLY SPIES 5 (1993) [hereinafter FRIENDLY SPIES]; Fraumann, *supra* note 3, at 204.

[13] *See* James Sherr, *Cultures of Spying*, NAT'L INTEREST, Winter 1994/1995, at 56, 59.

[14] *See* Foley, *supra* note 2, at 142.

[15] Sherr, *supra* note 13, at 59.

[16] *See* FRIENDLY SPIES, *supra* note 12, at 6.

[17] *See id.* at 5-6.

[18] *See id.* at 7; *see also infra* section 4 for reasons why corporations do not admit losses.

firms. Section Six describes the programs implemented by U.S. executive agencies to prevent economic espionage. Section Seven outlines the civil remedies and criminal provisions used to deter and punish trade secret theft, including the Economic Espionage Act of 1996. Section Eight offers recommendations for both the public and private sectors on additional ways to prevent economic espionage. This Comment concludes that what has emerged from the federal government in the past few years is a foundation for a strong assault on economic espionage against the United States.

2. ECONOMIC ESPIONAGE DEFINED

Economic espionage is different from traditional espionage and industrial espionage.[19] Economic espionage is a foreign government's sponsoring, coordinating or assisting intelligence efforts directed at a domestic government, corporation, establishment, or person that involves the unlawful or clandestine targeting or acquisition of (1) trade secrets[20] or (2) sensitive financial, trade, or economic policy information.[21] Traditional espionage is foreign sponsored or coordinated intelligence directed at a domestic government or domestic corporation, establishment, or person, that involves the identification, targeting and collection of

---

[19] Economic espionage should also be distinguished from economic intelligence. Economic intelligence involves the use of legal and legitimate tools for collecting publicly available information. *See* Peter Schweizer, *Hello, Cruel World: How to Succeed in Business*, NEWS & OBSERVER (Raleigh), Mar. 9, 1997, at G5.

[20] "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995). This Comment considers trade secrets and proprietary information to be equivalent.

[21] *See* The Economic Espionage Act of 1996, 18 U.S.C.A. §§ 1831-39 (West Supp. 1997); *Economic Espionage: Joint Hearing Before the Select Comm. on Intelligence of the U.S. Senate and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary of the U.S. Senate*, 104th Cong., 2d Sess. 1 (1996) (statement of Sen. Specter) [hereinafter Specter]; *The Threat of Foreign Econ. Espionage to U.S. Corps., 1992: Hearings Before the Subcomm. on Econ. and Commercial Law of the Comm. on the Judiciary*, 102d Cong., 2d Sess. 192-93 (1992) (prepared statement of Geoffrey E. Turner); Foley, *supra* note 2, at 135; Robert Dreyfuss, *Company Spies* (visited Sept. 24, 1997) <http://www.mojones.com/mother_jones/MJ94/dreyfuss.html>; *Welcome to ANSIR on the Internet* (last modified Jan. 16, 1997) <http://www.fbi.gov/ansir/ansir.htm>.

national defense information.[22] Industrial espionage is a corporation's use of illegal techniques to collect information, such as trade secrets, not voluntarily provided by the source.[23]

The key difference between economic espionage and industrial espionage is that only the former involves a government's efforts to collect information. An example of industrial espionage would be a South Korean company eavesdropping on Intel's communications. If, however, the South Korean government supplied the listening equipment or owned the company, then the Korean company's activities would be considered economic espionage. Despite some overlap in usage, economic, industrial, and traditional espionage are mutually exclusive terms.[24] This Comment will only discuss economic espionage.

3. PERPETRATORS AND TARGETS OF ECONOMIC ESPIONAGE

Companies around the world have become more vulnerable to trade secret theft for several reasons. First, the end of the Cold

---

[22] *See Welcome to ANSIR on the Internet*, *supra* note 21.

[23] *See* BENJAMIN GILAD AND TAMAR GILAD, THE BUSINESS INTELLIGENCE SYSTEM: A NEW TOOL FOR COMPETITIVE ADVANTAGE 4 (1988). Some commentators also consider legal information gathering as a form of industrial espionage. *See, e.g.*, RICHARD EELLS AND PETER NEHEMKIS, CORPORATE INTELLIGENCE AND ESPIONAGE: A BLUEPRINT FOR EXECUTIVE DECISIONMAKING 109 (1984).

[24] *See supra* note 21.

There is little agreement as to the proper definition of economic espionage. Peter Schweizer does not include a definition of economic espionage, or differentiate economic espionage from industrial espionage, in his oft-cited *Friendly Spies*. *See generally* FRIENDLY SPIES, *supra* note 12. Some authors have mistakenly referred to foreign industrial espionage when discussing economic espionage or vice versa. *See, e.g.*, Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, 108 Stat. 3432; Marc A. Moyer, Comment, *Section 301 of the Omnibus Trade and Competitiveness Act of 1988: A Formidable Weapon in the War Against Economic Espionage*, 15 NW. J. INT'L L. & BUS. 178 *passim* (1994). Even Schweizer uses the terms economic espionage and industrial espionage to mean the same thing. *See* FRIENDLY SPIES, *supra* note 12 *passim*.

The term "economic espionage" does not replace the term "industrial espionage." *But see* Moyer, *supra* at 178 n.1. Instead, there are clear differences between economic and industrial espionage. First, economic espionage involves a government's gathering or assisting in gathering information, while industrial espionage only involves private companies or citizens. Second, economic espionage may involve spying on another government, whereas industrial espionage rarely, if ever, does.

War made available intelligence resources previously devoted to securing military technology.[25] Second, disagreements between countries within the Western alliance are no longer of major strategic importance.[26] Third, intangible property,[27] which is often easier to steal than tangible property, has become more common.[28] Fourth, more employees typically have access to trade secrets than in the past.[29] Fifth, employees have greater opportunities to gain from knowledge of trade secrets, either by changing jobs or by becoming self-employed.[30] Sixth, computer "hackers" have the ability to steal information from corporate computer systems thousands of miles away.[31] Finally, advances in communications, such as the Internet,[32] cellular phones, and facsimile machines, have made collection of trade secrets easier.[33]

The United States is the primary target of economic espio-

---

[25] *See Economic Espionage: Joint Hearing Before the Select Subcomm. on Intelligence of the U.S. Senate and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary of the U.S. Senate*, 104th Cong., 2d Sess. 1 (1996) (prepared statement of Louis Freeh, Director, FBI) [hereinafter Freeh, Prepared Statement].

[26] *See The Growth of Economic Espionage*, *supra* note 7, at 13.

[27] Intangible property "has no intrinsic and marketable value, but is merely the representative or evidence of value, such as certificates of stock, bonds, promissory notes, copyrights, and franchises." BLACK'S LAW DICTIONARY 809 (6th ed. 1990).

[28] *See* Richard J. Heffernan, Testimony with Regard to Economic Espionage Before the House Comm. on the Judiciary Subcomm. on Crime Subcomm. on Crime (May 9, 1996) (noting a survey that found that intangible assets of U.S. manufacturing companies rose from 38% to 62% of market value from 1982 to 1992).

[29] *See* Peter J.G. Toren, *The Prosecution of Trade Secrets Thefts Under Federal Law*, 22 PEPP. L. REV. 59, 60-61 (1994).

[30] *See id.* at 61 & n.7.

[31] *See id.* at 62.

[32] The Internet is a computer network linking people, institutions, corporations and governments around the globe. *See* ACLU v. Reno, 929 F. Supp. 824, 830-31 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997). The Internet allows users to transmit "text, data, computer programs, sound, visual images (i.e., pictures), and moving video images." *Id.* at 834.

[33] *See* 142 CONG. REC. S12,208 (daily ed. Oct. 2, 1996). One commentator argues that American corporations' dependence on communications systems, computer networks and electronic equipment makes the United States more vulnerable to economic espionage than other countries. *See* Fraumann, *supra* note 3.

nage.[34] The openness of American government, industry and society makes information fluid and accessible.[35] The United States has the most sought-after technology and many of the best research facilities in the world;[36] no other country produces as much intellectual property as the United States.[37] In addition, few industrial spies in the United States are ever arrested,[38] and until recently, there were few penalties for those who were caught.[39]

The number of countries engaging in economic espionage against United States corporations is staggering. A FBI study of 173 countries found that 100 had spent money to acquire U.S. technology,[40] and that 57 of those had engaged in covert operations against U.S. corporations.[41] According to former CIA Director Robert Gates, "[g]overnments in Asia, Europe, the Middle East and, to a lesser degree, Latin America — nearly 20 governments overall — are involved in intelligence activities that are detrimental to our economic interests."[42] A recently declassi-

---

[34] *See* FRIENDLY SPIES, *supra* note 12, at 32. Nevertheless, other countries have been victims of economic espionage. *See, e.g.*, Heffernan, *supra* note 28 (England, Canada, and Germany); Rob Norton, *The CIA's Mission Improbable*, FORTUNE, Oct. 2, 1995, at 55 (France); *Egyptian 'Spying' Trial*, FINANCIAL TIMES (London), Apr. 25, 1997, at 4 (Egypt); Randy Newell & Southam News, *Economic Espionage; Corporate Spying Becoming a Growth Industry*, MONTREAL GAZETTE, April 15, 1993, at F1 (Canada); *Spies Among Our Apple Trees*, THE DOMINION (Wellington), Apr. 29, 1997, at 6 (Australia); *Swiss Won't Pursue Case Against Marc Rich*, WALL ST. J., Aug. 19, 1985 at 19 (Switzerland); *Unsmart — U.S. Wastes Time, Imperils Friendships with Economic Espionage on Our Allies*, HARRISBURG PATRIOT & EVENING NEWS, Oct. 19, 1995, at A14 (editorial) (Japan).

[35] *See* FRIENDLY SPIES, *supra* note 12, at 32-33. For example, research conducted at universities, which is more prevalent in the United States than in other countries, is poorly protected. *See id.* at 32.

[36] *See id.* at 32.

[37] *See* H.R. REP. NO. 104-788, at 4 (1996) ("The United States produces the vast majority of the intellectual property in the world.").

[38] *See infra* section 7 for a discussion of the reluctance of victimized corporations to press charges.

[39] *See infra* sections 7.2-7.3.2 for a discussion of prosecution of trade secret theft prior to the Economic Espionage Act of 1996.

[40] *See The Growth of Economic Espionage*, *supra* note 7, at 11.

[41] *See id.*

[42] Ronald E. Yates, *Cold War: Part II, Foreign Intelligence Agencies Have New Targets — U.S. Companies*, CHI. TRIB., Aug. 29 1993, at C1 (internal quotations omitted). Gates did not name the twenty governments.

According to popular press reports, the most aggressive and effective

fied CIA report on national security threats listed countries "extensively engaged in economic espionage" against the United States as France, Israel, China, Russia, Iran and Cuba.[43] Notably absent from the list was Japan, a country viewed by many as possessing one of the most brazen and efficient intelligence services worldwide.[44] The CIA concluded, however, that Japanese efforts are largely limited to legal data gathering and hiring "well-placed" consultants.[45]

3.1. Industries and Information Targeted

The primary targets of foreign intelligence agencies are high technology and defense-related industries;[46] however, even non-technology-intensive industries are at risk of theft.[47] The industries targeted by foreign agents tend to be of strategic interest to the United States for three reasons: (1) they produce classified products for the government; (2) they provide products used in both the military and the private sector; and (3) they are critical

---

economic espionage emanates from France, Japan, Israel, Germany, South Korea, Great Britain, Russia, China, Taiwan, Pakistan, India, Syria, Egypt, Iran, Cuba and Eastern European nations. *See generally* Norm Alster, *The Valley of the Spies*, FORBES, Oct. 26, 1992, at 200; John Berthelsen, *Friendly Spies*, FAR E. ECON. REV., Feb. 17, 1994, at 28; *French and Japanese Spies, Economic Espionage, 'Rival' KGB's Old Efforts, Experts Say*, NEW TECH. WK., Nov. 23, 1992, at A1; Bill Gertz, *FBI Official Says Friends, Foes Spy on U.S. Business*, WASH. TIMES, Apr. 22, 1997, at A6; Newell & News, *supra*, note 34, at F1; Yates, *supra*, at C1. *But see* Jackamo, *supra* note 4, at 944 & n.88 (stating that the Netherlands, Belgium and the Scandinavian countries are among those that pose "the greatest threat to the commercial secrets of the United States").

[43] *CIA: Israel Among Most 'Extensive' In Economic Espionage*, DEF. WK., Aug. 5, 1996, *available in* LEXIS, News Library, Curnws File.

[44] *See, e.g.*, FRIENDLY SPIES, *supra* note 12, at 18 ("The Japanese intelligence system is perhaps the most comprehensive and complex of the friendly spy networks being used against the United States."); Teresa Watanabe, *Japan Business Has a Lot of Bugs to Work Out as Wiretapping Rises*, L.A. TIMES, Oct. 21, 1995, at A8 ("Japan is believed to possess one of the most comprehensive business intelligence-gathering operations in the world . . . .").

[45] *CIA: Israel Among Most 'Extensive' In Economic Espionage*, *supra* note 43. Nevertheless, the vast majority of Japanese intelligence efforts are directed at the United States. *See* James A. Richter, *Clandestine Encounters: The New Wave of Industrial Espionage* (National Center for Manufacturing Sciences), 1995, at 8.

[46] *See* Freeh, *supra* note 3, at 47.

[47] *See* Ed Jopeck & Ken Sawka, *Foreign Espionage: Is Your Business at Risk* (visited Sept. 25, 1996) <http://www.scip.org/jan3.html>.

to maintaining economic security.[48] The most frequently targeted industries include aerospace, biotechnology, telecommunications, computer hardware and software, transportation technology, defense and armaments technology, automobiles, energy research, semiconductors, advanced materials, basic research, and lasers.[49] Future spying is expected to mirror the industries listed on the White House Critical Technologies List.[50]

Intelligence agents seek not only technology, but also proprietary business information from their targeted industries.[51] Pricing data, customer lists, product development data, basic research, sales figures, and marketing plans are stolen more often than advanced technology.[52] Foreign governments also seek development plans, propriety information reports, personnel data, contract bids, manufacturing cost analyses, propriety software, and strategic planning.[53]

Economic espionage directed at the United States government is also focused on a few key areas. According to the FBI, foreign governments seek the following information: U.S. economic, trade, and financial agreements; U.S. trade developments and policies; U.S. national debt levels; U.S. tax and monetary policies; foreign aid programs and export credits; technology transfer and

---

[48] *See* Freeh, *supra* note 3, at 48.

[49] *See* 142 CONG. REC. S12,208 (daily ed. Oct. 2, 1996) (statement of Sen. Specter); Freeh, *supra* note 3, at 47; Lloyd M. Burchette Jr., *Economic Espionage is a Big Threat to National Security*, GREENSBORO NEWS & REC., Mar. 6, 1994, at F1; *Economic Espionage*, SEATTLE TIMES, Nov. 6, 1991, at A3; Anne Eisele, *U.S. Urged: Be Tougher on Economic Espionage*, NEW TECH. WK., Aug. 21, 1995, *available in* LEXIS, News Library, Nwltrs File.

[50] *See French and Japanese Spies, Economic Espionage, 'Rival' KGB's Old Efforts, Experts Say*, *supra* note 42, at 4. In 1994, companies on the Critical Technologies List reported the majority of all attempts by foreign governments to acquire corporate secrets. *See Counterintelligence News & Developments* (Nat'l Counterintelligence Ctr.), Issue No. 1, (visited Sept. 25, 1997) <http://www.loyola.edu/dept/politics/hula/cind1.html>.

[51] *See* Freeh, *supra* note 3, at 47 ("Proprietary business information, i.e., bid, contract, customer and strategy information . . . is aggressively targeted . . . .").

[52] *See* Yates, *supra* note 42, at C1. The survey included all types of theft, not just economic espionage.

[53] *See* Freeh, *supra* note 3, at 47; *Economic Espionage: Joint Hearing Before the Select Comm. on Intelligence and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary of the U.S. Senate*, 104th Cong. 26 (1996) (statement of John J. Higgins) [hereinafter Higgins]; Paul Barker, *Economic Espionage Threat Real: CSIS; Canadian Security Intelligence Service*, COMPUTING CAN., Feb. 15, 1995, at 1.

munitions control regulations; U.S. energy policies and critical materials stockpiles data; U.S. commodity policies; and proposed legislation affecting foreign firms operating in the U.S.[54]

3.2. Regions of the United States Favored by Spies

Within the United States, economic espionage occurs with the greatest frequency in regions with high concentrations of high technology research and corporations. Dallas, Boston, and Washington, D.C. attract much of the espionage activity.[55] However, experts consider Silicon Valley the most targeted area.[56] Silicon Valley offers an ideal setting for economic espionage because of "its concentration of electronics, aerospace, and biotechnology industries, its national ties to the Far East, and its mobile, multinational work force."[57] Japan, Taiwan, South Korea, China, the former Soviet Union, and the Russian Republic have devoted the most resources to stealing Silicon Valley technology.[58]

3.3. Target Number One: International Business Machines

Perhaps no other company has been targeted by foreign intelligence agents as many times as International Business Machines ("IBM"). A leader in both computer hardware and software, IBM produces many products of strategic interest to other governments. According to IBM's internal documents,

---

[54] *See* Freeh, *supra* note 3, at 48-49.

[55] *See* John Berthelsen, *Friendly Spies*, FAR E. ECON. REV., Feb. 17, 1994, at 28.

[56] *See* Dreyfuss, *supra* note 21, at 39 (statement of Frank Figliuzzi, FBI special agent) ("Silicon Valley is an enormous target. . . . We like to say that it has a bull's-eye sitting over it, in terms of more intelligence services and foreign powers trying to get their hands on it.").

[57] Foley, *supra* note 2, at 143; *see also* Alster, *supra* note 42, at 200.

[58] *See* Foley, *supra* note 2, at 143 ("China has targeted Silicon Valley for many years . . . ."); Alster, *supra* note 42, at 200; Berthelsen, *supra* note 55, at 28 ("Asian governments and multinationals, particularly Japan, Taiwan and South Korea, are the chief culprits in the attempts to pilfer Silicon Valley's secrets."); Steven Roberts et al., *Why There Are Still Spies*, U.S. NEWS & WORLD REP., Mar. 7, 1994, at 32 ("[T]he Soviet Union began focusing its attention on high-tech centers such as California's Silicon Valley more than a decade ago."). One commentator argues that Japanese "espionage in Silicon Valley nearly devastated the U.S. computer industry." FRIENDLY SPIES, *supra* note 12, at 34.

foreign agents illegally sought to acquire business secrets twenty-five times over a ten year period.[59] A retired French spymaster has even admitted spying on IBM.[60] Referring to the proliferation of economic espionage, one IBM official stated, "we're all under attack."[61]

The most famous attempt to steal trade secrets from IBM mirrored that of an old Soviet spy operation. In 1980, an IBM employee stole some of the *Adirondack Workbooks*, a series of valuable books containing computer specifications and strategic planning, and sold them to Hitachi, a Japanese computer maker.[62] Not content with a partial set of the *Workbooks*, Hitachi sought the remaining *Workbooks* and other confidential material from other sources.[63] Over the next two years, the FBI, in conjunction with IBM, set up an elaborate sting operation.[64] In the end, Hitachi's efforts were thwarted, the conspirators were arrested, the Japanese government's involvement was revealed, and Hitachi paid IBM a considerable out-of-court settlement.[65] Still, the conspirators did not receive any jail time, and Hitachi greatly benefited from the *Workbooks*.[66]

4. SCOPE OF LOSS TO UNITED STATES INDUSTRY

Industry surveys indicate that many companies are targets of industrial spies. A 1988 National Institute of Justice study found that forty-eight percent of high-tech companies surveyed had been the victim of trade secrets theft.[67] The American Society for Industrial Security International found that foreign nationals were

---

[59] *See* FRIENDLY SPIES, *supra* note 12, at 34. IBM estimates that economic espionage and software piracy have cost it $1 billion. *See* Douglas Waller, *The Open Barn Door*, NEWSWEEK, May 4, 1992, at 58, 59.

[60] *See* Burchette, *supra* note 49, at F1.

[61] *Economic Espionage*, *supra* note 49, at A3.

[62] *See* FRIENDLY SPIES, *supra* note 12, at 46-48.

[63] *See id.* at 51-64.

[64] *See id.* at 48-64.

[65] *See id.* at 56-57, 62-64. The Japanese government aided Hitachi's scheme by providing transmission of information through diplomatic cables and the Japanese consulate. *See id.* at 56-57. The out-of-court settlement between Hitachi and IBM was rumored to be three hundred million dollars. *See id.* at 64.

[66] *See id.* at 63-64.

[67] *See* S. REP. NO. 104-359, at 8 (1996).

identified in twenty-one percent of incidents involving intellectual property loss where the nationality of the perpetrators was known.[68] A 1993 survey found that the number of thefts of proprietary information had increased 260 percent since 1985; those involving foreign governments increased fourfold.[69] Intellectual property losses between the 1992 and 1996 surveys rose 323 percent.[70] In 1994, seventy-four U.S. companies reported a total of 446 incidents of suspected targeting by foreign governments, either domestically or abroad.[71]

The monetary losses from the theft of corporate secrets are difficult to estimate. United States intelligence agencies have not studied in-depth the losses due to economic espionage.[72] Private sector surveys have been criticized for being based on small, unrepresentative samples that have emphasized domestic holdings.[73] Companies often prefer not to disclose that they have been the victims of industrial or economic espionage.[74] An admission can embarrass the company, lower stock prices, scare away investors and customers,[75] and reduce market share.[76]

---

[68] *See* H.R. REP. NO. 104-788, at 5-6 (1996).

[69] *See* 142 CONG. REC. S12,201-03 (1996).

[70] *See* H.R. REP. NO. 104-788, at 6.

[71] *See Counterintelligence News & Developments*, *supra* note 50. *But see* Robert Dreyfuss, *Tinker, Tailor Silicon Spy*, CAL. LAW., May 16, 1996, at 37, 39 (statement of Frank Dudley Berry, Deputy District Attorney in the High Technology Unit of the Santa Clara District Attorney's Office) ("It's nonsense. . . . There isn't any [economic espionage]. It doesn't exist.").

[72] *See* Freeh, *supra* note 3, at 49.

[73] *See, e.g., id.*

[74] *See* FRIENDLY SPIES, *supra* note 12, at 7; *accord Counterintelligence News & Developments*, *supra* note 50 (stating that 42% of surveyed corporations did not report suspected incidents of economic espionage to the government). The General Accounting Office was unable to complete a survey on economic espionage because few companies cooperated. *See* Ruth Sinai, *U.S. Intelligence Agencies Ponder Responses to Economic Espionage Allies Such as Japan, France, South Korea and Germany Spy on American Firms*, NEWS & OBSERVER (Raleigh), Feb. 22, 1993, at A4.

[75] "When companies have blamed U.S. allies by name, they have been known to lose large contracts in those countries." FRIENDLY SPIES, *supra*, note 12, at 7. Companies may also fear losing Pentagon clearance if they admit security breaches. *See French and Japanese Spies, Economic Espionage, 'Rival' KGB's Old Efforts, Experts Say*, *supra* note 42, at 1.

[76] *See* 142 CONG. REC. S12,201-03 (1996) (statement of Sen. Specter); Freeh, *supra* note 3, at 49. David Harris of Insigns Strategic Research summarized the pitfalls of admitting a loss due to espionage: "When you put your foot in it, you don't want to advertise the fact. . . . [Victimized companies] may feel it's

There is not likely to be a corresponding gain from revealing the misappropriation.[77] An even greater problem is that most misappropriations are probably undetected.[78]

Estimates of losses from economic espionage in the United States range from $2 billion to $260 billion per year.[79] Including overseas operations of American corporations, the estimates rise to $400 billion per year.[80] Estimates of jobs lost due to economic espionage range from one to six million.[81]

Economic espionage also has a long-term effect: a reduction in incentives for innovative behavior. Say firm A develops a new product at high cost and firm B steals the product design.[82] Each firm has produced the same product, but A's costs are much higher than B's. Firm A's return on investment will be quite low, while firm B's return will be high.[83] In the future, firm A may hesitate to develop new products. Indeed, one professor has demonstrated that when a significant amount of a firm's research

---

like advertising the fact that they're a soft target." Newell & News, *supra* note 34, at F1.

[77] *See* Moyer, *supra* note 24, at 180 n.12.

[78] *See id.* at 180.

[79] *See, e.g.*, Specter, *supra* note 21, at 2 (estimating that U.S. firms lose $100 billion a year); 142 CONG. REC. S12,201-03 (1996) (statement of Sen. Kohl) ($63 billion); Fraumann, *supra* note 3, at 303 (at least $50 billion); Toren, *supra* note 29, at 62 ($1.8 billion); John Danker, *Economic Espionage Increases, Threatening National Security*, INSIGHT ON THE NEWS, July 18, 1994, at 37 ($20 billion); *House Judiciary Panel Backs Stiffer Penalties for Economic Spying*, WALL. ST. J., Sept. 12, 1996 ($24 billion); *Economic Espionage: The Corporate Threat* (visited Oct. 22, 1996) <http://emporium.turnpike.net/~IntlInt/econ.html> ($260 billion); Sam Perry, *Economic Espionage and Corporate Responsibility* (last modified 1995) <http://www.acsp.uic.edu/oicj/pubs/cji/110203.htm> ($240 billion). Definitional problems may account for part of the range. Some argue that the higher figures come from "ex-spies seeking new career paths and by agencies seeking purpose in a post-Cold War world." Skip Kaltenheuser, *Industrial Espionage is Alive and Well*, WORLD TRADE, July 1997, at 24.

[80] *See, e.g.*, *Economic Espionage: The Corporate Threat*, *supra* note 79.

[81] The International Trade Commission estimates one million jobs in the United States lost due to economic espionage. *U.S. Losing High-tech Secrets to "Student" Spies*, SING. STRAITS TIMES, Apr. 8, 1997. ABC News reported that economic espionage eliminates six million jobs. *See* Specter, *supra* note 21, at 2.

[82] This example is an extrapolation of the discussion in FRIENDLY SPIES, *supra* note 12, at 25.

[83] This greatly simplified example assumes that the companies are essentially similar, that B is not penalized for stealing, and that the cost of stealing the design is less than the cost of developing it.

and development is stolen, a profit-maximizing firm will reduce or even eliminate its research and development activities.[84] Some believe that the disincentive to invest in new products caused by economic and industrial espionage is such a serious problem as to threaten "the country's national technological prowess."[85]

Many predict that losses due to economic espionage will continue to worsen.[86] Foreign intelligence agencies are continuing to devote additional resources to spying on friendly countries.[87]

5. METHODS OF DATA COLLECTION

Foreign governments increasingly use sophisticated data gathering techniques against U.S. corporations. Foreign agents tend to combine several methods of data collection and may use both legal and illegal means.[88] Foreign governments employ traditional espionage methods, as well as specialized economic collection methods, to pilfer trade secrets.[89] Former heads of the CIA and the FBI have stated that the French and Russian intelligence services now use the same methods to spy on U.S. corporations as they used to spy on each other during the Cold War.[90] The following discussion outlines some of the most common means of economic intelligence gathering.[91]

---

[84] *See* Y.H. Cheung, *The Economics of Industrial Espionage: A Game Theory Approach*, INT'L J. BUS. STUD. (forthcoming).

[85] FRIENDLY SPIES, *supra* note 12, at 25.

[86] *See, e.g.*, 142 CONG. REC. S377, S377 (1996) (statement of Sen. Cohen) ("[T]he threat to U.S. economic interests will absolutely increase as foreign governments attempt to ensure the success of their companies." (internal quotations omitted)); FRIENDLY SPIES, *supra* note 12, at 22 (quoting a source as saying that "the cost of espionage committed against the United States . . . will increase in both absolute and relative terms") .

[87] *See* FRIENDLY SPIES, *supra* note 12, at 26-27.

[88] *See Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* (July 1995) (visited Jan 27, 1997) <http://www.nacic.gov/f-y95rpt.html> [hereinafter *Annual Report*]. The 1996 report "noted little new in the origin of the threat, collection targets, or methods used in effecting economic collection and industrial espionage." *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* (May 1996) (visited Jan 27, 1997) <http://www.nacic.gov/cind/econ96.htm>.

[89] *See Annual Report*, *supra* note 88.

[90] *See* Yates, *supra* note 42, at C1.

[91] The general structure of the following discussion is taken from *Annual Report*, *supra* note 88.

The most effective means of economic espionage are specialized technical operations.[92] These include breaking into computers,[93] intercepting communications, and decoding encrypted messages.[94] The increasing use of satellites, microwaves, and cellular phones makes interception easy and detection difficult.[95] Japan's Ministry of International Trade and Industry allegedly listens to the phone lines of American firms in Japan under an agreement with the Japanese national phone company.[96] Some estimate that "seventy foreign governments regularly eavesdrop on U.S. corporate communications being transmitted on telephone systems overseas."[97] Many governments use surveillance and surreptitious entry as effective and inexpensive means of intelligence. Agents have stolen papers, computers, and computer disks from company offices and from the hotel rooms of executives traveling abroad.[98] French intelligence, for example, has placed hidden listening devices aboard some Air France planes in hopes of gaining useful information.[99]

A foreign government's best source of information is an employee of the target company, often called a "mole."[100] These employees' value lies in their direct and legitimate access to desired information.[101] Counterintelligence agents report that

---

[92] *See Annual Report*, *supra* note 88; *accord* FRIENDLY SPIES, *supra* note 12, at 42.

[93] A recent report by the National Counterintelligence Center noted that use of the Internet is the fastest-growing method of economic espionage. *See* James T. McKenna, *National Intelligence Agencies Are Tapping*, AVIATION WK. & SPACE TECH., Jan. 20, 1997, at 61. The FBI estimates that 85 to 97% of online intrusions are not detected. *See* Jon Swartz, *Modern Thieves Prefer Computers to Guns*, S.F. CHRON., Mar. 25, 1997, at A1.

[94] *See Annual Report*, *supra* note 88.

[95] *See* FRIENDLY SPIES, *supra* note 12, at 42.

[96] *See French and Japanese Spies, Economic Espionage, 'Rival' KGB's Old Efforts, Experts Say*, *supra* note 42.

[97] FRIENDLY SPIES, *supra* note 12, at 43.

[98] *See Annual Report*, *supra* note 88.

[99] *See Economic Espionage*, *supra* note 49, at A3.

[100] *See Annual Report*, *supra* note 88. One survey reported that three quarters of the loss of proprietary information may have been caused by employees and others with a "trusted relationship" with the company. *See* Heffernan, *supra* note 28. Another survey estimated that current or former employees were responsible for fifty-eight percent of losses of proprietary information. *See* Toren, *supra* note 29, at 61 n.8.

[101] *See* Freeh, *supra* note 3, at 50.

recruitment of moles is relatively easy in the United States.[102] Intelligence collectors target both high ranking employees and support staff.[103] Intelligence agencies favor international scientific conferences, trade shows, and air shows for recruiting moles because these events draw many scientists and engineers.[104] Occasionally, spy agencies will plant agents within the target company;[105] although, this is not a very effective method.[106]

To acquire technology, some governments use graduate students studying or researching in the United States.[107] Intelligence agencies may recruit students before, during, or after studying abroad.[108] One unidentified country allows students to study abroad and gather foreign business and technological data instead of performing compulsory military service.[109] The Japanese government has ordered some Japanese graduate students in the United States to report on scientific developments or face having their scholarships terminated.[110] Similarly, some countries debrief their citizens after foreign travel.[111]

Intelligence agencies have found recruiting persons of their own ethnic group to be an effective means of gaining proprietary and classified technology.[112] Foreign agents may appeal to a person's patriotism and sense of ethnic loyalty. American citizens

---

[102] Motivations for stealing information include greed, drug or alcohol problems, financial difficulty, and stress. *See Annual Report*, *supra* note 88. Many Americans may be unaware that the theft or transportation of trade secrets may be a crime, or they may simply believe that they can avoid detection or prosecution. Although few Americans would consider spying for the former Soviet Union, many may not see the harm in passing information to a traditional ally, such as Israel. *See* FRIENDLY SPIES, *supra* note 12, at 37.

[103] *See Annual Report*, *supra* note 88.

[104] *See id.*

[105] *See, e.g.*, Sinai, *supra* note 74, at A4 (discussing a French attempt to plant agents in IBM).

[106] *See* FRIENDLY SPIES, *supra* note 12, at 42 (quoting IBM official Robert Courtney) ("It's a crap shoot. You don't know what you get when you plant a mole. Chances are he'll probably be hired and employed in the wrong division or section . . . .").

[107] *See Annual Report*, *supra* note 88.

[108] *See id.*

[109] *See id.* The report does not identify which country has this program.

[110] *See French and Japanese Spies, Economic Espionage, 'Rival' KGB's Old Efforts, Experts Say*, *supra* note 42.

[111] *See Annual Report*, *supra* note 88.

[112] *See id.*

by birth, naturalized citizens, and permanent residents are all targets.[113] Israel is infamous for its ethnic targeting even though there is no evidence that Israel's efforts in this regard are unusual.[114]

Foreign corporations use corporate mergers and acquisitions on very rare occasions to collect intelligence on competitors.[115] For instance, in 1988 several French companies, in conjunction with Airbus, attempted to purchase a subcontractor of Boeing.[116] If the acquisition had succeeded, Airbus "would have known an enormous amount about [Boeing's] production processes, capabilities, costs, specifications, and future plans."[117]

Foreign intelligence agencies often hire information brokers and free-lance spies.[118] Information brokers gather proprietary information, sometimes by illegal means. Free-lance spies are attractive to intelligence agencies because they often specialize in certain fields and allow the agencies to insulate themselves from counterintelligence.[119]

Legal means of information gathering[120] — although not, strictly speaking, economic espionage — is also quite common. Commercial data bases, trade and scientific journals, computer bulletin boards, openly available U.S. government data, and corporate publications are just some of the readily available sources of information on employees, companies, new products, and new manufacturing techniques.[121] The use of the Freedom of Information Act ("FOIA") has become quite popular with

---

[113] *See id.*

[114] *See FBI: Ethnic Targeting Common Tactic in Economic Espionage*, DEF. WK., March 25, 1996, *available in* NEXIS, News Library, Nwltrs File. Another source states that the five nationalities that have stolen the most information are the Chinese, Canadian, French, Indian, and Japanese – not the Israelis. *See* Heffernan, *supra* note 28.

[115] *See Annual Report*, *supra* note 88; FRIENDLY SPIES, *supra* note 12, at 271-73.

[116] *See* FRIENDLY SPIES, *supra* note 12, at 272.

[117] *Id.* (quoting a senior Boeing official).

[118] *See id.* at 40; *Annual Report*, *supra* note 88.

[119] *See* FRIENDLY SPIES, *supra* note 12 at 40.

[120] Legal means of information gathering is sometimes referred to as economic intelligence, open-source data collection or commercial espionage. *See* FRIENDLY SPIES, *supra* note 12, at 44; Schweizer *supra* note 19, at G5; *supra* note 19.

[121] *See Annual Report*, *supra* note 88.

foreign governments and corporations.[122] Not wanting to alert U.S. counterintelligence agencies, some foreign governments seek open-source material covertly.[123]

6. RESPONSE OF THE EXECUTIVE BRANCH TO ECONOMIC ESPIONAGE

The Bush administration began a transformation in the U.S. intelligence community by focusing more on economic concerns, as opposed to military objectives.[124] In 1991, President Bush stated that the United States "must have intelligence to thwart anyone who tries to steal our technology or otherwise refuses to play by fair economic rules."[125] The government in 1992 evaluated U.S. counterintelligence agencies and issued them a new set of directives, forty percent of which were economic.[126]

President Clinton has continued the trend toward economic counterintelligence objectives. Some sources have stated that the administration believes that economic espionage by friendly nations could become a greater threat to the United States than did the KGB during the Cold War.[127] The White House's National Security Strategy annual issues have underscored that economic security is a vital part of national security.[128] The President's National Security Strategy of Engagement and Enlargement in 1995 directed the intelligence community "to detect and deter foreign intelligence targeting of U.S. economic and technological interests."[129] A discussion of the U.S. intelligence community and its increasing focus on economic espionage follows.

---

[122] For example, Mitsubishi made approximately fifteen-hundred FOIA requests in 1987. *See* FRIENDLY SPIES, *supra* note 12, at 45.

[123] *See Annual Report*, *supra* note 88.

[124] *See* Dreyfuss, *supra* note 71, at 40.

[125] Norton, *supra* note 34, at 55.

[126] *See* John Burgess & John Mintz, *CIA, FBI Chiefs Warn Panel Over Economic Espionage; U.S. Advanced Technology is a Target*, WASH. POST, April 30, 1992, at B11.

[127] *See* Foley, *supra* note 2, at 142.

[128] *See* Freeh, *supra* note 3, at 44.

[129] Anne Eisele, *supra* note 49 (quoting the National Security Strategy of Engagement and Enlargement of Feb. 1995).

6.1. Federal Bureau of Investigation

The FBI is the lead counterintelligence agency.[130] During the Cold War, the FBI was responsible for intercepting and countering the domestic intelligence activities of our traditional adversaries.[131] The FBI based its counterintelligence priorities on the Country Criteria List, which listed hostile countries with active intelligence services.[132] In 1990, the FBI first indicated that it would devote greater resources to countering "friendly" intelligence services.[133] One year later, the FBI replaced the Country Criteria List with a National Security Threat List. The National Security Threat List, which sets out the FBI's counterintelligence mission, includes national security threats regardless of origin and a classified list of countries whose intelligence services threaten U.S. security.[134] The United States considers economic espionage as one of the eight primary threats to national security.[135] In 1994, the FBI launched the Economic Counterintelligence program, in part to collect information and detect and counter economic espionage.[136]

The FBI is devoting more resources to fight economic espionage. In 1992, the FBI investigated ten industrial and economic espionage cases;[137] in 1996, the number rose to over 800.[138] The FBI conducts many of these investigations in conjunction with the CIA.[139] Over twenty FBI agents are investigating trade secret theft in Silicon Valley alone.[140]

The FBI informs the private sector of national security threats,

---

[130] *See* Howard M. Shapiro, *The FBI in the 21st Century*, 28 CORNELL INT'L L.J. 219, 220 (1995).

[131] *See* FRIENDLY SPIES, *supra* note 12, at 305.

[132] *See id.*

[133] *See id.* at 4.

[134] *See Welcome to ANSIR on the Internet*, *supra* note 21.

[135] *See id.*

[136] *See* Freeh, *supra* note 3, at 45.

[137] *See* Foley, *supra* note 2, at 139.

[138] *See Economic Espionage of U.S. Companies on the Rise: Report*, AGENCE FRANCE-PRESSE, Feb. 24, 1996, *available in* NEXIS, News Library, Curnws File.

[139] *See* Yates, *supra* note 42, at 1.

[140] *See* Alster, *supra* note 42, at 204. As noted in section 3.2, Silicon Valley is the most popular region in the United States for information gathering.

including economic espionage, through its Awareness of National Security Issues and Response ("ANSIR") program, formerly known as the Development of Espionage, Counterintelligence and Counterterrorism Awareness ("DECA") program.[141] For over twenty years, ANSIR agents at each of the FBI's field offices[142] have been working with corporate security regarding foreign security threats.[143] Recently, ANSIR has made greater efforts regarding economic espionage.[144] ANSIR informs U.S. organizations of the methods used by foreign governments and ways to prevent security breaches.[145] ANSIR also occasionally publishes threat information and recently began faxing unclassified information to interested companies.[146] In 1993 and 1994, the FBI briefed approximately twenty thousand companies on foreign threats.[147]

6.2. Central Intelligence Agency

The Central Intelligence Agency monitors foreign governments that sponsor economic espionage.[148] Under U.S. law, the CIA may only conduct intelligence activities outside the United States.[149] In 1993, the Director of Intelligence indicated that the agency would begin uncovering economic espionage schemes.[150] The CIA occasionally provides information to U.S. corporations regarding trends in economic espionage under the auspices of the National Counterintelligence Center's Awareness Working Group.[151] When the CIA discovers foreign intelligence services

---

[141] *See Welcome to ANSIR on the Internet*, *supra* note 21.

[142] *See Counterintelligence News & Developments*, *supra* note 50.

[143] *See Annual Report*, *supra* note 88.

[144] *See* S. REP. NO. 104-359, at 9 (1996).

[145] *See id.*

[146] *See id.*; Ben N. Venzke, *Economic/Industrial Espionage* (visited Oct. 23, 1996) <http://www.infowar.com/class_2/class2_2.html-ssi>.

[147] *See* S. REP. NO. 104-359, at 9.

[148] *See* Foley, *supra* note 2, at 138.

[149] *See* 50 U.S.C. § 403-3(d)(1) (1997); Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981), *reprinted in* 50 U.S.C. § 401 (1997).

[150] *See* 142 CONG. REC. S12,210 (daily ed. Oct. 2, 1996) (article by Peter Schweizer). Even before 1993, the CIA helped uncover foreign governments spying on U.S. companies. *See, e.g.*, FRIENDLY SPIES, *supra* note 12, at 302-03 (noting CIA involvement in 1989 investigation in France).

[151] *See Annual Report*, *supra* note 88.

targeting U.S. firms, the CIA will coordinate with other intelligence services before revealing the information.[152] Some popular press reports, however, indicate that many targeted corporations are never informed.[153]

6.3. National Security Agency

The National Security Agency ("NSA") educates its contractors as to foreign intelligence activities.[154] Although the NSA does not work directly with the private sector, when it discovers a foreign entity spying on a U.S. company, the NSA may relay this information to the FBI for possible release to the targeted company.[155] Government and industry officials indicate, however, that the NSA rarely informs victimized corporations known to the agency.[156] Nevertheless, recent comments from high ranking NSA officials suggest that the NSA may focus more of its efforts on economic concerns.[157]

6.4. Customs

Since the end of President Bush's term of office, the United States Customs Service has operated units to prevent the export of stolen technology.[158] As the primary U.S. border enforcement agency, the Customs Service has the responsibility to prevent exports to trade-sanctioned countries, which often engage in economic espionage.[159] Between 1990 and 1993, customs agents seized a half billion dollars worth of stolen technology from the Port of Los Angeles alone.[160] The agency also provides information about economic espionage to private industry relating

---

[152] *See id.*

[153] *See, e.g.*, Sinai, *supra* note 74, at A4.

[154] *See Annual Report*, *supra* note 88.

[155] *See id.*

[156] *See* Sinai, *supra* note 74, at A4.

[157] *See* FRIENDLY SPIES, *supra* note 12, at 290-91, 304 ("Vice Admiral William O. Studeman, in a remarkably candid speech for an NSA director, warned that his agency might soon begin turning its massive electronic spy systems on the economic and corporate affairs of our friends.").

[158] *See* Berthelsen, *supra* note 55, at 30; Yates, *supra* note 42, at 1.

[159] *See Annual Report*, *supra* note 88 (reporting the duty of the Customs Service to control exports of high-technology material and information).

[160] *See* Ronald E. Yates, *U.S Intelligence Retools to Fight New Brand of Espionage*, CHI. TRIB., Aug. 30, 1993, at 1.

to exports.[161]

6.5. Department of Defense

Counterintelligence at the Defense Intelligence Agency ("DIA") focuses on traditional espionage, but may include thwarting economic espionage.[162] The agency evaluates foreign threats to Department of Defense ("DOD") programs in conjunction with the FBI.[163] The DIA briefs government contractors on intelligence activities from friendly countries.[164] The DOD distributes over twenty-five thousand copies of its Security Awareness Bulletin, which often emphasizes economic espionage.[165] The DOD also informs companies that it knows are being targeted by other companies or governments.[166]

6.6. National Counterintelligence Center

President Clinton established the National Counterintelligence Center ("NACIC") in 1994 to improve coordination and cooperation among the agencies entrusted with counterintelligence duties.[167] The NACIC consists of personnel from the FBI, CIA, NSA, DIA, and the Departments of State, and Defense.[168] The agency is headed by an FBI agent but is based in the CIA headquarters and reports to the National Security Council.[169]

The NACIC has a substantial role in gathering and disseminating information on economic espionage. The agency analyzes economic espionage threats to U.S. industry, identifies data

---

[161] *See Annual Report*, *supra* note 88.

[162] *See generally id.*

[163] *See id.* ("[DOD] [m]ilitary services work closely with the FBI when the activity involves violations of U.S. laws or intelligence activity targeted against U.S. persons.").

[164] *See id.*

[165] *See id.*

[166] *See id.*

[167] *See* 142 CONG. REC. S12,209 (article by Douglas Pasternak with Gordon Witkin); *Counterintelligence News & Developments*, *supra* note 50; *Annual Report*, *supra* note 88. For an overview of the NACIC, see *National Counterintelligence Center Homepage* (visited Jan. 27, 1997) <http://www.nacic.gov>.

[168] *See Counterintelligence News & Developments*, *supra* note 50; *Counterintelligence Information (CI.INFO)* (last updated Oct. 23, 1996) <http://140.229.1.-7//htdocs/bboards/CI.INFO.index.html>.

[169] *See* 142 CONG. REC. S12,209 (article by Douglas Pasternak with Gordon Witkin); *Counterintelligence News & Developments*, *supra* note 50.

collection methods used by foreign governments, compiles foreign intelligence threat assessments, and predicts future threats to U.S. facilities.[170] The NACIC tries to identify the counterintelligence needs of private industry and also tries to promote a positive relationship between the government and private industry.[171] For example, the agency provides unclassified reports to U.S. corporations and sponsors counterintelligence awareness, identification, and prevention programs.[172]

6.7. Department of State

The State Department's Overseas Security Advisory Council ("OSAC") works with U.S. companies to address overseas security difficulties, including economic espionage.[173] The OSAC, along with ANSIR, is one of the primary agencies charged with relaying economic espionage data to the private sector.[174] "Country Councils," consisting of U.S. diplomatic security officers and security directors of U.S. multinationals, exchange security information in over twenty-five foreign cities.[175] The OSAC uses Country Councils "to pass threat information to industry and to gather information from U.S. corporations concerning threats to U.S. economic security."[176] In addition to publishing security booklets,[177] the OSAC maintains an electronic bulletin board as a means of exchanging information between companies and the government and among companies.[178] In 1992, the State Department began supplying fifty large U.S. corporations with secure

---

[170] *See Counterintelligence News & Developments*, *supra* note 50; *Annual Report*, *supra* note 88.

[171] *See Counterintelligence News & Developments*, *supra* note 50.

[172] *See id.*; *Annual Report*, *supra* note 88; *Counterintelligence Information*, *supra* note 168.

[173] *See Annual Report*, *supra* note 88 ("Over 1,400 private-sector organizations participate in its activities and receive information and guidance.").

[174] *See id.*

[175] *See id.*; Burchette, *supra* note 49, at F1.

[176] *Annual Report*, *supra* note 88.

[177] *See, e.g.*, U.S. DEPARTMENT OF STATE OVERSEAS SECURITY ADVISORY COUNCIL, GUIDELINES FOR PROTECTING U.S. BUSINESS INFORMATION OVERSEAS (1992).

[178] *See Annual Report*, *supra* note 88. In 1995, the electronic bulletin board contained "over 42,000 individual reports of various types of threats overseas." *Id.*

portable phones normally used by U.S. officials.[179]

6.8. Other Agencies

Several other United States agencies have important, but smaller, programs to prevent economic espionage. The Department of Energy's Counterintelligence Division provides the FBI information concerning economic espionage directed towards the Energy Department's facilities and personnel.[180] The Department of Commerce briefs contractors and consultants on security matters, including technology misappropriation.[181] In all, there are nearly ten U.S. agencies involved in the war on economic espionage.[182]

7. LEGAL PROTECTION OF TRADE SECRETS

Corporations whose trade secrets have been stolen have traditionally resorted to civil means of redress, rather than seeking criminal charges.[183] Many victimized companies do not press charges because of inadequate or nonexistent criminal penalties, the belief that prosecutors do not have the ability to win a conviction, discomfort in turning the case over to the government, a fear of disclosing proprietary information at hearing, the cost of cooperating with a criminal investigation and trial, and a fear of loss of public trust and public image.[184] Nevertheless, corporations, recognizing the value of their trade secrets, are increasingly seeking criminal sanctions to protect their private

---

[179] *See* Waller, *supra* note 59, at 60.

[180] *See Annual Report*, *supra* note 88; *see also Counterintelligence News & Developments*, *supra* note 50.

[181] *See Annual Report*, *supra* note 88. One source stated that the Commerce Department operated "special units aimed at thwarting foreign companies and governments out to steal technology"; however, the NACIC's report to Congress suggests otherwise. *Compare* Yates, *supra* note 160, at 1 *with Annual Report*, *supra* note 88.

[182] Some of the agencies are the FBI, CIA, NASA, NRO, NSA, NACIC, Customs, and the Departments of State, Energy, Commerce, and Defense. *See generally Annual Report*, *supra* note 88.

[183] *See* Toren, *supra* note 29, at 59.

[184] *See* Specter, supra note 21, at 3; Toren, supra note 29, at 59 & n.3; Richard Behar, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 56, 61, 64, 69.

information.[185]

7.1. Civil Remedies Under State Law

The Restatement of Torts recognizes a cause of action for theft of trade secrets;[186] consequently, organizations that improperly acquire other companies' proprietary information may be held liable under the common law of some states.[187] In addition, thirty-eight states and the District of Colombia have passed laws resembling the Uniform Trade Secrets Act ("UTSA"), which is based on the common law cause of action for theft of trade secrets.[188] The advantage of the UTSA over the old common law is that the UTSA allows recovery from a third party that receives stolen proprietary data.[189] If government A, for example, stole information from an American company and passed the information to a company in country A, the American firm could receive damages from the foreign company for actual harm plus punitive damages under the UTSA.[190]

Although the majority of states recognize a cause of action for trade secret loss, many have criticized state remedies as inadequate.[191] Companies may not seek civil redress due to a lack of resources, a judgment-proof defendant, insufficient investigative ability, or lack of remedies where the loss took place.[192] Instead, companies may look to state criminal laws to protect their trade secrets.

---

[185] *See* Toren, *supra* note 29, at 59-60; Stanley S. Arkin, *When Theft of an Idea Can Be a Crime*, N.Y.L.J., Apr. 11, 1996, at 3.

[186] *See* RESTATEMENT OF TORTS § 759 (1939). Most of the activities in section 5 of this article appear to fall within the scope of the Restatement provision.

[187] *See* Jeff Augustini, Note, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 LAW & POL'Y INT'L BUS. 459, 474 (1995).

[188] *See id.* at 475.

[189] *See id.* at 474-75.

[190] *See* UNI. TRADE SECRETS ACT § 3, 14 U.L.A. 455 (1985).

[191] *See, e.g.*, S. REP. NO. 104-359, at 11 (1996).

[192] *See id.*

7.2. Criminal Sanctions Under State Law

Criminal sanctions against trade secret theft vary widely from state to state. Peter J.G. Toren summarizes the disparate state laws:

> Thirteen states have statutes specifically covering theft of trade secrets; eight states include trade secrets as valuable property in their statutes governing crimes against property; two states include trade secrets in their computer crime statutes; two states list trade secrets separately from other property in their larceny statutes; and twenty-four states and the District of Columbia make no explicit mention of trade secrets in their penal statutes.[193]

Even those states that ostensibly safeguard trade secrets may actually provide little protection. Furthermore, states rarely prosecute trade secret theft,[194] perhaps because trade secret theft is usually classified as a misdemeanor, not a felony.[195] Thus, in many states, an employee could sell product designs he had memorized to competitors with impunity (assuming such activities are not illegal under federal law). Clearly, state criminal codes are inadequate to protect trade secrets.

7.3. Protection of Trade Secrets Under Federal Law Prior to the Economic Espionage Act of 1996

Until recently, no federal statute directly dealt with economic espionage or the misappropriation of trade secrets and intellectual property.[196] Rather, prosecutors have relied on the National Stolen Property Act[197] and mail and wire fraud statutes, all of

---

[193] Toren, *supra* note 29, at 94-95 (citations omitted).

[194] *See* S. REP. NO. 104-359, at 11.

[195] *See id.* Colorado, which "has one of the most comprehensive criminal statute [sic] applicable to the theft of trade secrets," treats such thefts as class one misdemeanors. Toren, *supra* note 29, at 95 n.255.

[196] *See* Freeh, *supra* note 3, at 54.

[197] 18 U.S.C.A. § 2314 (West 1994 & Supp. 1996).

which were designed to prevent other crimes.[198] Not surprisingly, federal prosecutors have had difficulty winning convictions and often decline to prosecute suspected violators.[199] The following section discusses the primary federal statutes used to prosecute trade secret theft.

7.3.1. The National Stolen Property Act

The National Stolen Property Act ("NSPA") prohibits the transportation, transmission or transfer of any "goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud."[200] While this statute works well for tangible property, such as automobiles, the NSPA does not function well for intangibles, such as pricing plans.

Courts have addressed whether intangible property, such as trade secrets, falls under the "goods, wares, [or] merchandise" requirement of the NSPA. The Supreme Court in *Dowling v. United States* reversed the NSPA conviction of a defendant for selling counterfeit music albums.[201] The Court noted that

---

[198] *See* Toren, *supra* note 29, at 96 & n.258 (noting that while "there are primarily three federal criminal statutes that apply to the theft of trade secrets . . . the reach of these statutes is limited"); Arkin, *supra* note 185, at 3 & 6 n.4 (noting that statutes like the National Stolen Properties Act "were written with tangible property in mind").

Prosecutors may also bring charges for receiving stolen property, access device fraud, unauthorized disclosure of confidential information, federal racketeering, or violating the Computer Fraud and Abuse Act of 1986. *See* 18 U.S.C. §§ 1029-1030 (1988 & Supp. V 1993) (covering access device and computer fraud); 18 U.S.C. § 1905 (1988 & Supp. V 1993) (prohibiting unauthorized disclosure of confidential information by officers, employees or agents of the United States); 18 U.S.C. §§ 1961-1968 (1988 & Supp. V 1993) (covering racketeering); 18 U.S.C. § 2315 (1994) (prohibiting the transportation of stolen goods and money). The Attorney General has authority to pay up to a half a million dollars for information leading to the arrest and conviction of anyone engaging in espionage "involving or directed at the United States." 18 U.S.C. §§ 3071-3072 (1994). For an excellent overview of federal statutes that may be used to prosecute trade secret theft, see Toren, *supra* note 29, at 64-67 & nn. 32-33, 35-36, 38.

[199] *See* Toren, *supra* note 29, at 64-94 (summarizing the recent history of cases prosecuted under Federal law); *Economic Espionage Bills: FBI Head Set to Testify*, NEW TECH. WK., Feb. 26, 1996, *available in* LEXIS, News Library, Nwltrs File.

[200] 18 U.S.C.A. § 2314.

[201] Dowling v. United States, 473 U.S. 207 (1985).

previous prosecutions under the NSPA had involved physical property and that the NSPA required "a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of the subject goods."[202] Similarly, in *United States v. Brown*, the Tenth Circuit found that "[p]urely intellectual property" does not fall under the NSPA.[203]

Taken together, *Dowling* and *Brown* support the proposition that only the misappropriation of a tangible item containing a trade secret violates the National Stolen Property Act.[204] In other words, if the trade secret is not physically taken, then the "goods, wares, [or] merchandise" standard is not met.[205] For instance, an employee that faxes customer lists to a competitor does not violate the NSPA. *Dowling* and *Brown* also suggest that an employee's temporarily taking proprietary information may not violate the NSPA, since there would not be a physical identity between the borrowed documents and the items eventually transported.[206] This would occur when an employee takes confidential documents, copies them using his or her own equipment, and returns the original documents.

---

[202] *Id.* at 216. *But see id.* at 230 (Powell J., dissenting) ("The statute makes no distinction between tangible and intangible property.").

[203] United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991).

[204] *See* Dowling, 473 U.S. at 216 (noting that finding against defendant for the unauthorized use of radio recordings "would make theft . . . equivalent to wrongful appropriation of statutorily protected rights in copyright"); Brown, 925 F.2d at 1308 (noting that a "computer program itself is an intangible intellectual property, and as such, it alone cannot constitute [stolen goods] with the meaning of [the NSPA]"); *see also* United States v. Greenwald, 479 F.2d 320, 322 (6th Cir. 1973) (finding that theft of documents containing secret chemical formulations violates the NSPA); United States v. Seagraves, 265 F.2d 876, 878-80 (3d Cir. 1959) (stating that theft of geophysical maps identifying possible oil deposits would violate the NSPA). The stolen item need not remain "entirely unaltered." Dowling, 473 U.S. at 216 (citing United States v. Moore, 571 F.2d 154, 158 (3d Cir. 1978)).

[205] *See* Dowling, 473 U.S. at 216; Brown, 925 F.2d at 1307-09 & n.14. *Cf.* United States v. Riggs, 739 F. Supp. 414, 420-23 (N.D. Ill. 1990) (finding that an electronic transfer of proprietary business information violates 18 U.S.C. § 2314).

[206] *See* Dowling, 473 U.S. at 216; Brown, 925 F.2d 1301, 1307; *see also* Toren, *supra* note 29, at 69. *But see* United States v. Bottone, 365 F.2d 389, 393-94 (2d Cir. 1966) (upholding a NSPA conviction for copying instructions for manufacturing a drug even though petitioner did not use the victim's paper or equipment); Arkin, *supra* note 185, at 3 ("Where the 'stolen goods' in question are photocopies . . . it is certainly conceivable that the employee . . . might have criminal exposure.").

Another requirement of the NSPA is that the stolen property must be worth at least five thousand dollars.[207] Clearly, the value of stolen information must be greater than the paper on which it is printed; however, there is rarely a market to determine the value of proprietary information.[208] While the courts have not espoused a uniform approach to valuing trade secrets,[209] satisfying the monetary standard of $5,000 has not proven especially difficult for prosecutors.[210]

7.3.2. Wire Fraud and Mail Fraud Statutes

Federal wire and mail fraud statutes prohibit the use of the mails, wire, radio, or television to obtain money or "property" fraudulently.[211] The courts have interpreted "property" in this

---

[207] *See* 18 U.S.C.A. § 2314 (West 1994 & Supp. 1997).

[208] *See* Arkin, *supra* note 185, at 3. Arkin argues that using development costs or licensing prices is not a good substitute for a market valuation. *See id.* at 3, 6.

[209] *See* Toren, *supra* note 29, at 82.

[210] *See id.* at 84-85.

[211] The mail fraud statute reads:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses . . . places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any such matter or thing whatever to be sent or delivered by any private or commercial or interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned more than 30 years, or both.

18 U.S.C. § 1341 (1994). The wire fraud statute reads:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

context to include intangible property[212] and have upheld wire and mail fraud convictions without finding a violation of the NSPA.[213] Despite the courts' broad reading of "property," prosecutors have had difficulty winning wire and mail fraud convictions.[214] Theft of corporate secrets usually does not involve the use of mail or wire,[215] and proving intent to defraud can be difficult.[216]

7.4. Protection of Trade Secrets Under The Economic Espionage Act of 1996

On October 14, 1996, President Clinton signed into law the Economic Espionage Act of 1996 ("EEA" or the "Act").[217] The EEA makes misappropriation of trade secrets a federal crime and stipulates harsh penalties for economic espionage.[218] Congress passed the EEA to (1) protect trade secrets,[219] (2) give federal prosecutors greater leeway to prosecute economic espionage, and (3) make up for inadequate state laws.[220] In contrast to previous state and federal statutes, the EEA is specifically designed to give intangible property the same degree of protection as tangible

---

18 U.S.C. § 1343 (1994).

[212] *See, e.g.*, United States v. Carpenter, 484 U.S. 19, 26 (1987) ("Confidential business information has long been recognized as property."); United States v. Cherif, 943 F.2d 692, 697-98 (7th Cir. 1991) (holding that a bank's confidential information is property within the meaning of 18 U.S.C. § 1341); United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (finding that a computer software system can be considered "property").

[213] *See* Toren, *supra* note 29, at 85 & n.192; *see also* Abbott v. United States, 239 F.2d 310, 312-13, 315 (5th Cir. 1956) (upholding a mail fraud conviction but finding the National Stolen Property Act's provisions unmet).

[214] *See* S. REP. NO. 104-359, at 10 (1996).

[215] *See id. But see* Toren, *supra* note 29, at 90 ("[T]he requirement that the mail be utilized in the scheme to defraud has not been rigidly applied.").

[216] *See* S. REP. NO. 104-359, at 10; Arkin, *supra* note 185, at 6.

[217] *See* Statement by the President Regarding H.R. 3723 (Oct. 14, 1996), *in* M2 Presswire, *available in* LEXIS, News Library, Wires File.

[218] *See* 18 U.S.C.A. § 1832(a) (West Supp. 1997).

[219] Protecting trade secrets is the primary goal of the legislation. *See* Senator Kohl, *State's Rights* (Letter to the editors), NEW REPUBLIC, Feb. 24, 1997, at 4 ("Put simply, the Economic Espionage Act is a federal trade secrets law.").

[220] *See* Laurence H. Reece III & Peter M. Lefkowitz, *Recent Developments in Trade Secret Law*, MASS. L. WKLY., Apr. 14, 1997, at 11.

property.[221] Furthermore, the EEA can be enforced without use of the mail or wire or a minimum value of the loss. Finally, the misappropriation, unauthorized conversion, duplication, alteration, and destruction of a trade secret is prohibited as well as its outright theft.[222]

7.4.1. Definition of Trade Secrets

The Act defines trade secrets as all forms and types of information, both tangible and intangible, if (1) "the owner thereof has taken reasonable measures to keep such information secret; and [(2)] the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."[223] Both a cursory reading of the statute and congressional testimony indicate that this definition should be read broadly.[224] Information need not be novel to be considered

---

[221] *See* H.R. REP. NO. 104-788, at 11 (1996) ("The intent of this statute . . . is to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished.").

[222] A person is guilty under the EEA if he acts with the requisite intent and:

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more persons do any act to effect the object of the conspiracy.

18 U.S.C.A. § 1832(a)(1)-(5).

[223] 18 U.S.C.A. § 1839(3) (West Supp. 1997). This definition is similar to the definition in the UNI. TRADE SECRETS ACT §1, 14 U.L.A. 437, 437 (1990) ("'Trade Secret' means information . . . that: (i) derives independent economic value, actual or potential, from not being readily ascertainable by proper means . . . and (ii) is subject to efforts that are responsible under the circumstances to maintain its secrecy").

[224] *See* H.R. REP. NO. 104-788, at 4 (noting that the definition of trade secrets "includes, but is not limited to information such as production process,

a trade secret, although novelty may be relevant in determining whether information is known to the public.[225] Nevertheless, general knowledge cannot constitute a trade secret.[226]

On the other hand, the standard used to determine what "reasonable measures" the owner must undertake is not clear. While a House of Representatives report stated that a facts-and-circumstances evaluation would suffice, Senate testimony indicated that in addition to satisfying the facts-and-circumstances standard, all owners must demonstrate that they have taken some minimum security precautions.[227] Some trade secrets case law suggests that cost-benefit analysis is the proper framework.[228] Regardless, the statute suggests that owners do not need to devote extraordinary resources to safeguard their information for it to qualify as trade secrets.[229]

7.4.2. Prohibited Activities

A person is guilty under the EEA if, in addition to wrongfully controlling or copying a trade secret, he acted with intent to achieve one of two results.[230] First, to show that the defendant intended to commit economic espionage, the government must show that he sought or expected to "benefit" a foreign government, instrumentality,[231] or agent.[232] Aiding a private foreign

---

bid estimates, production schedules, computer software, and technology schematics").

[225] *See* 142 CONG. REC. 12,213 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl).

[226] *See* H.R. REP. NO. 104-788, at 13; 142 CONG. REC. 12,213 (daily ed. Oct. 2, 1996); *see also* James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 190 (1997) ("[P]ublic disclosure of a trade secret will terminate protection for it . . . .").

[227] *Compare* H.R. REP. NO. 104-788, at 12-13 *with* 142 CONG. REC. 12,213 (daily ed. Oct. 6, 1996) (Statement of Sen. Kohl).

[228] *See* Pooley, *supra* note 226, at 217 & n.204.

[229] A recent article argues that even "accidental disclosure under unpreventable or unforeseeable circumstances should not automatically destroy trade secrecy." *Id.* at 191.

[230] *See* 18 U.S.C.A. §§ 1831(a), 1832(a) (West Supp. 1997).

[231] The EEA defines a foreign instrumentality as "any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C.A. § 1839(1) (West Supp. 1997).

corporation does not fall under the economic espionage provision. A cursory reading of this section of the Act suggests that satisfying the "benefit" requirement could be difficult. For instance, an employee of a U.S. corporation that sold research plans to a state-owned foreign company might not expect the foreign company to reap any economic gain from the information. Nevertheless, legislative history indicates that "benefit" should be read broadly to include reputational, strategic, and tactical gains.[233] Thus in practice, the "benefit" requirement should be quite easy to satisfy, since foreign organizations should only pay for information if they expect to obtain some gain, however elusive.

Alternatively, a person is guilty under the EEA if he or she misappropriates a trade secret.[234] The government must show that the actor intended: (1) that the stolen trade secret would be an "economic benefit" to someone other than the owner,[235] and (2) that the theft would disadvantage the rightful owner.[236] Furthermore, the trade secret must be related to a product — but not a service[237] — placed in interstate or international commerce.[238] The Act does not define "economic benefit";[239] however, legislative history indicates that abstract or reputational benefits are not economic benefits.[240] Thus, an "economic benefit" is a "benefit," but not vice versa. Unlike the economic espionage section, the government must also show that the trade

---

[232] 18 U.S.C.A. § 1831(a). The EEA defines a foreign agent as "any officer, employee, proxy, servant, delegate, or representative of a foreign government." *Id.* § 1839(2).

[233] *See* H.R. REP. NO. 104-788, at 11 (1996).

[234] See 18 U.S.C.A. § 1832(a).

[235] The EEA defines the owner of a trade secret as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed." 18 U.S.C.A. § 1839(4) (West Supp. 1997).

[236] *See* 18 U.S.C.A. § 1832(a).

[237] Exclusion of trade secrets related to services is one of the more curious features of the EEA, given the legislation's expansive definition of trade secrets. Despite this apparent shortcoming, one commentator suggests that the theft of any tangible item provided in connection with a service should satisfy the EEA. *See* Ronald Abramson, *Economic Espionage Act of 1996*, N.Y.L.J., Apr. 28, 1997, at S6.

[238] *See* 18 U.S.C.A. § 1832(a).

[239] This author hypothesizes that economic benefits would include information that, if properly used, would increase profits, revenues, returns on investment, stock prices, or credit ratings of the acquiring firm.

[240] *See* H.R. REP. NO. 104-788, at 11 (1996).

secret is related to interstate commerce and that the actor had reason to believe that the misappropriation would harm the rightful owner.[241] Neither requirement should be hard to meet.

The Economic Espionage Act should be a powerful tool in the battle against economic espionage. The EEA criminalizes many formerly legal activities that were thought to be very harmful. All of those potentially involved in economic espionage fall under the purview of the EEA: employees who steal information via computer, fax or paper; middlemen who purchase the information to be resold; foreign agents who purchase the information; foreign companies that receive the information; "hackers" who steal information by breaking into companies' computer systems; those who spy on or break into companies offices; specialized technical operators;[242] and foreign graduate students supplying their home country with research data. While some have expressed concern over holding an employer responsible for an employee's violation of the EEA,[243] such liability is consistent with the common law rule of respondeat superior[244] and should encourage corporations

---

[241] *See* 18 U.S.C.A. § 1832(a).

[242] See *supra* text accompanying notes 92-97 for an explanation of specialized technical operations.

[243] *See* 142 CONG. REC. S12,202-03, 12,213 (daily ed. Oct. 2, 1996). As the text accompanying note 263, *infra*, describes, organizations involved in trade secret theft and economic espionage may be fined up to five and ten million dollars, respectively.

[244] In explaining respondeat superior, the Virginia Supreme Court stated:

> In order to hold an employer liable for its employee's act under the doctrine of *respondeat superior*, an injured party is required to establish that the relationship of master and servant existed at the time and with respect to the specific action out of which the injury arose. . . . An act is within the scope of the employment relationship if (1) it be something fairly and naturally incident to the business, and (2) if it be done while the servant was engaged upon the master's business and be done, although mistakenly or ill-advisedly, with a view to further the master's interests, or from some impulse or emotion which naturally grew out of or was incident to the attempt to perform the master's business, and did not arise wholly from some external, independent, and personal motive on the part of the servant to do the act upon his own account.

Smith v. Landmark Communications, Inc., 306 S.E.2d 306, 307-08 (Va. 1993) (citations omitted).

Holding a company liable for an employee's stealing a trade secret comports with respondeat superior. First, the development and acquisition of trade secrets is a natural function of most businesses. Second, an employee is most likely to steal a trade secret to further his employer's business. On the

to ensure that their employees uphold the law.

Despite the broad prohibitions of the EEA, there are several important limits to its reach. First, the EEA does not inhibit the natural flow of employees among companies or the ability of employees to start their own businesses.[245] Taking advantage of knowledge gained through employment, if not stolen or misappropriated, does not fall under the purview of the EEA.[246] Second, parallel development of trade secrets does not violate the EEA.[247] Companies may develop the same technology concurrently or at different times.[248] Third, reverse engineering[249] does not violate the EEA per se.[250] Although some commentators have expressed concern that the EEA may prohibit some reverse engineering,[251] nowhere does the legislative history reflect a desire to limit such activity.[252] Congress intended to cast a wide net for trade secret theft but did not intend to transform legitimate business activities into crimes. Fourth, the EEA does not cast its net so wide as to make open-source data collection illegal.[253] For example, foreign governments may still use the FOIA without fear of prosecution. Fifth, the EEA does not affect a foreign buyout of or merger with an American corporation in

---

other hand, if the trade secret is patently useless to the employer, the second prong is probably not met and liability should not be imposed on the employer.

[245] *See* 142 CONG. REC. 12,213 (daily ed. Oct. 2, 1996); Reece & Lefkowitz, *supra* note 220, at 11.

[246] *See* 142 CONG. REC. 12,213 (daily ed. Oct. 2, 1996). Using acquired trade secrets may, however, violate confidentiality arrangements, noncompetition covenants, or other contractual agreements with one's former employer.

[247] *See id.* at 12,212.

[248] *See id.*

[249] Reverse engineering is "a method of industrial engineering in which one begins with a known finished product and works backward to divine the processes and specifications involved in the product's development and manufacture." Rockwell Graphic Sys., Inc. v. DEV Indus., 91 F.3d 914, 917 n.3 (7th Cir. 1996) (citations omitted).

[250] *See* 142 CONG. REC. S12,212-13 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl).

[251] *See, e.g.*, Pooley, *supra* note 226, at 195.

[252] *See, e.g.*, 142 Cong. Rec. S12212-13 (statement of Sen. Kohl) ("If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent or [the EEA], then that form of 'reverse engineering' should be fine.").

[253] See *supra* text accompanying notes 120-123 for an explanation of open source data collection.

order to acquire its trade secrets. Such a purchase would not involve "the theft, unauthorized appropriation or conversion, duplication, alteration, or destruction of a trade secret,"[254] as required by the EEA.

7.4.3. Confidentiality Provision

In order to encourage owners of trade secrets to cooperate with prosecutors,[255] Congress included a provision in the EEA to ensure the confidentiality of proprietary information.[256] Nonetheless, courts hearing cases under the EEA may only protect the privacy of any information revealed to the extent permitted by the relevant rules of procedure.[257] In addition, all grand jury proceedings, including those necessary to bring charges under the EEA, are closed to the public. Even before a U.S. Attorney convenes a grand jury, he may seek a federal court order authorizing the FBI to tap or intercept both oral and electronic communications related to the suspect's trade secret theft.[258] Furthermore, a U.S. Attorney may seek an injunction to prevent the dissemination of stolen trade secrets[259] without the delay present in other civil actions.[260]

---

[254] *See* H.R. REP. NO. 104-788, at 11 (1996).

[255] *See id.* at 13.

[256] "[T]he court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C.A. § 1835 (West Supp. 1997).

This provision is considerably less detailed and provides greater flexibility to judges than does the Classified Information Procedures Act ("CIPA"). Classified Information Procedures Act (CIPA), 18 U.S.C. App. §§ 1-22 (1997). CIPA was designed "to confront the problem of a criminal defendant who threatens to reveal classified information during the course of his trial in the hope of forcing the government to drop the criminal charge against him." United States v. Fernandez, 887 F.2d 465, 466 (4th Cir. 1989) (quotation omitted). It remains to be seen if the courts will use CIPA as a guide for protecting trade secrets at trial.

[257] *See* H.R. REP. NO. 104-788, at 13.

[258] *See* Neal R. Brendel & Lucas G. Paglia, *The Economic Espionage Act*, PA. L. WKLY., July 7, 1997, at 12.

[259] *See* 18 U.S.C.A. § 1836(a) (West Supp. 1997) (permitting the Attorney General in a civil action "to obtain appropriate relief against any violation of this section").

[260] *See* Brendel & Paglia, *supra* note 258, at 12.

7.4.4. Penalties

The EEA provides for fines and prison terms for offenders. Under the trade secrets provision, the maximum sentence is ten years in prison and a fine determined according to the provisions of title twenty-eight.[261] Under the economic espionage section, the maximum sentence is fifteen years in prison and a half million dollar fine.[262] If an organization violates the EEA, the maximum fine rises to five million dollars for trade secrets theft and ten million dollars for economic espionage.[263]

In addition to prison terms and monetary fines, the EEA contains a forfeiture provision.[264] Under this section, proceeds from violating the EEA, as well as property used to commit the offense, may be forfeited to the federal government.[265] The Attorney General then has the authority to return the forfeited property to the rightful owner.[266] The forfeiture clause provides a strong incentive not to steal trade secrets or engage in economic espionage. Monetary fines alone may be inadequate to deter organizations from trade secret theft where the pilfered trade secrets are worth more than the penalty; however, penalizing an offending person or organization by an amount equal to the gains from misappropriation ensures that offenders will not profit from

---

[261] *See* 18 U.S.C.A. § 1832(a).

[262] *See id.* § 1831(a).

[263] *See id.* §§ 1831(b), 1832(b).

[264] The forfeiture provision reads in part:

> The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States—
> (1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
> (2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

Id. § 1834(a).

[265] *See id.*

[266] *See* 142 CONG. REC. S12,201-03, 12,213 (daily ed. Oct. 2, 1996).

their crime.[267]

7.4.5. Civil Actions

The EEA also empowers the Attorney General to commence civil proceedings to enjoin violations,[268] pursuant to the standards for injunctive relief set by the Federal Rules of Civil Procedure.[269] Conspicuously absent from the EEA is a private cause of action for trade secret theft; nevertheless, the EEA should reduce the burden on victims to recover damages. A conviction under the EEA may carry evidentiary weight in a subsequent civil action.[270] Therefore, corporations, with the aid of the FBI and Department of Justice, should be able to prove trade secret theft without the expenses inherent in a civil action.[271]

7.4.6. Territorial Reach

The EEA has a very broad territorial reach. The EEA applies to conduct outside the United States so long as the conduct is in furtherance of a crime that occurred in the United States.[272] Thus, acts of economic espionage against U.S. corporations abroad – some of the most common targets[273] – violate the EEA. In addition, economic espionage between two foreign nations would also fall under the jurisdiction of the EEA if any part of the crime occurred in the United States or involved a

---

[267] This discussion is a bit simplified. A company will steal trade secrets if the expected gains from the theft are greater than the expected losses. In other words, if the gains from a successful theft times the expectation of success are greater than the resulting harm from being caught times the chance of being caught, then an organization will attempt to steal trade secrets. The forfeiture clause affects this equation by increasing the harm resulting from being caught; consequently, companies will have less incentive to engage in trade secret theft.

[268] The civil proceedings section reads:

> (a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.
> (b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

18 U.S.C.A. § 1836.

[269] *See* H.R. REP. NO. 104-788, at 14 (1996).

[270] *See* Brendel & Paglia, *supra* note 258, at 12.

[271] *See id.*

[272] *See* 18 U.S.C.A. § 1837.

[273] *See Hearing on Econ. Espionage, Tech. Transfers and Nat'l Sec. Before the Joint Econ. Comm.*, 104th Cong., 1st Sess. (1997) (statement of John Fialka).

United States citizen or permanent resident alien.[274]

7.4.7. Early Results of the Economic Espionage Act of 1996

By the time of publication, two groups had been charged in actions arising under the EEA. In the first, an employee was accused of stealing computer diskettes, blueprints, research and other materials from his employer, PPG Industries.[275] When he and his brother attempted to sell the trade secrets to a competitor,[276] the competitor alerted PPG Industries, which informed the FBI.[277] Both brothers pleaded guilty to stealing trade secrets.[278] The employee received fifteen months in jail and three years probation, and his brother received five years probation.[279] Consistent with the confidentiality provision of the EEA, the District Court placed documents related to the relevant trade secrets under seal throughout the proceedings.[280]

In the second case, two Taiwanese individuals were indicted for allegedly trying to steal trade secrets related to the manufacture of the anti-cancer drug Taxol from Bristol-Myers Squibb Company ("BMS").[281] The accused hired an FBI agent, posing as a technology broker, to purchase information from a BMS executive posing as a corrupt BMS scientist.[282] The arrests came after a two year operation, allegedly culminating in the purchase of trade secrets from the BMS employee who cooperated with the FBI.[283] The individuals were charged with conspiracy and attempt to steal trade secrets, among other crimes.[284]

These two cases may offer some insight into the future

---

[274] *See* 18 U.S.C.A. § 1837.

[275] *See 15 Months for Selling Secrets*, PITT. POST-GAZETTE, June 6, 1997, at C3.

[276] *See id.*

[277] *See id.*

[278] *See id.*

[279] *See id.*

[280] *See* Brendel & Paglia, *supra* note 258, at 12.

[281] *See FBI Charges Taiwanese Tried to Steal Taxol Trade Secrets from BMS*, ANDREWS INTELL. PROP. LITIG. REP., June 18, 1997, at 3.

[282] *See id.*

[283] *See id.*

[284] *See Two Taiwan Men Among Suspects in Trade Secrets Case*, AGENCE FRANCE PRESSE, July 10, 1997, *available in* LEXIS, News Library, Curnws File.

enforcement and deterrent value of the EEA. It does not appear that the U.S. government will only use the EEA to prosecute theft implicating national security.[285] In both cases, individuals attempted to steal trade secrets without the aid of a foreign government. As a result, we have yet to see an act of economic espionage prosecuted under the EEA. Some commentators have criticized the light sentences in the PPG case and contend that such sentences are likely in other cases as well.[286] Moreover, the federal sentencing guidelines are likely to be lenient because white-collar defendants are usually first-time offenders.[287]

There are early indications that foreign companies and officials are attempting to comply with the EEA. To facilitate compliance, the FBI has offered to brief representatives of foreign companies about the EEA.[288] Also, the Department of Justice is preparing guidelines for foreign companies to warn them about acts that would lead to prosecution under the EEA.[289]

8. RECOMMENDATIONS

Although the federal government has taken strong action to check economic espionage in the last few years, both the government and the private sector can do more. First, Washington should punish the most egregious cases of economic espionage with strong diplomatic action. In the past, the United States has simply asked spies caught stealing trade secrets to leave the country quietly.[290] While this may have been necessary during the Cold War to maintain the western alliance,[291] no such need exists today. The United States can now afford to confront its

---

[285] *But see* Charles M. Sennott et al., *Business of Spying*, STAR TRIB. (Minneapolis-St. Paul), Feb 4, 1997, at 1D ("Will the FBI and the Justice Department really devote resources to this? . . . My hunch is they won't, unless it involves theft of major trade secrets with national security implications."(internal quotes omitted)).

[286] *See also* Stan Crock & Jonathan Moore, *Corporate Spies Feel a Sting*, BUS. WK., July 14, 1997, at 76 (quoting an observer as saying that "companies that want to see people suffer greatly are going to be disappointed").

[287] *See id.* at 77.

[288] *See* Gene Koprowski, *DOJ, FBI Bear Down on International Cybercrime*, DEF. WK., Mar. 10, 1997, *available in* LEXIS, News Library, Curnws File.

[289] *See id.*

[290] *See The Growth of Economic Espionage*, *supra* note 7, at 14.

[291] *See* FRIENDLY SPIES, *supra* note 12, at 6.

allies regarding their economic espionage activities. A potential fallout in relations with an ally does not have the national security implications of the past.

The United States has numerous diplomatic options to punish offenders: treating apprehended foreign agents the same as Soviet spies of the past, rather than as friendly diplomats that have erred;[292] severing research agreements and denying access to U.S. labs;[293] severing joint intelligence operations;[294] withholding access to the U.S. market and government contracts; and expelling diplomats publicly. Diplomatic punishment may be especially useful when criminal or civil action is unlikely or inadequate, such as when the FBI catches foreign diplomats attempting to steal trade secrets from a U.S. corporation. Criminal charges would be impossible in such a situation because of the diplomat's immunity from prosecution. In addition, the corporation could not recover damages because no theft took place. In such an instance, the White House should penalize the offending nation; otherwise, the offending nation would not be discouraged from illegal information gathering in the future.

Second, counterintelligence and law enforcement bodies need to coordinate their activities and develop an overall strategy for preventing economic espionage. A NACIC report to Congress noted that counterintelligence and law enforcement groups usually fail to work together and that previous interagency committees failed to harmonize the agencies' efforts.[295] Senator Cohen summarized the government's effort against economic espionage as "chaotic and largely ineffective."[296] Given that almost ten executive agencies are involved in preventing and countering economic espionage,[297] the need to coordinate activities is great.

Third, United States counterintelligence services should provide more information about economic espionage to the

---

[292] *See* 142 CONG. REC. S12,201-03, S12,208.

[293] *See* Amy Borrus, *Why Pinstripes Don't Suit the Cloak-and-Dagger Crowd*, BUS. WK., May 17, 1993, at 39, 39.

[294] After Jonathan Pollard was arrested in 1985 for spying for Israel, the United States temporarily suspended intelligence sharing with Israel. *See* Bill Gertz, *Spying for Friendly Nations Can Also Help Foes*, WASH. TIMES, Sept. 26, 1996, at A13.

[295] *See Annual Report*, *supra* note 88.

[296] 142 CONG. REC. S377, S378 (daily ed. Jan. 25, 1996).

[297] *See supra* section 6.

private sector so that the private sector can better protect itself. The CIA has discovered foreign governments spying on U.S. industry for years but has rarely informed the target companies.[298] Federal agencies need to overcome their fear of engaging in industrial policy and educate the private sector. Even former CIA director, James Woolsey, suggested that the CIA should help U.S. companies combat industrial espionage and provide information on economic trends.[299] ANSIR and the OSAC are examples of agencies already working closely with the private sector.[300] The U.S. intelligence network should not, of course, become a private security consultant; however, when counterintelligence uncovers a foreign government spying on U.S. industry, the targeted companies should be informed.

Fourth, the private sector needs to recognize and take precautions against the danger of economic espionage. Corporate executives are often unaware of economic espionage or the need to counter it.[301] Fewer than five percent of major U.S. companies have an intelligence division.[302] Even victimized companies may remain naïve, believing that their past losses were just isolated incidents.[303]

The private sector must also take steps to protect proprietary information. One industry survey found that many U.S. corporations do not have formal programs for protecting trade secrets.[304] A consultant specializing in counterespionage stated that "[a]n alarming number of companies seem to have resigned themselves to the loss of their trade secrets."[305] Corporate managers have a duty to shareholders to safeguard the company's assets, and as noted previously, trade secrets are often a large

---

[298] *See* Borrus, *supra* note 293, at 39.

[299] *See* Jim Mann, *Woolsey Cites Dangers in Economic Espionage Intelligence: U.S. Will Have Clear Policy to Govern, and Defend Against, Such Activity, CIA Nominee Says*, L.A. TIMES, Feb. 3, 1993, at A10.

[300] See *supra* sections 6.1 & 6.7 for a discussion of ANSIR and the OSAC.

[301] *See* Perry, supra note 79. *But see* FRIENDLY SPIES, *supra* note 12, at 260 ("It does not appear that American businesses are unaware of the espionage carried out around them.").

[302] *See* Perry, *supra* note 79.

[303] *See* FRIENDLY SPIES, *supra* note 12, at 260.

[304] *See* Heffernan, *supra* note 28 ("The recent A.S.I.S. report revealed that only three-quarters of the responding companies have formal programs for safeguarding proprietary information.").

[305] Perry, *supra* note 79.

component of a corporation's value.[306] Organizations should also take reasonable measures to ensure that their proprietary information is considered trade secrets under the EEA.[307]

Finally, Congress should increase appropriations to counter economic espionage. Despite the end of the Cold War, traditional espionage threats continue.[308] In addition, the intelligence community must now confront economic espionage. Current funding may be adequate to address spying by traditional enemies because the intelligence community is already familiar with those countries' intelligence operations.[309] Present outlays may not, however, be sufficient to investigate the activities of friendly countries spying on the United States because U.S. law enforcement has little experience investigating these countries' intelligence operations.[310] In addition, enforcement of the Economic Espionage Act of 1996 may require additional funding.[311]

---

[306] *See id.* (noting that failure to take appropriate measures may "[a]ccording to emerging legal thinking . . . actually border on managerial and fiscal irresponsibility" and that the "[f]ake the loss and move on approach is becoming increasingly unacceptable to shareholders [and others] who must bear the losses").

[307] Means of protecting trade secrets include: instituting a company counterintelligence program; requiring executives to attend FBI counterintelligence training; developing security policies regarding confidential information; using encryption devices; screening job applicants for security risks; using security features contained in office equipment; requiring employee nondisclosure and non-compete agreements; implementing visitor controls; restricting copier use; shredding sensitive materials, monitoring e-mail; and working with state and federal law enforcement authorities. *See generally Security and Freedom Through Encryption (Safe) Act: Hearing on H.R. 3011 Before the House of Representatives Comm. on the Judiciary*, 104th Cong. 17, 18 (1996) (statement of Hon. Bob Goodlatte) (noting that strong encryption will allow U.S. businesses to protect themselves against the threat of economic espionage); FRIENDLY SPIES, *supra* note 12, at 308 (advocating government training of U.S. business executives travelling overseas in counterintelligence techniques); Michelle Cole, *Psst! Wanna Sell a Secret? Spies are Even in Boise Now*, IDAHO STATESMAN, Apr. 28, 1997, at 10B (advocating a variety of measures that companies can use to foil espionage); Denine Phillips, *Secure the Area!*, OFFICE SYSTEMS, May 1997, at 36 (advocating the use of standard protection features as well as more sophisticated encryption techniques); Perry, *supra* note 79.

[308] *See* Shapiro, *supra* note 130, at 221 (observing that the "classic type of espionage is not a relic of the past").

[309] *See Annual Report*, *supra* note 88.

[310] *Cf. id.*

[311] The Congressional Budget Office has estimated that the EEA would require three million dollars in additional discretionary spending over the 1997-

9. CONCLUSION

After the Cold War, many foreign intelligence services that had previously focused on the Soviet Union began spying on U.S. corporations. What is perhaps most surprising about this problem is that many traditional allies of the United States were involved. Foreign governments were using many of the same data-gathering methods against U.S. organizations as they had against the former Soviet Union. Although estimates are tenuous, the subsequent losses were likely in the tens of billions of dollars annually.

Both state and federal laws were grossly inadequate to prosecute misappropriation of trade secrets. Those caught stealing proprietary information often could not be prosecuted because no law had been broken. Successful prosecutions resulted from the handful of states with laws protecting trade secrets and from federal laws that were originally designed to prevent other forms of theft.

Within a matter of years, however, both the executive and legislative branches of the government took strong action to catch and prosecute those engaged in economic espionage. Congress passed the Economic Espionage Act of 1996, which, for the first time specifically outlawed economic espionage and protected trade secrets at the federal level. Even before this law was in place, several executive agencies had developed counterintelligence programs to deal specifically with economic espionage. More can be done to prevent economic espionage; however, the federal government has laid the groundwork for a successful war on economic espionage.

2002 period. *See* H.R. REP. NO. 104-788 (1996).