PERSEREC

Technical Report 05-10
May 2005

Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage

Lisa A. Kramer
Defense Personnel Security Research Center

Richards J. Heuer, Jr.
RJH Research

Kent S. Crawford
Defense Personnel Security Research Center

Approved for Public Distribution:
Distribution Unlimited

Research Conducted by
Defense Personnel Security Research Center

Technical Report 05-10 **May 2005**

Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage

Lisa A. Kramer
Defense Personnel Security Research Center

Richards J. Heuer, Jr.
RJH Research

Kent S. Crawford
Defense Personnel Security Research Center

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
16-05-2005	Technical	2005 – 2009

4. TITLE AND SUBTITLE

Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lisa A. Kramer
Richards J. Heuer, Jr.
Kent S. Crawford

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 05-10

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Personnel Security Research Center
99 Pacific Street, Suite. 455-E
Monterey, CA 93940-2497

10. SPONSORING/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study explores ten technological, social, and economic trends in the United States and globally that are serving to increase opportunity and motivation for espionage. Findings suggest that American "insiders" have an unprecedented level of access to classified and proprietary information due to technological advances in information storage and retrieval. American employees have greater opportunity to establish contact with foreign entities and to transfer information to them through traveling internationally more often and by participating in international research and business ventures more frequently. Internet use is expanding globally and computer-users are becoming more culturally and linguistically diverse. The Internet can now be used to transmit massive amounts of digitized information to multiple foreign parties simultaneously. Finally, the market for U.S. information is expanding. American insiders can sell more types of information to a broader range of foreign buyers than ever before. In addition to these new opportunities for espionage, American employees are more often encountering situations that can provide motivation for this crime. More insiders are experiencing financial problems and gambling addiction, both of which can provide impetus for workplace theft. Loyalty to organizations is diminishing and a greater proportion of American workers are at risk for becoming disgruntled. A growing number of insiders have emotional and financial ties to other countries. Under some circumstances, insiders with loyalties to other peoples may be less inclined to view espionage as morally wrong. It is possible that some insiders with a global orientation to world affairs will view espionage as morally justifiable if they feel that sharing information will benefit the "world community" or prevent armed conflict.

15. SUBJECT TERMS

espionage, insider, IT systems, Internet, financial problems, organizational loyalty, foreign influence, globalization

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR	46	James A. Riedel, Director (831) 657-3000

Preface

Most open-source literature that explores the phenomenon of insider espionage consists of journalistic accounts, biographical works, case studies of individual spies, and memoirs of intelligence officer defectors. As an organization responsible for systematic research on personnel security, PERSEREC occasionally applies social science methods to the study of espionage. We recently published *Espionage Against the United States by American Citizens: 1947-2001*, a documentation of statistical analyses conducted with a large unclassified dataset of espionage cases. PERSEREC researchers have published an anthology of significant studies of insider espionage entitled *Citizen Espionage: Studies in Trust and Betrayal,* and a comprehensive literature review entitled *Temperament Constructs Related to Betrayal of Trust*. Soon, PERSEREC will publish *Counterintelligence Reporting Essentials,* a guide to identifying behaviors in the workplace that are of counterintelligence concern and which should be reported by coworkers and supervisors.

Building upon findings of previous research, the current study explores insider espionage from an especially broad perspective by examining factors that are relevant to prevalence of espionage. Rather than analyzing psychological factors that influence an individual's decision to spy, this study examines situational factors that affect the frequency with which insider espionage will occur. The technological, social, and economic trends explored in this study suggest that greater numbers of American employees have opportunity to commit espionage and are more often encountering situations that may motivate them to commit this crime.

The factors explored in this study are relevant to espionage involving the theft of classified as well as proprietary information, and pertain primarily to the illicit transfer of material to foreign rather than domestic recipients. Because this study presents data gathered from open sources, this report is unclassified. It is our hope that this publicly available document will be of value to those who are interested in U.S. vulnerability to insider espionage, but who do not have access to classified espionage research.

James. A. Riedel
Director

Executive Summary

Permanent and temporary employees, vendors, contractors, suppliers, ex-employees, and other types of "insiders" are among those who are most capable of exploiting organizational assets at greatest expense to U.S. interests. Due to their knowledge of the public agencies and private companies that employ them, their familiarity with computer systems that contain classified and proprietary information, and their awareness of the value of protected information in the global market, insiders constitute a significant area of vulnerability for national security.

Using a methodology similar to that employed in epidemiological studies where scientists explain or forecast changes in prevalence of certain diseases, this study examines prevalence of insider espionage. The medical researcher knows that heart disease is associated with age, weight, amount of exercise, blood pressure, diet, stress, genetics, and other factors, and can thus predict changes in the pervasiveness of heart disease by analyzing changes in these variables. Similarly, because we know that opportunity and motivation come together to create the crime of espionage, we can forecast changes in the prevalence of insider espionage by analyzing trends that influence opportunity and motivation for spying. As the medical researcher can identify higher risk groups but cannot predict which specific individuals will develop heart disease, we can make observations regarding U.S. vulnerability to insider espionage but cannot predict exactly which insiders will engage in this crime.

Findings of this study suggest that the information revolution, global economic competition, the evolvement of new and nontraditional intelligence adversaries, and other changes in the domestic and international environment have converged to create unusually fertile ground for insider espionage. Primary findings of this research are as follows:

- Technological advances in information storage and retrieval are dramatically improving insiders' ability to access and steal classified and proprietary information.

- The global market for protected U.S. information is expanding. American insiders can sell more types of information to a broader range of foreign buyers than ever before.

- The internationalization of science and commerce is placing more employees in a strategic position to establish contact with foreign scientists, businesspersons, and intelligence collectors, and to transfer scientific and technological material to them.

- The increasing frequency of international travel is creating new opportunity for motivated sellers of information to establish contact with, and transfer information to, foreign entities. Foreign buyers have greater opportunity to contact and assess the vulnerabilities of American personnel with access to protected information.

- Global Internet expansion is providing new opportunities for insider espionage. The Internet allows sellers and seekers of information to remain anonymous and provides means by which massive amounts of digitized material can be transmitted to foreign parties in a secure manner.

- Americans are more vulnerable to experiencing severe financial crisis due to aggressive consumer spending habits and other factors. Financial problems are a common source of motivation for insider espionage.

- The increasing popularity of gambling and prevalence of gambling disorders suggests that greater numbers of insiders will commit workplace crimes such as espionage to pay off debts and to sustain gambling activities.

- Because organizational loyalty is diminishing, fewer employees may be deterred from committing espionage due to a sense of obligation to the agencies and companies that employ them. Changing conditions in the American workplace suggest that greater numbers of insiders may become motivated to steal information from employers to exact revenge for perceived mistreatment.

- More insiders now have ethnic ties to other countries, communicate with friends and family abroad, and interact with foreign businesspersons and governments. Foreign connections provide insiders with opportunity to transfer information outside the United States, and foreign ties can provide motivation for doing so.

- More Americans view human society as an evolving system of ethnically and ideologically diverse, interdependent persons and groups. While this is highly beneficial in innumerable respects, it is also possible that some insiders with a global orientation to world affairs will, under extreme circumstances, view espionage as morally justifiable if they feel that sharing information will benefit the "world community."

While described separately for discussion purposes, the trends discussed in this study are converging and interacting with one another to create an insider espionage risk that can be described as greater than the sum of its parts. The vulnerabilities created by each trend are magnified by the negative effects of the others. The fact that these trends will interact with one another—*are* interacting with one another—suggests we are at greater risk for experiencing insider espionage than in previous decades. In this analysis we did not identify a single countervailing trend that will make insider espionage more difficult or less likely in the immediate future.

The trends explored in this research indicate that mitigating U.S. vulnerability to insider espionage will increasingly require the orchestrated efforts of personnel security,

information security, and counterintelligence professionals. Improved personnel security screening can reduce the number of potential espionage offenders, more rigorous information security measures can reduce the vulnerability of computer systems, and more effective counterintelligence operations will limit the damage that insider spies can inflict by detecting their activities sooner.

By denying access to insiders whose backgrounds suggest they are at risk for engaging in unreliable, untrustworthy, or disloyal behavior, personnel security measures provide an essential safeguard against the loss of classified and proprietary information. For this reason, personnel security policies and practices must be improved. However, even a more effective personnel security system will not fully eliminate the insider espionage threat. Owing to the inherent difficulty of predicting human behavior, it will never be possible to identify all individuals who, under certain circumstances, will choose to steal classified and proprietary information. Because we will always have insiders in our midst who, unbeknownst to us have become sufficiently motivated to commit espionage, we must consider the extent to which these insiders have opportunity to do so.

It is too frequently assumed that information contained within large databases and computer networks is secure because authorized users (sometimes thousands of users) have security clearances. Unfortunately, neither the clearance process nor other personnel security countermeasures can offer this type of guarantee. People change in response to situations they encounter in their personal and professional lives. Lessons learned from the post-World War II history of espionage illustrate the fact that not all insiders who are reliable and trustworthy at the time they are granted a position of trust, will remain so. For this reason, American organizations must protect intellectual assets by reducing opportunity for information theft. Findings of this study suggest that American organizations within government and industry must better control access to, and track the use of, digitized proprietary and classified files.

Table of Contents

List of Tables

List of Figures

Introduction

Permanent and temporary employees, vendors, contractors, suppliers, ex-employees, and other types of "insiders" are among those who are most capable of exploiting organizational assets at greatest expense to U.S. interests. Due to their knowledge of the public agencies and private companies that employ them, their familiarity with computer systems that contain classified and proprietary information, and their awareness of the value of protected information in the global market, insiders constitute a significant area of vulnerability for national security (Fialka, 1997; Freeh, 1996; Nockels, 2001; Shaw, Ruby, & Post, 1998; Thurman, 1999; Venzke, 2002). An estimated 2.4 million insiders have access to classified information currently, and while difficult to approximate, insiders with access to proprietary and sensitive technological information are likely to number in the tens of millions (National Security Institute, June 2002). While the deliberate compromise of classified or proprietary information to foreign entities is a relatively rare crime, even one case of insider espionage can cause extraordinary damage to national security.

Because espionage is a secret activity, we cannot know how many undiscovered spies are currently active in American organizations, or what the future will bring in terms of discovered espionage cases. Nevertheless, we are not entirely in the dark when assessing the magnitude of the insider espionage threat. We can draw inferences from relevant changes in technology, society, and the international environment that affect opportunity and motivation for spying.

Approach

In exploring current and future prevalence of insider espionage, this study employs an approach similar to that used in epidemiological research where scientists explain or forecast changes in the prevalence of disease within a population. The medical researcher knows, for example, that heart disease is associated with age, weight, amount of exercise, blood pressure, diet, stress, genetics, and other factors, and can thus estimate pervasiveness of heart disease by analyzing changes in these variables. Similarly, because we know that certain factors influence the likelihood that insider espionage will occur, we can forecast changes in the frequency of insider espionage by analyzing trends that influence these factors.

Opportunity for espionage consists of access to classified or proprietary information that can be exchanged for money or other benefits, access to foreign entities interested in obtaining this information, and means for transferring this information to foreign recipients. Motivation, broadly defined, is a feeling or state of mind that influences one's choices and actions. While motivation for espionage results from a complex interaction between personality characteristics and situational factors (Crawford & Bosshardt, 1993; Eoyang, 1994; Sarbin, 1994; Parker & Wiskoff, 1991; Shaw, Ruby & Post, 1998; Timm, 1991), this study focuses primarily on the latter. Despite the significance of individual characteristics in determining which insiders will commit espionage, if more insiders are encountering situations that can provide motivation for espionage, more insiders could

become sufficiently motivated to spy. If greater numbers of motivated insiders also have opportunity for espionage, as the findings of this study indicate, it is logical to conclude that U.S. vulnerability to insider espionage is increasing.

Part I
Trends That Affect Opportunity for Insider Espionage

Part I of this study explores five technological, social, and economic trends that are resulting in greater opportunity for insider espionage: technological advancements in information storage and retrieval, increasing global demand for protected U.S. information, the internationalization of scientific research and commerce, the increasing frequency of international travel, and global Internet expansion.

A. Technological Advancements in Information Storage and Retrieval

Technological advances in information storage and retrieval are making it increasingly difficult to control access to classified and proprietary information. The same characteristics of information technology (IT) systems that are improving employee productivity are serving to enhance an insider's capacity to gather information for foreign entities. Two specific IT advancements have particularly dramatic implications with respect to insider espionage: the development of large, networked databases with automated search functions and the miniaturization of mass data-storage devices.

Emergence of Searchable Databases

Large, networked databases are becoming more prevalent in organizations. Because greater numbers of employees have access to networked systems, and because these systems can be searched electronically for very specific kinds of data, malicious insiders are now often highly equipped to procure information that is of value to foreign entities. While the vast majority of employees do not exploit organizational IT systems for personal gain, those who choose to do so are now armed with technologies that make them particularly effective in this capacity.

Aldrich Ames, a veteran employee of the CIA, obtained information for Soviet intelligence officers by searching large digitized datasets. "For the KGB it was rather like subscribing to a new and highly classified database called CIA Online," writes David Wise (1995, p. 55). CIA officer Harold Nicholson obtained U.S. intelligence information on Chechnya for Russian operatives by surfing large organizational databases that he had no legitimate need to access. Air Force veteran Brian Regan searched *Intelink*, a classified government database of intelligence documents, to gather information pertaining to military preparedness of China, Iran, Iraq, and Libya. Among other information, Regan obtained the coded coordinates of Iraqi and Chinese missile sites. *Intelink* is estimated to have over 50,000 users with access to Sensitive Compartmented Information and is housed on over 200 servers at over 100 different physical sites. Another 265,000 *Intelink* users have access at the lower, Secret level (Poulson, 2001; Whitelaw & Enrich, 2001).

Miniaturization of Data Storage Devices

In addition to improving an employee's ability to locate specific types of classified and proprietary information, IT advances are making it easier for insiders to physically remove information from organizations. Data-storage devices that once held between 100 and 200 megabytes of data per cartridge now store 20 gigabytes or more. Hard-card storage systems no larger than credit cards now hold up to 8 gigabytes of data—the equivalent of the hard-drive contents of an average office desktop computer system (Kipp, 2001). Examples of new, portable, high-memory devices include the keychain drive, a device about the size of a key that can be popped into a USB port. The device holds between 16 megabytes and two gigabytes of data—the equivalent of a pickup truck filled with books (Mossberg, 2003). Another such gadget is the USB Memory Watch, a seemingly normal timekeeping device with a USB cable hidden in the band and the capacity to store 512 megabytes of data (around 11,000 pages of text). The USB Memory Pen is a fully functional refillable ink pen measuring 5.75 inches in length that can store 256 megabytes of data (about 5,500 pages of text). As the miniaturization of data storage hardware continues, we may see the emergence of nanoscale devices—devices with structural features in the range of 1 to 100 nanometers. (A nanometer is one billionth of a meter.) Potential applications of nanoscale electronics in the future include tiny mass data storage devices with capacities that are 1,000 times greater than today (National Science Board, 2002).

The Case of Robert Hanssen

FBI officer Robert Hanssen capitalized on the vulnerability of IT systems and his status as a trusted employee to become one of the most damaging spies in United States history. Charged with spying against the United States for over 20 years, Hanssen provided Soviet (and then Russian) intelligence agents with highly classified documents concerning U.S. intelligence sources and electronic surveillance techniques.

Hanssen's computer queries, which extended substantially beyond the realm of information he had a need to know, did not arouse suspicion among his colleagues because he was an authorized user of the databases he exploited. Hanssen walked into Bureau units in which he had worked long before, logged onto stand-alone data systems, and retrieved the identities of foreign agents whom U.S. intelligence services had compromised (Commission for the Review of FBI Security Programs, 2002).

Using specialized data-storage devices, Hanssen removed at least 26 encrypted floppy-diskettes from the FBI using a technique called "40-track mode" in which text is hidden on what appears to others to be a blank diskette (Verton, 2001). *Hanssen also made use of his counterintelligence skills and knowledge of FBI automated record systems to confirm that his illicit activities had gone undetected. Before leaving material for his Russian handlers, Hanssen would search the Bureau's systems to determine whether the locations had been identified as drop sites* (Commission for the Review of FBI Security Programs, 2002). *Hanssen's espionage activities illustrate how automated information systems "are likely to become the spy's best friend" in the years ahead* (Herbig & Wiskoff, 2002, p. 74).

Implications for Insider Espionage

Technological advances in information storage and retrieval are making it increasingly difficult to prevent the illicit dissemination of classified and proprietary information. The growth of automated databases and computer networks is expanding the amount

of information that can be collected and compromised by employees, and increases our vulnerability to every single malicious insider. Employees can now locate, duplicate, and distribute classified and proprietary files while sitting at a workplace computer station engaged in what appears to coworkers and supervisors as normal work activities. The steadily increasing capacity and decreasing size of data storage devices makes it possible for insiders to remove large quantities of information from organizations with little risk of being caught. The relative ease with which digitized information can be stolen likely increases an individual's confidence they will avoid detection. Recent cases of espionage involving government and industry personnel suggest that employees will increasingly capitalize upon information technologies to commit espionage in the years ahead.

B. An Expanding Market for Protected U.S. Information

As a result of America's emergence as the dominant political, economic, and military force, and the increasingly competitive global economy, foreign demand for protected U.S. information is increasing (Freeh, 1996). American insiders have access to more types of protected information that can be sold for profit, and can sell information to a broader range of private and government-sponsored entities.

More Types of Information Can Be Sold to Foreign Buyers

Insiders working within American biotechnology, aerospace, telecommunications, computer software and hardware, advanced transportation, manufacturing, energy research, pharmaceutical, and semiconductor industries have access to proprietary information that foreign businesses and intelligence collectors will pay substantial sums of money to obtain (Freeh, 1996; Moule, 1996). Increasing demand for American proprietary information supplements ongoing demand for classified information pertaining to information systems; sensors and lasers; electronics, aeronautics, armaments and energetic materials; marine and space systems; guidance, navigation and vehicle systems; signature control systems; space systems; materials, manufacturing and fabrication; information warfare; nuclear systems technologies; power systems; chemical-biological systems; weapons effects and countermeasures; ground systems; and directed and kinetic energy systems (Defense Security Service, 2002; National Counterintelligence Executive, 2000).

While the United States distinguishes information as classified, proprietary, and dual-use (technologies with both military and commercial applications), it is worth noting that foreign entities gathering and utilizing American intelligence do not necessarily make such distinctions. As economic strength becomes "the new currency of national power," the distinction between espionage involving the theft of classified information and espionage involving the theft of proprietary information may be lessening with respect to national security implications (Schweizer, January/February 1996, p. 1).

More Foreign Buyers of Protected Information

The supervising agent of the FBI field office in Palo Alto, CA, recently stated that at least 20 foreign nations have repeatedly attempted to steal U.S. trade secrets in Silicon Valley over the past 5 years (Iwata, 2003). Former FBI Director Louis Freeh reported to a U.S. Senate committee in 1998 that entities from at least 23 countries were engaged in suspicious intelligence collection activities directed at U.S. interests (Freeh, 1998). A senior FBI official who attended a 1996 conference sponsored by PERSEREC indicated that the FBI had 800 active espionage investigations underway, involving 23 different countries (Geide, 1996).

In addition to foreign governments, American employees can now sell protected information to foreign and multinational corporations, foreign research and science institutions, freelance agents (some of whom are former intelligence officers), terrorist organizations, revolutionary groups, extremist ethnic or religious organizations, drug syndicates, and organized crime groups.

Implications for Insider Espionage

The expanding market for protected U.S. information is increasing our vulnerability to espionage in several ways. More Americans have access to information that foreign entities want and are willing to pay for, and there are more foreign entities to which this information can be sold. The increasing demand for protected U.S. technologies suggests that greater numbers of foreign nationals from more countries will be striving to recruit insiders into espionage. As the world's leading industrial power and leader in technology development, the United States is a prime target of foreign economic collection (National Counterintelligence Executive, 2001). As more allies pursue U.S. technological information, some insiders may find it easier to rationalize committing espionage. Some individuals who consider it reprehensible to sell U.S. technology or military secrets to an avowed enemy of the United States may be less reticent to sell this information to individuals or organizations located in countries that are viewed as friendly to U.S. interests.

C. Internationalization of Scientific Research and Commerce

International R&D and business relationships allow foreign and American organizations to share costs, pool risks, and consolidate resources, but these relationships can also lead to espionage against the United States. Joint ventures, joint research, co-production and other exchange agreements, as well as international conventions and seminars, place foreign personnel in close proximity to U.S. personnel. Insiders can use these venues to identify potential foreign buyers, and foreign buyers can use the same venues to assess and recruit American employees (National Security Agency, 1997). Scientific conferences and international research facilities are rich targeting grounds as specific technologies are linked with knowledgeable personnel (Defense Investigative Service, 1996; National Counterintelligence Executive, 2000; Overseas Security Advisory Council, 1992). International R&D alliances and foreign trade relationships are now so diverse and flexible that the extent and growth of such relationships is difficult to

measure statistically. Available data suggest that greater numbers of insiders routinely participate in collaborative international scientific and commercial endeavors.

International R&D Alliances

The number of international science and technology agreements being forged between the U.S. government and foreign counterparts is increasing over time (Government Accounting Office, 1999). One GAO study showed that seven government organizations established 575 international research agreements during 1997 alone. The organizations that established these agreements are Department of Energy, National Aeronautics and Space Administration, National Institutes of Health, National Institutes of Standards and Technology, the National Oceanographic and Atmospheric Administration, National Science Foundation, and Department of State. These cooperative ventures involved 57 countries, eight international organizations, and 10 groups of organizations or countries. Fifty-four of these agreements were broad-based arrangements between the U.S. government and the governments of foreign countries. The remaining 521 agreements were between research agencies and their counterparts in foreign governments and organizations, or agreements to conduct cooperative research, to provide technical support, or to share data and equipment.

Scientific collaboration between the United States and other countries is occurring more often in the private sector as well. Between 1990 and 2000, 6,477 technology alliances were established, compared with the establishment of 3,826 such alliances between 1980 and 1989 (National Science Board, 2002). The majority of these international alliances involved companies from the United States, Japan, and countries of Western Europe. Eighty percent of these alliances involved at least one U.S.-owned organization (National Science Board, 2002). The percentage of papers authored by U.S. scientists in conjunction with foreign scientists has been increasing steadily for decades (National Science Board, 2002).

Establishment of International Research Facilities

The increasingly multicultural nature of R&D is furthermore illustrated by the establishment of international research facilities. In 1997 U.S. firms established 186 research and development facilities in other countries. As of 1998 (the latest year for which data are available), 715 R&D facilities were operated by 375 foreign-owned companies in the United States. Thirty-five percent of these facilities were owned by Japanese parent-companies. Other countries with a significant presence in the United States are Germany and the United Kingdom. R&D spending by U.S. affiliates of foreign companies in the United States increased 28 percent between 1997 and 1998—from $17 billion to $22 billion. This is the largest single-year increase in such expenditures since 1990 (National Science Board, 2002).

American Firms Exporting Abroad

Economic globalization is resulting in more frequent interaction between American employees and foreign businesspersons and government representatives. Broad measures of the level of interaction between insiders and foreign entities are the number of American organizations involved in the exportation of goods and services to foreign countries, and the value of these goods and services. About 69,000 U.S. companies engaged in the exportation of goods and services to other nations in 1987. Ten years later in 1997, over 200,000 such organizations were identified. In 1993 total U.S. exports in goods and services were valued at around $643 billion. Eight years later in 2001, U.S. exports totaled over 1 trillion (U.S. Department of Commerce, 2003).

Reflecting the fact that new technologies more often have both military and commercial applications, greater numbers of American personnel are in the awkward position of selling unclassified and approved-for-export versions of products to countries whose intelligence services are actively conducting espionage to acquire classified technologies in the same industries. For example, cleared defense contractor personnel employed in highly compartmented programs to develop and launch reconnaissance satellites and imaging systems now travel to foreign countries to sell unclassified versions of these technologies.

Implications for Insider Espionage

By increasing the frequency with which knowledgeable insiders meet with foreigners interested in exploiting their knowledge, the globalization of business and scientific research is expanding opportunity for espionage. Relationships established through participation in joint projects and attendant activities provide opportunities for Americans to sell classified information and make it easier for foreign entities to assess and recruit Americans with exploitable weaknesses. The frequency and circumstances of these relationships also makes it increasingly difficult for security and counterintelligence personnel to distinguish normal relationships from the few that represent a significant security risk.

Foreign business relationships create an environment that is particularly conducive to espionage. Some feel there is a growing inclination of those involved to regard the unauthorized transfer of information or technology as a “business matter rather than an act of national betrayal or treason” (Wells, 2000). Foreign business relationships commonly involve discussions in which sellers and buyers bargain over price, quantity, and quality—and sensitive information or a side contract as a “technical consultant” can easily enter into these negotiations.

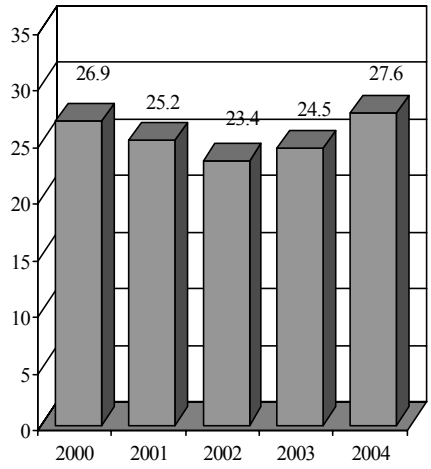
Collaboration on scientific or technical research projects, by its very nature, involves the approved exchange of scientific and technical information. Some insiders participating in these exchanges have access to protected information that should not be shared, but the line between protected and public information is not always clear. Some scientists believe that research findings should always be shared rather than protected.

D. Increasing Frequency of International Travel

Persons who travel overseas are in a position to establish contact with foreign buyers of information. An insider's risk of being targeted for exploitation by foreign intelligence services increases outside the United States where foreign operatives are less vulnerable to detection by U.S. counterintelligence services. Foreign operatives are more aggressive in their attempts to recruit Americans into espionage when Americans are on unfamiliar ground and may be more easily approached (National Security Agency, 2001). While travel from the United States declined from 2000 to 2002, and travel to the United States declined from 2000 to 2003, travel to and from the United States regained an upward momentum in 2004 and is projected to increase in the years ahead.

Figure 1

Overseas Travel by Americans 2000–2004 (in millions)



Office of Travel and Tourism Industries (2004a) and R. Erdmann (personal communication, January 24, 2005).

U.S. Travelers to Overseas Destinations

As shown in Figure 1, 26.9 million visits were made overseas by U.S. residents in 2000. In 2001, Americans traveled overseas an estimated 25.2 million visits and in 2002, overseas travel dropped to 23.4 million visits. In 2003, however, overseas visits by American rose to 24.5 million. While final figures are not yet available, based on travel occurring January-September, outbound travel to overseas destinations is estimated to total 27.6 million in 2004 (Office of Travel and Tourism Industries, 2004a; R. Erdmann, personal communication, January 24, 2005).

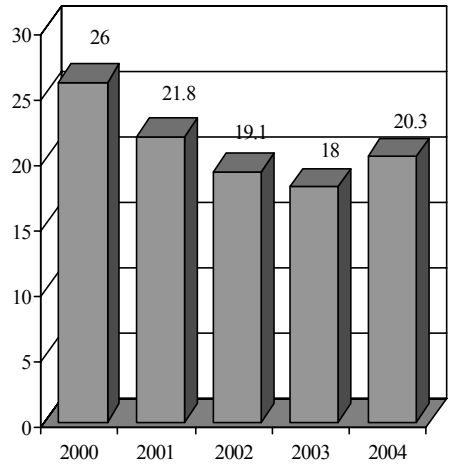
Visits to China by U.S. residents are projected to reach 437,000 in the year 2006, a 21 percent increase from the 361,000 documented visits that occurred in 2002. Visits to Taiwan by U.S. residents are projected to reach 324,000 in 2006, a 13 percent increase from the 288,000 visits documented in 2002. Visits to India are projected to number 320,000 in 2006, a 25 percent increase from the 257,000 visits documented in 2002. Visits to Korea are projected to number 759,000 in 2006, a 19 percent increase from the 639,000 documented visits in 2002. Visits to Germany are projected to number 1.4 million in 2006, a 17 percent increase from 1.2 million documented visits in 2002. Visits to Israel are projected to number 331,000 in 2006, a 26 percent increase from the 263,000 documented visits in 2002. Finally, visits to Japan are projected to number 4.3 million in 2006, a 19 percent increase from the 3.6 documented visits of 2002 (Office of Travel and Tourism Industries & Global Insight, 2003).

Overseas Arrivals to the United States

As shown in Figure 2, 26.0 million overseas visitors traveled to the United States in the year 2000. Travel to the United States was documented at 21.8 million in 2001, dropping to 19.1 million in 2002. In 2003, overseas travel to the United States dropped again, to 18 million. Based on available data for 2004, however, arrivals to the United States from overseas destinations are expected to reach 20.3 million by the end of 2004. While not shown, arrivals to the United States are projected to reach 20.7 million in 2005, 22.0 million in 2006, and 23.4 million in 2007 (Office of Travel and Tourism Industries, 2004a; 2004b; R. Erdmann, personal communication, January 24, 2005).

Figure 2

Overseas Arrivals to U.S. 2000–2004 (in millions)



Office of Travel and Tourism Industries (2004a; 2004b) and R. Erdmann (personal communication, January 24, 2005).

Implications for Insider Espionage

Barring unforeseen changes related to terrorism and other domestic and international developments, travel to and from the United States is expected to increase in the years ahead. The greater number of Americans engaging in international travel, and the increasing number of foreign visits to American soil is resulting in greater opportunity for the transfer of proprietary and classified U.S. information. Foreign travel facilitates interaction between Americans with access to protected information and foreign nationals. Whether this interaction occurs in the United States or abroad, insiders who are considering espionage are more able to establish contact with foreign buyers. Similarly, it is becoming easier for foreign nationals to establish contact with American insiders who have access to protected information. Due to increasing international travel, foreign nationals are in a better position to recruit and exploit American personnel. At the same time it is becoming easier for American employees to establish contact with foreign entities it is becoming more difficult for counterintelligence personnel to distinguish foreign travel that is of security concern.

E. Global Internet Expansion

The Internet's technological indifference to political borders and the anonymity it affords its users make it a highly effective tool for espionage. Insiders can use the Internet to establish contact with potential foreign buyers and to transmit massive amounts of stolen material to them. There is virtually no limit to the amount of information that can

be transferred to foreign buyers by a technically competent insider with access to digitized proprietary files and the Internet.

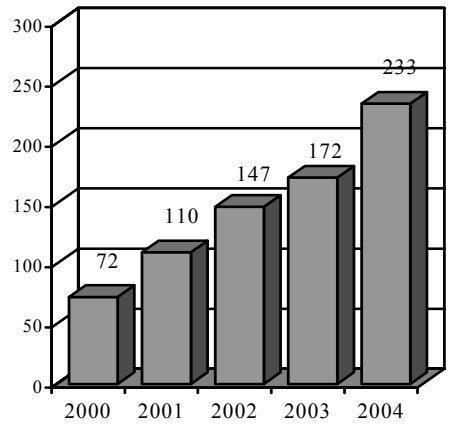
In addition to providing advantages to those who volunteer information for sale, increasing numbers of insiders are at risk for being recruited online. Foreign businesspersons and intelligence collectors scrutinize commentary posted in Internet discussion groups, newsgroup postings, online bulletin boards, and websites to identify American government offices, companies, research laboratories, and employees who have access to the types of information and technologies they seek. The growing popularity of the Internet as an espionage tool is reflected in rising U.S. defense industry reports of computer-based collection attempts (Defense Investigative Service, 1996). Internet use is continuing to expand domestically and abroad, in the workplace and in the home (Internet Software Consortium, 2002; U.S. Department of Commerce, 2002).

Internet Expansion

The annual *Domain Survey,* one of the longest running measurements of the Internet's size, documents a rapid rise in the number of Internet hosts worldwide. (An Internet host is a computer connected to the Internet.) In the year 2000, this study identified 72 million Internet hosts globally. Internet hosts numbered 110 million by 2001, 147 million in 2002, 172 million in 2003, and 233 million in 2004 (Figure 3). Some analysts project that by the year 2010, 95 percent of the population of the industrialized world, and half the population of the developing world, will be online (Cetron & Davies, 2001). Within the American workplace, the proportion of employees using the Internet and/or email grew from about 18 percent in 1998 to almost 42 percent in 2001 (U.S. Department of Commerce, 2002).

Figure 3

Internet Hosts Worldwide 2000–2004 (in millions)



Internet Software Consortium (2002). *Annual Domain Survey 2002* http://www.isc.org/ds/www. 200201/index. html.

Online Language Populations

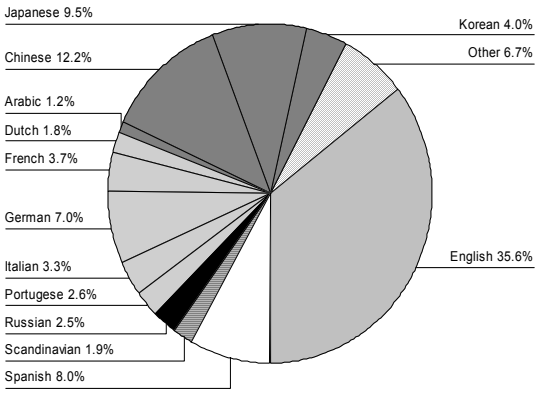
Reflecting the growing cultural diversity of computer-users, as of September 2003, 64 percent of all Internet hosts were non-English speaking (Global Reach, 2003). Nine and one-half percent of users were Japanese-speaking, over 12 percent were Chinese-speaking, and over 4 percent were Korean-speaking (Figure 4). Around seven percent of Internet users were German-speaking and over 3 percent spoke Italian. Two and one-half percent of Internet users were Russian-speaking. Of the 200 million Internet search requests processed by *Google* daily, about two-thirds are initiated in languages other than English (Friedman, 2003).

Geographic Regions of Greatest Internet Growth

The Asia-Pacific region is believed to be the fastest growing area of Internet use currently, with Internet subscriptions doubling from 2000 to 2001, to total 143 million. Internet use in China is poised to grow particularly dramatically in the years ahead. China has a population of 1.3 billion but currently has around 23 million Internet users. Latin American Internet use is also experiencing high growth. Users in the region are expected to increase from 26 million to over 30 million by 2003. Middle East Internet use is at 4.2 million—up from 1.9 million in the year 2000. Israel has about 1.3 million Internet users; nearly 90 percent of Israeli homes have personal computers (Internet Software Consortium, 2002).

Figure 4

Online Language Populations
680 Million Users Estimated



Global Reach (January 2004). *Global Internet Statistics by Language* (www.glreach.com/ glob stats/).

Implications for Insider Espionage

Internet use is expanding domestically and globally, and the cultural and linguistic diversity of users is increasing. More American employees have access to the Internet in their workplaces and in their homes. As the Internet creates a large and efficient marketplace for exchanging a wide variety of products and services, it also brings potential buyers and sellers together for the purposes of espionage. It allows potential buyers and sellers of information to learn a great deal about one other, provides means for establishing contact, and provides an efficient and relatively secure mechanism for transmitting unlimited quantities of information across national boundaries. Sellers and buyers of information can interact without revealing their identities, as illustrated by the recently convicted spy, NRO employee Brian Regan.

Research posted on the Internet allows foreign intelligence collectors to identify government offices, businesses, and research laboratories that possess the specific types of information they seek, and to obtain substantial amounts of information about insiders who work for these entities. Intelligence collectors regularly troll Internet chat rooms, bulletin boards, and newsgroup postings to identify individuals or information of interest. Once a person is identified as a potential target, a knowledgeable information collector may search for and read that person's other newsgroup, bulletin board, or chat room postings and will look for a means to establish direct contact. Unsolicited email requests for information are an increasingly common method of establishing contact with American targets (Defense Security Service, 2002).

Concluding Remarks Part I

Opportunity for espionage consists of access to classified or proprietary information that can be exchanged for money or other material or nonmaterial benefits, access to foreign entities interested in obtaining this information, and means for transferring this information to these foreign recipients. Findings of Part I of this study indicate that technological advancements in information storage and retrieval, increasing global demand for protected U.S. information, the internationalization of research and commerce, increasing international travel, and global Internet expansion are converging to create unprecedented opportunity for insiders to steal and transfer protected U.S. information to foreign entities. Part II of this study examines the frequency with which insiders are encountering situations that can provide motivation for spying.

Part II
Situations That Can Provide Motivation for Insider Espionage

Motivation, broadly defined, is a feeling or state of mind that influences one's choices and actions. Motivation for insider espionage results from a complex, interaction between personality characteristics and situational variables (Crawford & Bosshardt, 1993; Eoyang, 1994; Sarbin, 1994; Parker & Wiskoff, 1991; Timm, 1991). While most insiders possess personal qualities that are not conducive to committing espionage (or any serious crime for that matter), some insiders with access to classified and proprietary files become motivated to commit espionage when they encounter the right conditions in their personal and professional lives. Insiders commit espionage to satisfy needs and desires and to alleviate problems. Situations that can provide motivation for espionage include the experiencing of financial crisis or the development of a gambling addiction. Other factors explored here that can result in motivation for spying are emotional and financial ties to foreign countries, perceived mistreatment by one's employer, and feelings of obligation or loyalty to a foreign country or to a global community.

A. Americans' Vulnerability to Experiencing Financial Crisis

Employees who are financially overextended may be at risk for engaging in illegal acts to generate funds. Of the many factors known to provide motivation for insider espionage, the experience of personal financial difficulties is among the more prominent. Spies believed to be partially or primarily motivated by a desire to alleviate financial pressures include David Barnett, William Bell, David Boone, Robert Haguewood, Robert Hanssen, Robert Kim, Kurt Lessenthien, Richard Miller, Bruce Ott, Ronald Pelton, Earl Pitts, Brian Regan, and others (Harris, Thompson & Ciccarello, 2002; Herbig & Wiskoff, 2002). Common causes of financial crisis include gambling addiction, substance abuse, loss of job, divorce or separation, unexpected medical expenses, and increasingly—the accumulation of consumer debt (Sullivan, Warren & Westbrook, 2000).

Consumer Debt

Comparisons of research findings over time (findings of the Consumer Bankruptcy Project I, the Consumer Bankruptcy Project II, and the Ohio Bankruptcy Study) by Sullivan et al. (2000) show that credit card debt plays a significant role in creating financial instability for Americans. Whereas in 1981 the average debtor filing for bankruptcy owed about 18 percent of his or her yearly income in credit card loans, in 1991 the average debtor in bankruptcy had accumulated the equivalent of nearly half a year's take-home income in credit card balances. By 1997, the average debtor filing for bankruptcy was estimated to have revolving credit card debt equivalent to $77 for every $100 of annual income (Sullivan et al., 2000, p. 124-126).

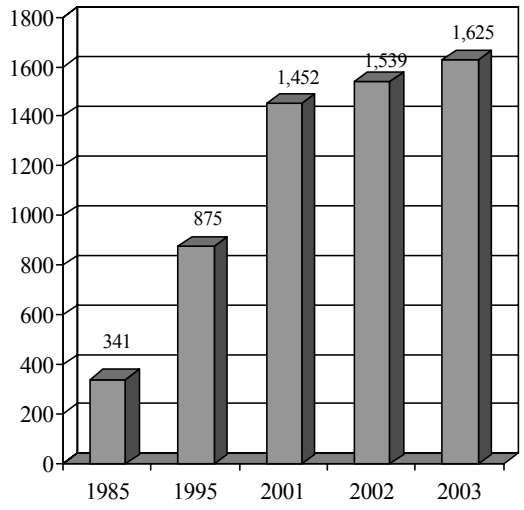
Consumer credit increased by 5 percent in May 2003, to 1.76 trillion, and total American household credit now stands at 110 percent of annual disposable income—up from 76 percent in 1986 (Dobbs, 2003, p. 36). Lending to individuals with poor credit histories or who are already burdened with debt (e.g., "sub-prime" lending) has become one of the most profitable, and hence one of the most rapidly growing segments of the consumer lending industry (Sullivan et. al., 2000).

Personal Bankruptcy Filings in the United States

Bankruptcy law changed in 1979 making it easier to file, but this alone does not explain the accelerating rate of filings that has occurred since the mid-eighties (Figure 5). In 1985, 341,000 non-business bankruptcies were filed in the United States. Ten years later in 1995, over 875,000 bankruptcies were filed. In the year 2001, bankruptcies exceeded 1.4 million—a 500 percent increase in filings since 1980. Americans set a new record in 2002 for going bankrupt, with over 1.5 million people filing for personal bankruptcy. Finally, in 2003, over 1.6 million personal bankruptcy filings occurred. "If each family were a business," says Harvard law professor Elizabeth Warren, "we would describe America's businesses as vastly overleveraged…far too many are on the brink of disaster." Joseph Pomykala, an economics professor at Towson University states that the bankruptcy rate in the United States is now 12 times the rate it was during the Great Depression (Dobbs, 2003, p. 36).

Figure 5

Non-Business U.S. Bankruptcy Filings 1985–2003 (in thousands)



ABI World (2002). U.S. Bankruptcy Filings 1980-2001 Business, Non-Business, Total. (http://www.abiworld.org/stats/newstatsfront.html).

Implications for Insider Espionage

Americans are increasingly living close to the financial edge. Because greater numbers of insiders are encountering serious financial pressures, it is logical to suspect that more insiders may turn to theft, fraud, embezzlement, or other illegal behaviors—including espionage—in a desperate effort to alleviate those pressures. At the same time more families are experiencing financial stress, the potential financial gain from espionage is increasing. In the Information Age, typified by global competition and rapid technological change, information has become a valuable currency. Information or material that enables a country or company to field a new weapons system or develop a new product or technology has tremendous monetary value.

B. Increasing Prevalence of Compulsive Gambling

Problems brought about by irresponsible or compulsive gambling include indebtedness, defaults on debts, disrupted interpersonal relationships, poor work performance, and participation in criminal activities to finance the continuation of gambling (Ladouceur, Dube & Bujold, 1994; Meyer & Stadler, 1999). As access to funds becomes limited, some compulsive gamblers resort to crimes to pay debts and to garner more money to sustain their addictions (American Psychiatric Association, 1992; Bixby, 2000; Brunner, 1992; Committee on the Social and Economic Impact of Pathological Gambling, 1999; Meyer and Stadler, 1999; Volberg, 2001). George French, Nelson Drummond, Daniel Richardson, and James Wood are convicted spies whose motivation for espionage appears to have evolved at least partially out of desires to alleviate debts incurred as a result of compulsive gambling. For most Americans gambling is simply a form of entertainment, but for an increasing proportion of the population, gambling is becoming an uncontrollable addiction. Problem or "compulsive" gambling may become a more prominent security issue in the days ahead.

Increasing Popularity of Gambling

The popularity of gambling has increased dramatically in the last three decades. Gambling is currently the fastest-growing entertainment enterprise in the United States (Thompson, 2001). Legal gambling activities in the United States now include state lotteries, pari-mutuel betting on horses, greyhounds, jai-alai, sports book-making, card games, keno, bingo, slot machines, progressive slot machines, video poker machines, video keno machines, video blackjack machines, and video roulette machines (although not all of these forms of gaming are legal in all regions). In 1998 there were an estimated 90 casinos, 39 lotteries, eight Bingo games and 53 sports books available on the Internet. In 1999 there were 250 casinos, 64 lotteries, 20 Bingo games, and 139 sports books available online (Rolling Good Times, 1999). Pari-mutuel racetracks are currently the most widespread form of gambling in the United States—now legal in over 40 states. Indian casinos now operate in every region of the country (National Opinion Research Center, 1999).

Increasing Prevalence of Gambling Disorders

Reflecting the escalating popularity and availability of gambling, an increasing number of Americans are developing gambling disorders (Jacobs, 2000; Potenza, 2002). The proportion of problem gamblers who are most seriously troubled, and who are most difficult to treat, is expanding rapidly (National Opinion Research Center, 1999; Volberg, 2001). Analyses conducted by a Harvard research team show that pathological gaming—the most severe form of gambling—has increased by more than 50 percent among adults since 1977 (Shaffer, 1999). The *National Gambling Impact and Behavior Study,* one of the most extensive studies of the social and economic impacts of gambling ever conducted, shows that about 2.5 million American adults are pathological gamblers and that another 3 million American adults are classifiable as problem gamblers (have dysfunctional gambling habits that are less severe than those of pathological gamblers). An additional 15 million American adults are believed to be at risk for developing serious gambling problems. Gambling disorders are even more prevalent among younger Americans (Jacobs, 2000). One study estimated that 5.7 million American adolescents have a gambling problem and that 2.2 million adolescents are pathological gamblers (Shaffer, 1999).

Implications for Insider Espionage

Problems associated with large gambling losses often create a sense of desperation to repay funds and hide losses from one's family. Research shows that compulsive gamblers are at risk for committing workplace crimes such as fraud and embezzlement (Meyer & Stadler, 1999). The increasing popularity of gambling and prevalence of gambling addiction suggest that a greater number of insiders who have access to classified and proprietary information may become motivated to sell this information for personal profit.

C. Diminishing Organizational Loyalty

The topic of workplace revenge has received much attention in recent years, particularly as murderous rampages by disgruntled employees have become increasingly common. More often, however, disgruntled employees commit crimes against their employers in the form of fraud, embezzlement, and sabotage (Ambrose, Seabright & Schminke, 2002; Morris & Sherman, 1981; Mowday, Porter & Steers, 1982; Peak, 1995; Shaw, Ruby & Post, 1998). Several Americans convicted of espionage against the United States were motivated by desires to exact revenge upon the organizations that employed them (Herbig & Wiskoff, 2002). Disgruntled government insiders who committed espionage include John Charlton, John Allen Davies, Douglas Groat, and Edwin Earl Pitts among others. Changing conditions in the American workplace suggest that loyalty to organizations is diminishing and that workers are at greater risk for becoming disgruntled.

The Changing Psychological Contract

In *Psychological Contracts in Organizations: Written and Unwritten Agreements*, Rousseau (1995) explores employees' and employers' changing expectations and diminishing levels of commitment to one another. Rousseau concludes that in the new economy, neither employers nor employees expect long-term, mutually satisfying relationships. Instead, both parties are more likely to conceptualize employment as the short-term exchange of benefits and contributions.

In adapting to the rapidly changing business environment, American organizations more often downsize, automate, transfer jobs overseas, and lay off personnel who are no longer needed. American employers increasingly hire part-time and temporary workers who are offered limited benefits and minimal job security. Terminated American workers are less likely to receive severance pay, extended health benefits, or other types of assistance than in previous decades, and more often suffer from "layoff survivor syndrome" in which mistrust and anxiety has replaced feelings of fidelity to organizations (Quinn, 1996; Reichheld, 1996). Many insiders with access to highly marketable technological information are transient workers who voluntarily move from one new employment opportunity to the next, "cashing out their career investments on a regular basis" (Tulgan, 1996, p. 2). Organizational loyalty among computer programmers, for example, has been undermined by high demand for their services and high rates of turnover in the profession (Shaw, Ruby & Post, 1998, p. 11). Some feel that American workers in high-tech fields often view themselves as owners of their own skills and knowledge—"as investments to be parlayed into the highest possible dividends" (Walker Information, Inc., 2000, p. 5).

Implications for Insider Espionage

The psychological contract between employees and employers is changing. In striving to compete in the global marketplace, American organizations more often engage in practices that some employees will experience as alienating and indicative of a lack of loyalty. More employees, lacking job security and other benefits, may become disgruntled. Individuals who perceive that they have been treated insensitively or unfairly may seek revenge against their employers. Disgruntlement can provide motivation for espionage directly as well as making it easier for insiders to rationalize espionage that is actually committed to satisfy other needs or desires.

D. Ethnic Diversification of the American Workforce

The United States has experienced a profound demographic transformation in the last three decades resulting in a substantial increase in the number of U.S. residents with close foreign ties. Emotional ties to a foreign country, or to family or friends in a foreign country, can result in conflicts of conscience concerning national loyalty. Insiders with such ties are in a better position to transfer U.S. information to foreign contacts and are better equipped to use information obtained through their employment in U.S. firms to participate in joint ventures or to start their own companies abroad (Christie, 2002;

Nadel, 2002; Overseas Security Advisory Council, 1992; Saxenian, Motoyama & Quan, 2002). Government insiders whose espionage activities appear to have been influenced by motivation and opportunity stemming from foreign ties, include Joseph Santos, Robert Kim, Douglas Tsou, Charles Anzalone, Thomas Dolce, and Jonathan Pollard (Herbig & Wiskoff, 2002).

The Case of Jonathan Pollard

Jonathan Pollard is frequently cited as an example of an insider whose loyalty to a foreign country played a substantial role in his decision to spy. Pollard's allegiance to Israel and desires to become a Zionist hero led him to pass thousands of pages of classified Navy documents to Israel, including satellite photographs of Arab weapons systems and Iraqi nuclear test sites (Zacharia, 2000, p. 7B).

While desires for money appeared to become an added source of influence over time (as Pollard and his wife received tens of thousands of dollars in cash and jewelry), Pollard's desire to serve Israeli interests is the prevailing explanation for his actions. Pollard asserted that it would have been an "outright betrayal" of his heritage, his personal integrity, "and an entire family lost in the ovens of the Holocaust" if he had "closed his eyes to what had to be done" (Kurtz, 1987, p. B1).

Diversity of Cleared Personnel

Between 1970 and 2000, the total foreign-born population in the United States grew from 9.7 million to 28.4 million (an increase of 191 percent), to constitute over 10 percent of the U.S. population. In 2000, around 60 million U.S. resident—about one fifth of the U.S. population—had one or more foreign-born parents (Schmidley, 2001).

The changing composition of the U.S. population is reflected in the composition of the American workforce in general, and the cleared DoD workforce specifically. The number of naturalized or derived citizens among active duty military personnel, reserve, and DoD civilian employees holding SCI, Top Secret, Secret, and Confidential clearances has increased substantially as a percentage of total clearances. (A derived citizen is a child who becomes a citizen when a parent becomes a naturalized U.S. citizen.) As shown in Table 1, the total number of active clearances decreased from 2.6 million in September 1992 to about 1.9 million in March 2002 (a reduction of about 29 percent), but the number of clearances held by naturalized or derived citizens increased from 35,734 to 43,594 (up by 23 percent) during this period (Heuer, 2003; Goral, 2002).

Defense contractors are not included in Table 1 as comparable data for 1992 are not available. Based on 2002 data, however, naturalized and derived citizens within the contractor community are disproportionately employed in the most sensitive positions. Naturalized or derived citizens compose .2 percent of the SCI contractor population for example, but compose .01 percent of each of the other clearance categories (Table 2) (Heuer, 2003; Goral, 2002).

Table 1
Proportion of Naturalized/Derived Citizens
Among DoD Active Duty, Reserve, and Civilian Clearance Holders
September 1992 and March 2002

	Clearance Holders		*Number Naturalized/ Derived Citizens*		*Percent Naturalized/ Derived Citizens*	
Clearance Holder	*September 1992*	*March 2002*	*September 1992*	*March 2002*	*September 1992*	*March 2002*
SCI	187,520	243,316	2,730	5,170	1.5	2.1
Top Secret	331,306	136,244	4,860	2,996	1.5	2.2
Secret	1,993,263	1,442,398	24,920	33,903	1.3	2.4
Confidential	87,114	35,347	3,224	1,525	3.7	4.3
Total	2,599,203	1,857,305	35,734	43,594	1.4	2.3

Table 2
Proportion of Naturalized or Derived Citizens
Among DoD Contractors March 2002

Type of Clearance Holder	*Clearance Holders*	*Number of Naturalized Or Derived Citizens*	*Percent Naturalized or Derived Citizens*
SCI	34,642	716	.2
Top Secret	110,395	119	.01
Secret	413,982	516	.01
Confidential	25,832	35	.01
Total	584,851	1,386	.02

Changing Attitudes Regarding American Citizenship

In addition to more insiders with foreign connections holding positions of trust, it appears that a smaller proportion of these insiders feel a strong sense of loyalty to the United States. While many foreigners continue to seek residence in the United States, new generations of immigrants appear to be less interested in adopting American values and customs. More immigrants are coming to the U.S. for economic advantages rather than for political or ideological reasons (Yang, 1994). An increasing percentage of immigrants choose not to become American citizens, and more of those who do obtain U.S. citizenship, maintain citizenship elsewhere (Massey, 1995; Renshon, 2001). Between 1970 and 2000 the naturalized citizen foreign-born population in the United States increased by 71 percent. During this same period, the noncitizen foreign-born population in the United States increased by 401 percent (Schmidley, 2001).

Implications for Insider Espionage

The increasing proportion of insiders with foreign backgrounds and connections suggests that more insiders will be in a position to provide classified or other protected information abroad, and may more often become motivated to do so due to financial and emotional ties. Foreign intelligence organizations typically emphasize the recruitment of individuals with whom they share common national, ethnic, racial, or religious backgrounds (National Counterintelligence Executive, 2002; Overseas Security Advisory Council, 1992). The increasing frequency of foreign connections affords sellers and buyers of U.S. information greater opportunity to initiate and maintain contact. Because more insiders have foreign ties, it is becoming more difficult to identify insiders whose foreign connections pose a security risk.

E. Growing Allegiance to a Global Community?

The growing frequency of communication between Americans and individuals of other nationalities is resulting in a deepening global consciousness among U.S. citizens and a greater appreciation of other cultures, religious beliefs, and value systems (Arnett, 2002; Craige, 1996; Elgin & LeDrew, 1997; Giddens, 1991; Robertson, 1992). While there are enormous benefits associated with Americans' greater awareness of the needs and interests of other peoples, and perspective of the world as an interdependent system, under extreme circumstances it is possible that an insider who feels a compelling sense of duty to a global society may experience a conflict of conscience similar to that experienced by an individual with foreign emotional ties. While it has long been recognized that a security risk can exist when an insider is bound by affection, influence, or obligation to a foreign government or to persons who are not citizens of the United States, the impact that globalization will have on national allegiance is not well understood.

American Citizens in a Global Society

Given our concern that insiders with foreign preferences may be at greater risk for sharing protected information with foreign entities, it is relevant that increasing numbers of insiders see themselves as both American citizens and citizens of a global society. Research indicates that growing numbers of Americans, especially younger generations of Americans, are bicultural in that aspects of their identity are rooted in local American traditions while other elements are rooted in an awareness of, and sense of belonging to, the larger global culture (Arnett, 2002; Elgin & LeDrew, 1997; Giddens, 1991). Research suggests that growing numbers of Americans feel a sense of loyalty to the United States and other nations simultaneously (Craige, 1996). Comments made by recently convicted spy, Ana Montes, suggest that a strong sense of obligation to serve the needs of a “world homeland” can, under some circumstances, provide sufficient motivation for trust betrayal.

The Case of Ana Montes

In a recent and very damaging case of insider espionage, Defense Intelligence Agency analyst Ana Montes passed classified information to Cuba. Owing to her beliefs in the moral righteousness of her actions, Montes expressed little remorse for helping Cuba "defend itself" against what she described as unfair and oppressive U.S. foreign policies.

Montes related that it is essential to "love one's neighbor as much as oneself" and that this principle is "the essential guide to harmonious relations between all of our nation-neighborhoods." Montes did not simply feel justified to commit espionage as a result of these beliefs – she felt "morally obligated" to do so (National Security Institute, November 2002, p. 7).

Montes stated that she hoped her actions would encourage the U.S. government to abandon its hostility towards Cuba and to work with Havana in "a spirit of tolerance, mutual respect and understanding." Montes expressed that a more friendly U.S. policy toward Cuba would permit the United States and Cuba "to work together and with other nations to promote tolerance and cooperation in our world country, in our only world-homeland" (Golden, 2002, p. 1).

Implications for Insider Espionage

Research suggests that greater numbers of Americans view themselves as both citizens of the United States and citizens of the world. Increasing numbers of Americans may be including within their community the inhabitants of countries that are currently conducting espionage against the United States. While Americans' increasing global consciousness is obviously beneficial in innumerable respects, it is possible that allegiance to a global community—to all the world's "nation-neighborhoods" to use Ana Montes' words—may compel an individual to conceptualize espionage as a moral duty. The increasing acceptance of global as well as national values may also make it easier for a potential spy to rationalize actions that are driven by baser motives.

Part III
Conclusions

The world is in the midst of an information revolution that many prominent thinkers believe will have as far reaching an impact on politics, economics, and culture as that of the Industrial Revolution (Toffler, 1987; Drucker, 1999; Hundley et al., 2000). Globalization is affecting the manner in which nation states and other international actors compete politically, economically and militarily. It is likely that globalization will expand the role of espionage in international competition and conflict.

In evaluating the implications of the technological, social, and economic trends discussed in this study, it is important to recognize that the vulnerabilities created by these trends are compounding one another to create an insider espionage risk that can be described as greater than the sum of its parts. That is to say, the vulnerabilities created by each trend are magnified by the presence of vulnerabilities created by other trends.

While it is true that greater numbers of insiders have access to large networked databases containing classified or proprietary files, for example, our increasing vulnerability to insider espionage stems from the fact that greater numbers of insiders with access to these databases *also* have access to technologies that allow them to download

massive amounts of information, *also* have means for secreting this information out of organizations, *also* have access to the Internet, *also* have foreign contacts, and *also* have financial problems that may provide motivation for espionage. It is not just that American insiders are traveling internationally more frequently and are participating in international scientific and commercial ventures more often, it is that these insiders more frequently have loyalties to other countries or cultures as well, and are more consistently targeted for recruitment by foreign intelligence collectors.

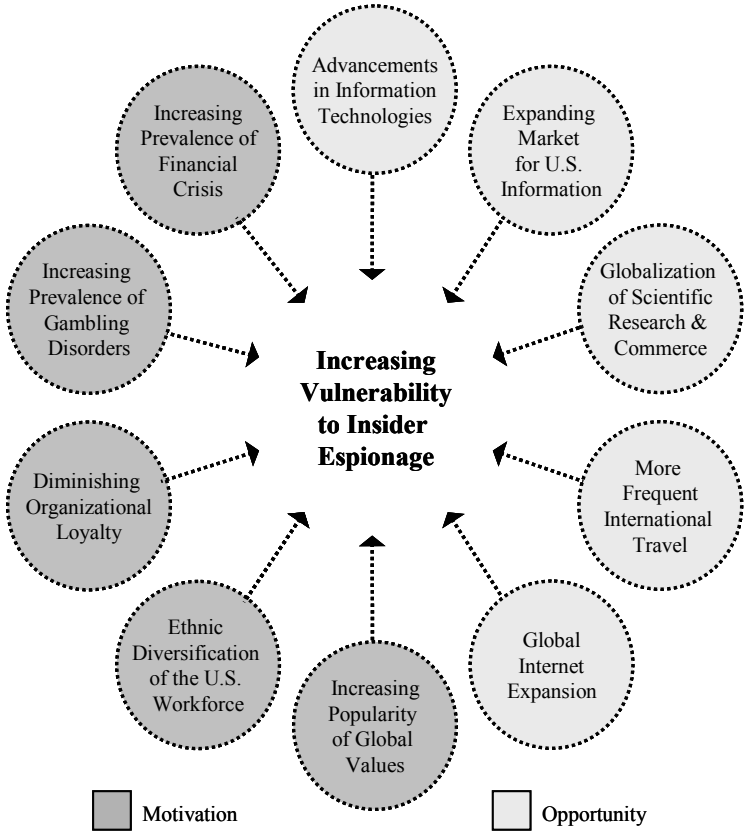
In summary, greater numbers of American insiders...

> ...are better able to access and steal classified and proprietary information due to technological advances in information storage and retrieval, *AND*...
>
> ...can sell more types of information to a broader range of foreign buyers than ever before, *AND*...
>
> ...have greater opportunity to establish contact with, and transfer information to foreign entities due to increasing international travel and global Internet expansion, *AND*...
>
> ...are more vulnerable to experiencing severe financial crisis due to aggressive consumer spending habits and gambling addiction, *AND*...
>
> ...are more vulnerable to becoming disgruntled and are less likely to feel an obligation to the organizations that employ them, *AND*...
>
> ...have ethnic ties to other countries, communicate with friends and family abroad, and interact with foreign businesspersons and governments, *AND*...
>
> ...have a holistic view of world affairs that under some circumstances may result in their conceptualizing espionage as morally justifiable.

It is not possible to describe all the ways the factors outlined in this study (Figure 6) may converge with one other, and other variables not discussed here, to create opportunity and motivation for spying. The fact that the vulnerabilities created by these trends are compounding one another does suggest, however, that we are at greater risk for experiencing insider espionage than in previous decades. Throughout our research we did not identify a single countervailing trend that will make insider espionage more difficult or less likely in the immediate future.

Figure 6

Technological, Social, and Economic Trends that are Increasing U.S. Vulnerability to Insider Espionage[a]



[a]There are other factors that provide opportunity and motivation for insider espionage that are not explored in this study or included in this diagram.

Part IV
Discussion

Results of this study show that mitigating U.S. vulnerability to insider espionage will increasingly require the orchestrated efforts of personnel security, information security, and counterintelligence organizations. An improved personnel security system is needed to reduce the number of potential espionage offenders, more rigorous information security measures are needed to reduce the vulnerability of IT systems that contain classified and proprietary files, and more effective counterintelligence operations are needed to detect insider spies sooner to limit the damage they can inflict.

The goal of the personnel security system, as expressed in Executive Order 12968, is to ensure that access to classified information is granted only to employees whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, freedom from conflicting

allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. To the extent that personnel security screening satisfies this objective, fewer unprincipled, irresponsible, troubled, or disloyal employees will gain and retain access to classified information. By denying access to individuals whose backgrounds or current behavior signifies they might be unreliable, untrustworthy, or disloyal, personnel security measures reduce the likelihood that insider espionage will occur.

In addition to achieving these more general objectives, however, the findings of this study indicate that it is becoming increasingly important that the personnel security system be improved with respect to identifying personnel of counterintelligence concern. It is essential that individuals who abuse substances or who have demonstrated financial irresponsibility are denied access to classified information, but it is also very important that the background investigation lend greater insight into potential foreign influence and outside activities issues.

Even the most effective personnel security program will never fully eliminate the insider espionage threat, however. Owing to the inherent difficulty of predicting human behavior, it will never be possible to identify all individuals who, under some combination of circumstances, will choose to steal classified and proprietary information. Because we will always have insiders in our midst who will become sufficiently motivated to spy, we must also consider the extent to which such insiders have opportunity to access and steal classified information. One of the areas of greatest concern identified by our research is the increased risk resulting from technological advancements in information storage and retrieval.

While improving employee productivity, information technologies are making it increasingly difficult for organizations to control access to and distribution of protected information. The growth of automated databases and computer networks is rapidly expanding the amount of information that can be collected and compromised by every insider spy. The steadily increasing capacity and diminishing physical size of data-storage devices is making it easier for insiders to remove large quantities of information with less risk of being caught. The relative ease with which information can now be stolen may serve to increase an individual's confidence that they will be able to commit espionage without being detected.

Policies have recently been enacted to encourage increased sharing of national security information within agencies and among agencies, and between federal, state and local government agencies for homeland security purposes (U.S. Senate, S. 1025, Sec. 334, 2003). While there are many benefits to the increased availability of information, with this increased availability comes greater risk of compromise. Congress rightly recognizes that increased information sharing will succeed only with revised security policies and the employment of technologies to reduce the insider threat to classified computer networks (U.S. Senate 108–44, 2003). Results of this study support the need for security policies that will result in improved control of digitized files and more effective monitoring and tracking of insiders' use of digitized information.

Information security policies and practices must reflect a risk-management paradigm in which the benefits of information availability and sharing are weighed against the risks. The advantages associated with granting thousands of insiders access to databases that are foreign espionage targets must be weighed against the potential costs to national security if information contained within these databases is compromised. Because personnel security measures will never be capable of guaranteeing the continued reliability and trustworthiness of all cleared personnel, employees' ability to exploit multiple databases—especially those they do not need access to perform their work—must be curtailed.

References

Ambrose, M.L., Seabright, M.A., & Schminke, M. (2002). Sabotage in the workplace: The role of organizational justice. *Organizational Behavior and Human Decision Processes, 89,* 947–965.

American Bankruptcy Institute. (2002). *U.S. bankruptcy filings 1980-2001 business, non-business, total.* Retrieved August 12, 2002, from http://www.abiworld.org/stats/newstatsfront.html

American Psychiatric Association. (1992). *Diagnostic and statistical manual of mental disorders*, Fourth Ed. Washington, DC: Author.

Arnett, J.J. (2002). The psychology of globalization. *American Psychologist, 57*, 774–783.

Bixby, L. (2000, August 23). Thefts feed a casino habit. *The Hartford Courant,* A8.

Brunner, T. (1992). *Casino gambling in Chicago: Better Government Association staff white paper.* Chicago, IL: Better Government Association.

Cetron, M.J., & Davies, O. (2001). *Fifty trends now changing the world*. Bethesda, MD: World Future Society.

Christie, S. (2002). *New indictment expands charges against former Lucent scientists accused of passing trade secrets to Chinese Company*. U.S. Department of Justice. Retrieved April 4, 2003, from http://www.cybercrime.gov/lucent SupIndict.htm

Commission for the Review of FBI Security Programs. (2002). *A review of FBI security programs*. Washington, DC: Department of Justice.

Committee on the Social and Economic Impact of Pathological Gambling. (1999). *Pathological gambling: A critical review.* Washington, DC: National Academy Press.

Craige, B.J. (1996). *American patriotism in a global society.* Albany, NY: State University of New York Press.

Crawford, K.S., & Bosshardt, M.J. (1993). *Assessment of position factors that increase vulnerability to espionage*. Monterey, CA: Defense Personnel Security Research Center.

Defense Investigative Service. (1996). Computer espionage. *American Reporter, 288.* Retrieved August 8, 2003, from http://www.kimsoft.com/korea/edispy.htm

Defense Security Service. (2002). *Technology collection trends in the U.S. defense industry.* Alexandria, VA: Defense Security Service.

Defense Security Service. (2002, August). *Foreign collection activities directed against the U.S. defense industry: Methods, indicators, and security countermeasures.* Alexandria, VA: Defense Security Service.

Dobbs, L. (2003, July 21). In hock to the hilt. *U.S. News and World Report*, 36.

Drucker, P.F. (1999). Beyond the information revolution. *The Atlantic Monthly.* Retrieved September 9, 2003, from http://www.theatlantic.com/issues/99oct/9910drucker.htm

Elgin, D., & LeDrew, C. (1997). *Global consciousness change: Indicators of an emerging paradigm*. San Anselmo, CA: Millennium Project.

Eoyang, C. (1994). Models of espionage. In T.R. Sarbin, R.M. Carney, & C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal* (pp. 69–91). Westport, CT: Praeger.

Fialka, J.J. (1997). *War by other means: Economic espionage in America*. New York: W.W. Norton.

Freeh, L.J. (1996). *Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the House judiciary Committee Subcommittee on Crime*. Retrieved December 4, 2002, from http://www.fas.org/irp/congress/1996_hr/h/h960509f.htm

Freeh, L.J. (1998, January 28). *Threats to U.S. national security*. Statement for the record before the Senate Select Committee on Intelligence.

Friedman, T.L. (2003, June 30). Is Google God? Retrieved June 29, 2003 from http://www.nytimes.com/2003/06/29/opinion/29FRIE.html

Geide, K.M. (1996). Economic espionage: Looking head. In T.R. Sarbin (Ed.), *Vision 2021: Security issues for the next quarter century.* (Proceedings of a conference sponsored by PERSEREC and the Security Policy Board Staff, June 25–25, 1996.) Monterey, CA: Defense Personnel Security Research Center.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Cambridge, England: Polity Press.

Global Reach. (2003, March). *Global Internet statistics by language.* Retrieved January 8, 2003, from http://www.glreach.com/glob stats

Golden, T. (2002, October 16). Ex-U.S. aide sentenced to 25 years for spying for Cuba. *The New York Times,* D-7.

Goral, J. (2002). Data provided by John Goral. Monterey, CA: Defense Manpower Data Center.

Government Accounting Office. (1999). *Federal research: Information on international science and technology agreements* (GAO/RCED-99-108). Washington, DC: Author.

Harris, G., Thompson, T., & Ciccarello, N. (2002). *Anger and espionage: Report of an interview with Earl Edwin Pitts, 28-29 August, 2002*. Vienna, VA: Personnel Security Managers' Research Program.

Herbig, K.L., & Wiskoff, M.F. (2002). *Espionage against the United States by American citizens: 1947-2001*. Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (2003). *Investigation and adjudication of foreign influence issues*. Monterey, CA: Defense Personnel Security Research Center.

Hundley, R.O., Anderson, R.H., Bikson, T.K., Dewar, J.A., Green, J., Libicki, M., & Neu, D.R. (2000). *The global course of the information revolution: Political, economic, and social consequences.* Santa Monica, CA: Rand.

Internet Software Consortium. (2002) *The domain survey*. Retrieved June 15, 2002, from http://www.isc.org

Iwata, E. (2003, February 13). More U.S. trade secrets walk out the door with foreign spies. *USA Today,* 18.

Jacobs, D. (2000). Juvenile gambling in North America: An analysis of long-term trends and future prospects. *Journal of Gambling Studies, 16,* 119–-151.

Kipp, S. (2001). *Espionage and the insider*. San Francisco, CA: SANS Institute.

Kurtz, H. (1987, February 11). Pollard letter asserts "obligation" to spy: Abandonment by Israel is lamented. *The Washington Post,* B6.

Ladouceur, R., Dube, D., & Bujold, A. (1994). Prevalence of pathological gambling and related problems among college students in the Quebec Metropolitan Area. *Canadian Journal of Psychiatry, 39,* 289–293.

Massey, D. (1995). The new immigration and ethnicity in the United States. *Population and Development Review, 21,* 631–652.

Meyer, G., & Stadler, M. (1999). Criminal behavior associated with pathological gambling. *Journal of Gambling Studies, 15,* 29–43.

Morris, J., & Sherman, J. (1981). Generalizability of an attitudinal commitment model. *Academy of Management Journal, 24,* 512–526.

Moule, G. (1996). *A study of security countermeasures to reduce economic espionage in the United States from 1975 to 1996*. Retrieved August 8, 2002, from http://www.spybusters.com

Mossberg, W.S. (2003, November 12). A road test of 'keychain' drives. *The Wall Street Journal*, D4.

Mowday, R., Porter, L., & Steers, R. (1982). *Employee-organizational linkages: The psychology of commitment, absenteeism, and turnover*. New York: Academic Press.

Nadel, R. (2002). *Pair from Cupertino and San Jose, California, indicted for economic espionage and theft of trade secrets from Silicon Valley companies.* Retrieved June 12, 2002, from http://www.cybercrime.gov/yeIndict.htm

National Opinion Research Center. (1999). *Gambling impact and behavior study*. Report to the National Gambling Impact Study Commission. Washington, DC: Author.

National Science Board. (2000). *Science and engineering indicators – 2000* (NSB-00-1). Arlington, VA: National Science Foundation.

National Science Board. (2002). *Science and engineering indicators – 2002* (NSB-02-1). Arlington, VA: National Science Foundation, 2002.

National Security Agency. (1997). *Foreign intelligence recruitment approaches*. Washington, DC: Author.

National Security Agency. (2001). *Espionage: The threat is real.* Washington, DC: National Security Agency.

National Security Institute. (2002, June). U.S. security managers warned to brace for more terrorism, espionage. *National Security Institute Advisory, 17-11,* 7.

National Security Institute. (2002, November). Survey: U.S. firms lost up to $59 billion in proprietary information. *National Security Institute Advisory, 18-4,* 6.

National Counterintelligence Executive. (2000). *Annual report to Congress on foreign economic collection and industrial espionage.* Washington, DC: Author. Retrieved September 9, 2001, from http://www.ncix.gov/ pubs/pubs.html.

National Counterintelligence Executive. (2001). *Annual report to Congress on foreign economic collection and industrial espionage.* Washington, DC: National Counterintelligence Center. Retrieved October 28, 2001 from http://www. ncix.gov/ pubs/pubs.html

National Counterintelligence Executive. (2002, January 29). China: Journals urge use of overseas scientists for technology transfer. *News and Developments.* Retrieved October 28, 2001, from http://www.ncix.gov/news

Nockels, J. (2001). *Changing security issues for government*. Retrieved on December 12, 2001, from http://www.law.gov.au/SIG/papers /nockels.html

Office of Travel and Tourism Industries. (2004a). *International travelers to and from the U.S. 1993r-2003r*. Retrieved January 25, 2005, from http://www.tinet.ita.doc.gov/view/f-2003-05-001/index.html

Office of Travel and Tourism Industries. (2004b). *Forecast of international travel to the United States*. Retrieved January 25, 2005, from http://www.tinet.ita.doc.gov/view/f-2004-99-001/intlforecast.html

Office of Travel and Tourism Industries & Global Insight. (2003). *Forecast of top overseas travel markets to the United States*. Retrieved July 2, 2002, from http://tinet.ita.doc.gov/view/f-2000-99-001/forcastpage1.html

Overseas Security Advisory Council. (1992). *Guidelines for protecting U.S. business information overseas.* Washington, DC: Department of State.

Parker, J.P., & Wiskoff, M.F. (1991). *Temperament constructs related to betrayal of trust*. Monterey, CA: Defense Personnel Security Research Center.

Peak, M. (1995). Employees are our greatest asset and our worst headache! *Academy of Management Review, 84,* 47-51.

Potenza, M.N. (2002). A perspective on future directions in the prevention, treatment, and research of pathological gambling. *Psychiatric Annals, 32,* 203-207.

Poulson, K. (2001). Digital trail led to accused spy. *Security Focus News.* Retrieved September 9, 2003, from http://www.securityfocus.com/news/245

Quinn, J.B. (1996, February). A paycheck revolt in '96? *Newsweek*, *6*, 52.

Reichheld, F. (1996). *The loyalty effect: The hidden force behind growth, profits, and lasting value*. Boston: Harvard Business School Press.

Renshon, S. (2001). *Dual citizenship and American national identity.* Washington, DC: Center for Immigration Studies.

Robertson, R. (1992). *Globalization: Social theory and global culture*. London: Sage.

Rolling Good Times. (1999). *RGT: The premiere gaming E-Zine on the web*. Retrieved June 4, 2000, from http://www.rgtonline.com

Rousseau, D. (1995). *Psychological contracts in organizations: Understanding written and unwritten agreements*. New York: Sage.

Sarbin, T.R. (1994). A criminological approach to security violations. In T.R. Sarbin, R.M. Carney, & C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal*. Westport, CT: Praeger.

Sarbin, T.R. Carney, R.M., & Eoyang, C. (Eds.) (1994). *Citizen espionage: Studies in trust and betrayal.* Westport, CT: Praeger.

Saxenian, A., Motoyama, Y., & Quan, X. (2002). *Local and global networks of immigrant professionals in Silicon Valley.* San Francisco, CA: Public Policy Institute.

Schmidley, A. (2001). *Profile of the foreign-born population in the U.S.: 2000.* U.S. Census Bureau Current Population Reports, Series P23-206. Washington, DC: U.S. Government Printing Office.

Schweizer, P. (1996, January/February). The growth of economic espionage: America is target number one. *Foreign Affairs.* Retrieved July 4, 2003, from http://www.foreignaffairs.org

Shaffer, H. (1999). Strange bedfellows: A critical view of pathological gambling and addiction. *Addiction, 94*, 1445-1448.

Shaw, E.D., Ruby, K.G., & Post, J.M. (1998). The insider threat to information systems. *Security Awareness Bulletin, (2-98)*. Washington, DC: Department of Defense Security Institute.

Sullivan, T.A., Warren, E., & Westbrook, J.L. (2000). *The fragile middle class: Americans in debt.* New Haven: Yale University Press.

Thompson, W.N. (2001). *Gambling in America: An encyclopedia of history, issues, and society.* Santa Barbara, CA: ABC-Clio.

Thurman, J.N. (1999). Spying on America: It's a growth industry. *Christian Science Monitor, 80,* p. 1.

Timm, H.W. (1991). Who will spy? Five conditions must be met before an employee commits espionage. Here they are. Forewarned is forearmed. *Security Management,* 49-53.

Toffler, A. (1987). *The third wave.* New York: Random House.

Tulgan, B. (1996). *Managing Generation X: How to bring out the best in young talent.* New York: Capstone Publishing.

U.S. Department of Commerce. (2002, February). *A nation online: How Americans are expanding their use of the Internet.* Washington, DC: Author.

U.S. Department of Commerce. (2003). *U.S. international trade in goods and services.* Retrieved July 8, 2003, from http://www.census.gov/foreign-trade/Press-Release/2002pr/Final_Revisions_ 2002/#goods

U.S. Senate, 108th Congress. (2003). Senate Bill 1025, *Intelligence Authorization Act for FY2004.* Section 334.

U.S. Senate, 108th Congress. (2003) *Senate Report 108-44, Authorizing Appropriations for Fiscal year 2004 for Intelligence and Intelligence-Related Activities of the United States Government.*

Venzke, B. (2002). *Economic/ industrial espionage.* Retrieved June, 19, 2002, from http://www.infowar.com/class

Verton, D. (2001). Spy case demos insider threat. *Computerworld, 35,* 1-2.

Volberg, R. (2001). *When the chips are down: Problem gambling in America.* New York: Century Foundation Press.

Walker Information, Inc. (2000). *Halfway out the door: The Walker Information and Hudson Institute National Employee Relationship Report.* Indianapolis, IN: Author.

Wells, L. (2000). *The changing nature of information security in the Department of Defense.* Retrieved July 18, 2002, from http://www.cisp.org/imp/February_ 2000/02_00wells.htm

Whitelaw, K., & Enrich, D. (2001). Surfing for secrets. *U.S. News and World Report, 131*, 20.

Wise, D. (1995). The Ames spy hunt. *Time, 145,* 54-60.

Yang, P.Q. (1994). Explaining immigrant naturalization. *Immigrant Naturalization Review, 28,* 449-477.

Zacharia, J. (2000, December). A time to forgive? *The Jerusalem Post*, 7B.