International Journal of Intelligence and CounterIntelligence, 20: 50–64, 2007

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850600600888698

Routledge
Taylor & Francis Group

LISA A. KRAMER and RICHARDS J. HEUER JR.

America's Increased Vulnerability to Insider Espionage

Because espionage is a secret activity, it is not possible to know how many spies are currently active in American organizations or exactly what the future will bring in terms of discovered espionage cases. Nevertheless, it is possible to explore U.S. vulnerability to the crime of insider espionage by examining known factors that, on the basis of past experience, can serve to make insider espionage more or less likely to occur. A recent study has identified technological, social, and economic trends that are serving to increase the opportunity and motivation for insider espionage.[1]

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 an individual's choices and actions. While motivation for espionage results from a complex interaction between personality characteristics and situational factors,[2] the focus here is primarily on the latter. If more insiders are encountering situations that provide motivation and opportunity for espionage, the

Lisa A. Kramer is a Project Manager at the Department of Defense Personnel Security Research Center (PERSEREC) in Monterey, California. She has a Master's Degree in Psychology and a Ph.D. in Sociology. Her research interests include insider espionage, terrorism, counterintelligence, and social psychology. Richards J. Heuer Jr., a retired CIA officer, now conducts research for PERSEREC on the role of the personnel security system in mitigating the insider threat. He is the author of Psychology of Intelligence Analysis *(Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 1999). The opinions, conclusions, and recommendations expressed in this article are those of the authors and do not necessarily represent the views of PERSEREC or the Department of Defense.*

logical conclusion is that United States vulnerability to this crime is increasing.

TRENDS AFFECTING OPPORTUNITY FOR INSIDER ESPIONAGE

Technological Advancement 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 improve employee productivity also enhance employee capacity to gather information for the purposes of espionage. Two specific technological advances have particularly dramatic implications for spying: the development of large, networked databases with automated search functions and the miniaturization of data-storage devices. The increasing dependence upon networked databases exponentially increases the amount of information a single malicious insider can access. Automated search functions make it possible for insider spies to locate specific kinds of data—for example, information that is of particular value to foreign buyers. American spies who exploited large organizational databases include Aldrich Ames, Harold Nicholson, Brian Regan, and Robert Hanssen.

In addition to improved ability to locate specific types of information, rapid advances in the miniaturization of data storage devices make it easier for an insider to remove large quantities of information from an organization without being detected. The physical size and cost of memory sticks and flash drives are decreasing, yet the data storage capacities of these devices are expanding. As the miniaturization of storage hardware continues, the emergence of nanoscale devices—devices with structural features in the range of 1 to 100 nanometers—is likely. Potential future applications of nanoscale electronics include tiny data storage devices with capacities that are 1,000 times greater than those of today.[3] Numerous products now available do not look like data storage devices, but hold substantial sums of material. For example, the USB Memory Watch appears to be a normal timekeeping device, but it has a USB cable hidden in the band and the capacity to store up to 1 megabyte of data—around 22,000 pages of text.

An Expanding Market for Protected U.S. Information

As a result of America's status as a dominant political, economic, and military force, and the increasingly competitive global economy, foreign demand for protected U.S. information is increasing. American insiders now 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 than ever before. 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.[4]

Increasing demand for American proprietary information supplements an ongoing demand for classified information pertaining to information systems, sensors and lasers, electronics, aeronautics, armaments, energetic materials, marine and space systems, guidance systems, navigation and vehicle systems, signature control systems, space systems, nuclear systems technologies, chemical-biological systems, weapons effects and countermeasures, ground systems, and directed and kinetic energy systems.[5] In addition to foreign government representatives, 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.

As more allied and friendly countries pursue U.S. technological information, some insiders may find it easier to rationalize committing espionage. Other individuals who consider it reprehensible to sell American technology or military secrets to an avowed enemy of the United States may be less reluctant to sell this information to individuals or organizations in countries that are viewed as friendly to U.S. interests.

Internationalization of Scientific Research and Commerce

The globalization of business and scientific research is expanding the opportunity for espionage by increasing the frequency with which insiders are able to establish and maintain contact with foreigners interested in exploiting their knowledge. Relationships established through participation in joint research and business projects and attendant activities provide opportunities for Americans to share or sell classified information and make it easier for foreign entities to identify and recruit Americans with exploitable weaknesses. The frequency and nature of foreign scientific and business relationships also makes it more difficult for security and counterintelligence personnel to distinguish relationships that present a significant security risk from those which do not.

Participation in joint business ventures creates an environment that may be particularly conducive to espionage. According to Deputy Assistant Secretary of Defense Linton Wells, the inclination of those involved in multinational trade to regard the unauthorized transfer of information or technology as a business matter rather than an act of national betrayal or

treason may be growing.[6] Foreign business relationships commonly involve discussions in which sellers and buyers bargain over price, quantity, and quality. Providing sensitive information or working as a ''technical consultant'' can be a bargaining chip in these negotiations.

Collaboration on scientific 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, yet may find it difficult to determine exactly which information is protected and which is public. Some scientists believe that, in the spirit of furthering scientific discovery, research findings must be divulged.

Available data suggests that greater numbers of insiders routinely participate in collaborative international scientific and commercial endeavors, and that the number of international science and technology agreements being forged between the U.S. government and foreign counterparts is increasing over time.[7] The percentage of papers authored by U.S. scientists in conjunction with foreign scientists has been increasing steadily for decades.[8] Scientific collaboration between the United States and other countries is occurring more often in the private sector as well. The increasingly multinational nature of research and development is illustrated by the growing establishment of international research facilities.[9] Finally, the number of American organizations involved in the exportation of goods and services to foreign countries, and the value of these goods and services, have gone up dramatically in the last twenty years.[10]

Increasing Frequency of International Travel

Americans are making more visits abroad, and citizens of other nations are visiting the United States more often.[11] Increased frequency of international travel results in increased opportunity for the transfer of classified and other protected information to foreign entities. American insiders with access to valuable information are better able to establish contact with foreign buyers, and foreign nationals have more opportunity to spot, assess, and recruit American personnel. At the same time, while it is becoming easier for American sellers of information and foreign buyers to contact each other, security and counterintelligence personnel are experiencing greater difficulty in distinguishing between foreign travel and contacts that are of security concern.

Global Internet Expansion

Just as the Internet creates a large and efficient marketplace for exchanging a wide variety of products and services, it brings potential buyers and sellers together for the illegal sale of classified or other protected information. It

provides a means for potential buyers and sellers of information to establish contact, and constitutes an efficient and relatively secure mechanism for transmitting unlimited quantities of information across national boundaries. Sellers and buyers can interact without revealing their identities.

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. By 2004, the number of Internet hosts had grown to 233 million. 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.[12] Of the 200 million Internet search requests processed daily by Google, about two-thirds are initiated in languages other than English.[13]

TRENDS AFFECTING MOTIVATION FOR INSIDER ESPIONAGE

Motivation is a feeling or state of mind that influences a person's choices and actions. It often results from an interaction between personality characteristics and situational factors.[14] While most insiders with access to classified or other protected information do not possess characteristics that make them vulnerable to committing espionage under any circumstances, research suggests that some insiders can become motivated to commit espionage if they encounter situations in their personal or professional lives that make espionage appear attractive or viable. Motivation for spying can arise from situational factors such as experiencing a financial crisis or gambling addiction, becoming disgruntled with an employer, and having emotional ties to a foreign country or to a global community.[15]

Increasing Prevalence of Personal Financial Problems

Of the many factors known to provide motivation for insider espionage, experiencing personal financial stress is among the more prominent. Serious financial pressure may cause an individual to turn to theft, fraud, embezzlement, or other illegal behaviors—including espionage—in an effort to alleviate financial problems. Spies believed to have been 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, among others.

Credit card debt is playing an increasingly significant role in creating financial instability for Americans. Total American household credit now stands at 110 percent of annual disposable income—up from 76 percent in 1986.[16] Lending at high interest rates to individuals with poor credit

histories, or who are already burdened with debt, has become a major source of profits and one of the most rapidly growing segments of the consumer lending industry.[17] "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."[18]

Bankruptcy law was 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. In 1985, 341,000 personal 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. In 2003, filings reached 1.6 million.[19]

The bankruptcy law revision approved by Congress in 2005 will significantly increase the financial pressures on employees needing to file for bankruptcy due to unavoidable medical expenses, the loss of a job by a spouse, divorce, or irresponsible spending. Many Americans will no longer be able to liquidate debts by filing for bankruptcy under Chapter 7. They will instead have to file under Chapter 13, which requires full or partial payment of all debts over a 3–5 year period.

Increasing Prevalence of Compulsive Gambling

Moderate gambling, like sensible alcohol use, is an accepted part of contemporary U.S. culture. As with alcohol use, however, excessive gambling is not uncommon, and can lead to serious security problems. As access to funds becomes limited, compulsive gamblers become more desperate and can resort to crime to garner the money required to pay their debts and sustain their addiction.[20] The National Gambling Impact Study Commission, mandated by Congress to study the social and economic impact of gambling in the United States, found that 3 percent of American adults are pathological or problem gamblers and another 8 percent are at risk of developing a significant gambling problem. Compulsive gambling is reportedly the fastest growing addiction among both adults and youth.[21] The increasing prevalence of gambling addiction in the United States suggests that a growing number of insiders with access to classified or other protected information may become motivated to sell this information for personal profit.

Diminishing Organizational Loyalty

A lack of commitment to one's employer or the resentment of an employer resulting from real or perceived mistreatment, makes it easier for an insider to rationalize the theft and sale of the employer's information. Disgruntled insiders who have committed espionage involving the theft of classified information include John Charlton, John Allen Davies, Douglas Groat, and

Edwin Earl Pitts, among others.[22] Changing conditions in the American workplace suggest that organizational loyalty is diminishing, and that increasing numbers of employees may be at risk of becoming disgruntled.

In striving to compete in the global marketplace, American organizations more often engage in practices that can alienate personnel. They more often downsize, automate, transfer jobs overseas, and lay off employees. American employers increasingly hire part-time and temporary workers to whom they offer 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,'' where mistrust and anxiety replace feelings of fidelity to organizations.[23]

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.[24] In *Psychological Contracts in Organizations: Written and Unwritten Agreements*, Denise Rousseau explored employees' and employers' changing expectations and diminishing levels of commitment to one another. Rousseau concluded 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.[25]

Ethnic Diversification of the American Workforce

The growing number of insiders with foreign backgrounds and connections suggests that more of them will be in a position to provide classified or other protected information to foreign entities, and may more often become motivated to do so due to feelings of obligation or loyalty to the foreign country or foreign friends and relatives. Foreign intelligence organizations typically emphasize the recruitment of individuals with whom they share common national, ethnic, racial, or religious backgrounds.[26] Because more insiders have foreign ties, identifying insiders whose foreign connections pose a security risk is becoming more difficult.

The United States has experienced a profound demographic transformation in the last three decades, resulting in a substantial increase in the number of American citizens with relatives, friends, or business contacts residing in other nations. Emotional ties to family or friends in a foreign country, or to a foreign government, can result in conflicts of conscience. Insiders with foreign ties are in a better position to transfer U.S. information to foreign entities, 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.[27]

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. residents—about one fifth of the U.S. population—had one or more foreign-born parents.[28] The changing composition of the U.S. population is reflected in the composition of the American workforce in general, and the cleared Department of Defense (DoD) workforce specifically.[29]

A smaller proportion of immigrants apparently now 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.[30] An increasing percentage of immigrants choose to not become American citizens, and more of those who obtain U.S. citizenship retain citizenship elsewhere.[31] This change in attitudes toward citizenship may be fostered by dramatic improvements in the technology that allows for global communication. Immigrants who are able to maintain constant contact with family, friends, and news services in their native country are also more likely to retain emotional ties.

Growing Allegiance to a Global Community?

The increasing level of interaction between Americans and individuals of other nationalities appears to be resulting in a deeper global consciousness among U.S. citizens and a greater appreciation of other cultures, religious beliefs, and value systems.[32] Studies show that growing numbers of Americans—especially the younger generations of Americans—are bicultural, in that some aspects of their identity are rooted in local American traditions while other elements are rooted in an awareness of, and sense of belonging to, a larger global culture.[33] These Americans feel a sense of loyalty to both the United States and a global community.[34] They may even include within their global community people in countries that are currently conducting espionage against the United States. The increasing acceptance of global as well as national values may make it easier for a potential spy to rationalize actions that are actually driven by baser motives.

While many benefits are associated with Americans' greater awareness of the needs and interests of other peoples, and a perspective of the world as an interdependent system, this may, in extreme cases, lead to a conflict of conscience similar to that experienced by an American with dual national loyalties. The security risk that exists when an insider is bound by obligation or a sense of duty to a foreign government or to persons who are not citizens of the United States is well recognized. But the impact that globalization may have on national allegiance is not yet well understood.

Statements by a U.S. Defense Intelligence Agency (DIA) analyst recently convicted of espionage, 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 espionage. Owing to her belief in the moral righteousness of her actions, Montes expressed no remorse for helping Cuba ''defend itself'' against what she described as unfair and oppressive U.S. foreign policies. Montes stated 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 merely feel justified to commit espionage as a result of these beliefs; she felt morally obligated to do so.

UNDERSTANDING DEVELOPING TRENDS

Recognizing that these technological, social, and economic trends are converging and interacting to create an insider espionage risk greater than the sum of its parts is important (Figure 1). That is, the risk presented by

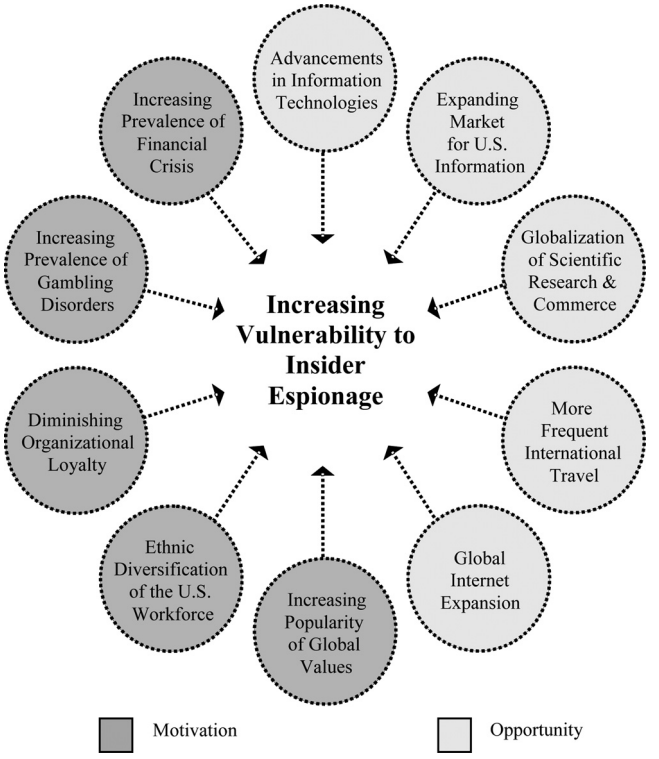

Figure 1. Technological, Social, and Economic Trends That Are Increasing Vulnerability to Insider Espionage.

each trend is exacerbated by the risk that results from the other trends. While a greater number of insiders have access to large networked databases, this fact is even more significant when they have this access *and* can sell more kinds of information to a broader range of foreign buyers . . . *and* have greater opportunity to establish contact with and transfer information to foreign entities . . . *and* are more vulnerable to experiencing financial crisis . . . *and* are more vulnerable to becoming disgruntled and less likely to feel an obligation to the organizations that employ them . . . *and* have close personal ties to other countries . . . *and* have a holistic view of the world that under some circumstances may result in their conceptualizing espionage as morally justifiable.

POLICY IMPLICATIONS

From a policy perspective, the obvious implication is that the vulnerability of U.S. government and industry to insider espionage is growing. While predicting what will actually transpire is not possible, a noteworthy aspect of our research is its inability to identify a single countervailing trend that will make insider espionage less likely to occur in the future.

Three disciplines share responsibility for mitigating the insider espionage threat:

(1) Personnel security: a program of due diligence that seeks to screen out potentially unreliable, untrustworthy, or disloyal individuals;
(2) Counterintelligence: which seeks to detect insider spies before they can inflict serious damage; and
(3) Information assurance: which protects information systems against attack from inside or outside organizations, and strives to identify anomalous activity that may indicate insider misuse.

Better collaboration among these three stove-piped disciplines is one means by which vulnerability to insider espionage can be reduced. Each discipline gathers items of information about the same body of cleared personnel, but these items are rarely, if ever, pieced together in a manner designed to identify security risks.

Lowering the Chance of Espionage

With respect to personnel security, the insider espionage threat can be reduced through (a) conducting more effective initial screening and continuing evaluation of personnel; (b) doing a better job of enlisting the support of coworkers and supervisors in identifying personnel who are engaging in behaviors of counterintelligence concern; and (c) assisting employees who are experiencing problems which, if unresolved, could provide motivation for espionage.

The security clearance process mitigates the risk of espionage in two ways. First, to the extent that it has a reputation for effectiveness, it deters undesirable people from seeking eligibility for access. Second, the initial background investigation and a periodic reinvestigation screen out some individuals with alcohol or drug problems, serious criminal records, records of financial irresponsibility, serious mental health issues, and those who are vulnerable to foreign influence or who have conflicting loyalties. New initiatives are needed to improve the security clearance process—especially to assess the loyalty of personnel with many foreign connections—but discussion of the required changes is beyond the scope of this article.

Observant supervisors and coworkers are often thought to be the first line of defense against the insider threat, but recent research shows that they often fail to recognize or report behaviors of significant security concern. Coworkers were found to be more likely to report on something when they see a direct link between a colleague's activities and national security interests. This indicates a need for organizations to clearly define a set of observable indicators that must always be reported, and to educate personnel about these indicators.[35]

The insider espionage risk can also be reduced by doing a better job of addressing a staff member's personal problems before they escalate to the level of becoming a security risk. Better training of supervisors is needed so they can recognize and deal with problem employees and can help resolve workplace conflicts before they lead to serious disgruntlement and a desire for revenge. Greater use of employee assistance programs (EAPs) may reduce the incidence of motivation for espionage.[36] Our research indicates that financial crises and gambling addiction are likely to be increasingly common. Employees must be helped to deal with these types of problems in the earliest stages, before they become desperate and at increased risk for taking drastic measures such as selling proprietary or classified information to alleviate financial crisis.

To the extent that the security screening, supervisor and coworker reporting, employee assistance, and other personnel security measures achieve their goals, fewer unprincipled, irresponsible, troubled, or disloyal personnel will gain or retain access to classified information. But these types of measures cannot eliminate all individuals who, under some unpredictable combination of circumstances, will choose to sell classified or other protected information. Due to the inherent difficulty of predicting human behavior, knowing which specific insiders will engage in espionage is impossible. Extensive research has been conducted with the goal of producing a valid profile of an American spy, yet studies have revealed no single, identifiable characteristic that all insider spies have in common.

Because even the most effective personnel security measures are limited in their capacity to mitigate the risk of insider espionage, to assume that classified and other protected information stored within large organizational databases is secure because all authorized users have a security clearance is both dangerous and naïve. Only one person is needed to compromise an entire information network. Thus, additional approaches to mitigating the insider threat are clearly needed, including a renewed emphasis on the compartmentation of information and need-to-know when authorizing access.

Optimism Possible

While information technology may be the most important single cause of increased risk of insider espionage, it may also be the nation's best hope for the future detection of offenders. From a security perspective, the great benefit of information technology is that its use leaves an audit trail. The audit trail can be programmed to provide early warning that a trusted insider may be engaged in an activity with security or counterintelligence implications.

Regarding the detection of offenders, the National Counterintelligence Strategy approved by President George W. Bush in March 2005 represents a promising step forward. It requires a shift from a reactive posture to a more proactive strategy to protect sensitive technologies and expose the activities of foreign intelligence collectors.[37] Historically, most American spies have been identified through the penetration of foreign intelligence services.

A few options for reducing the insider espionage threat have been presented here. Whether organizations pursue these or alternative approaches, action is clearly needed. If the United States is unable to meet the new challenges of protecting its classified and proprietary information, the country's security, military, and economic interests could be severely compromised.

REFERENCES

[1] Lisa A. Kramer and Richards J. Heuer Jr., *Technological, Social, and Economic Trends That are Increasing U.S. Vulnerability to Insider Espionage* (Monterey, CA: Defense Personnel Security Research Center, 2005). This report is available at http://www.fas.org/sgp/othergov/dod/insider.pdf

[2] Carson Eoyang, ''Models of Espionage,'' in Theodore S. Sarbin, Ralph M. Carney, and Carson Eoyang, eds., *Citizen Espionage: Studies in Trust and Betrayal* (Westport, CT: Praeger, 1994), pp. 69–91.

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

[4] Defense Security Service, *Technology Collection Trends in the U.S. Defense Industry* (Alexandria, VA: Defense Security Service, 2002).

[5] National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004* (Washington, DC: National Counterintelligence Executive, 2005).

[6] Linton Wells, *The Changing Nature of Information Security in the Department of Defense*, retrieved 18 July 2002, from www.cisp.org/imp/February_2000/02_00wells.htm

[7] *Federal Research: Information on International Science and Technology Agreements* (GAO/RCED-99-108) (Washington, DC: Government Accountability Office, 1999).

[8] National Science Board, *Science and engineering indicators–2002* (NSB-02 1).

[9] *Ibid.*

[10] *U.S. International Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, 2003), retrieved 8 July 2003, from www.census.gov/foreign-trade/Press-Release/2002pr/final_Revisions_2002/#goods

[11] Office of Travel and Tourism Industries, *International Travelers to and from the U.S. 1993r–2003r*, retrieved 25 January 2005 from www.tinet.ita.doc.gov, and Office of Travel and Tourism Industries, *Forecast of International Travel to the United States*, 2004, retrieved 25 January 2005 from www.tinet.ita.doc.gov/view/f-2004-99-001/intlforecast.html

[12] Marvin J. Cetron and Owen Davies, *Fifty Trends Now Changing the World* (Bethesda, MD: World Future Society, 2001).

[13] Thomas L. Friedman, "Is Google God?," *The New York Times*, 30 June 2003, retrieved 29 June 2003 from www.nytimes.com/2003/06/29/opinion/29FRIE.html

[14] Carson Eoyang, "Models of Espionage."

[15] Katherine L. Herbig and Martin F. Wiskoff, *Espionage Against the United States by American Citizens: 1947–2001* (Monterey, CA: Defense Personnel Security Research Center, 2002). This report is available at www.dss.mil/training/espionage/espionage_1947_2001.pdf

[16] Lou Dobbs, "In Hock to the Hilt," *U.S. News and World Report*, 21 July 2003, p. 36.

[17] Theresa A. Sullivan, Elizabeth Warren, and Jay L. Westbrook, *The Fragile Middle Class: Americans in Debt* (New Haven, CT: Yale University Press, 2001)

[18] *Ibid.*

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

[20] Lyn Bixby, "Thefts Feed a Casino Habit," *The Hartford Courant*, 23 August 2000, p. A8; Rachel Volberg, *When the Chips are Down: Problem Gambling in America* (New York: Century Foundation Press, 2001); Gerhard Meyer and Michael Stadler, "Criminal Behavior Associated with Pathological Gambling," *Journal of Gambling Studies*, No. 15, 1999, pp. 29–43.

[21] Dean Gerstein, John Hoffmann, Cindy Larison, Laszlo Engelman, Sally Murphy, Amanda Palmer, Lucian Chuchro, Marianna Toce, Robert Johnson, Tracy Buie, and Mary Ann Hill, *Gambling Impact and Behavior Study: Report to the National Gambling Impact Study Commission* (1999), retrieved on 27 April 2006, from http://cloud9.norc. uchicago.edu/dlib/ngis.htm

[22] Katherine L. Herbig and Martin F. Wiskoff, *Espionage Against the United States by American Citizens: 1947–2001*.

[23] Jane B. Quinn, "A Paycheck Revolt in '96?," *Newsweek*, No. 6, February 1996, p. 52; Frederick F. Reichheld, *The Loyalty Effect: The Hidden Force Behind Growth, Profits, and Lasting Value* (Boston: Harvard Business School Press, 1996).

[24] Bruce Tulgan, *Managing Generation X: How to Bring Out the Best in Young Talent* (New York: Capstone Publishing, 1996).

[25] Denise R. Rousseau, *Psychological Contracts in Organizations: Understanding Written and Unwritten Agreements* (New York: Sage, 1995).

[26] National Counterintelligence Executive, "China: Journals Urge Use of Overseas Scientists for Technology Transfer," *News and Developments*, 29 January 2002, retrieved 28 October, 2001, from http://www.ncix.gov/news

[27] AnnaLee Saxenian, Yasuyuki Motoyama, and Xiaohong Quan, *Local and Global Networks of Immigrant Professionals in Silicon Valley* (San Francisco: Public Policy Institute, 2002).

[28] Diane Schmidley, *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, 2001).

[29] Data provided by John Goral, Defense Manpower Data Center, Monterey, CA, 2002.

[30] Philip Yang, "Explaining Immigrant Naturalization," *Immigrant Naturalization Review*, No. 28, 1994, pp. 449–477.

[31] Douglas Massey, "The New Immigration and Ethnicity in the United States," *Population and Development Review*, No. 21, 1995, pp. 631–652; Scott Renshon, *Dual Citizenship and American National Identity* (Washington, DC: Center for Immigration Studies, 2001).

[32] Duane Elgin and Colleen LeDrew, *Global Consciousness Change: Indicators of an Emerging Paradigm* (San Anselmo, CA: Millennium Project, 1997); Anthony Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age* (Cambridge, England: Polity Press, 1991); Roland Robertson, *Globalization: Social Theory and Global Culture* (London: Sage, 1992).

[33] Jeffrey Arnett, "The Psychology of Globalization," *American Psychologist*, No.57, 2002, pp. 774–783; Duane Elgin and Colleen LeDrew, *Global Consciousness Change: Indicators of an Emerging Paradigm*; Anthony Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age*.

[34] Betty Jean Craige, *American Patriotism in a Global Society* (Albany: State University of New York Press, 1996).

[35] Two relevant PERSEREC reports are available: *Improving Supervisor and Coworker Reporting of Information of Security Concern* by Suzie Wood and Joanne Marshall-Mies (2003) and *Counterintelligence Reporting Essentials* by Kent Crawford, Suzie Wood, and Eric Lang (2004). The latter provides a succinct list of behaviors that indicate an individual may be engaging in insider espionage, and which coworkers and supervisors should be required to report. An electronic copy of either report is available by e-mail to perserec@osd.pentagon.mil

[36] Suzie Wood and Lynn Fischer, *Cleared DoD Employees at Risk: Public Options for Removing Barriers to Seeking Help*, Reports I and II (Monterey, CA: Defense Personnel Security Research Center, 2002).

[37] Office of the National Counterintelligence Executive, *National Counterintelligence Strategy of the United States, 2005*, retrieved 12 July 2005 from http://www.ncix.gov/whatsNew/index.html