Technical Report 08-05
March 2008

Changes in Espionage by Americans: 1947-2007

Katherine L. Herbig
Northrop Grumman Technical Services

Approved for Public Distribution: Distribution Unlimited
Defense Personnel Security Research Center

Technical Report 08-05 **March 2008**

Changes in Espionage by Americans: 1947-2007

Katherine L. Herbig, Northrop Grumman Technical Services

Released By – James A. Riedel

BACKGROUND

Since 1987, the Defense Personnel Security Research Center (PERSEREC) has maintained a database on espionage by American citizens based largely on open sources, and has collected files on each of the 173 individuals in the database. Espionage by Americans is the worst outcome for the personnel security system that works to reduce the risk of insider threat. Although its main focus is the personnel security system, PERSEREC monitors and analyzes espionage by Americans in order to improve understanding of this betrayal of trust by a small minority of citizens. This report is the third in a series of technical reports on espionage based on the PERSEREC Espionage Database, files of information from the press, and scholarship on espionage. The focus of this report is on changes and trends in espionage by Americans since 1990, compared with two earlier periods during the Cold War.

HIGHLIGHTS

This report documents changes and trends in American espionage since 1990. Its subjects are American citizens. Unlike two earlier reports in this series, individuals are compared across three groups based on when they began espionage activities. The three groups are defined as between 1947 and 1979, 1980 and 1989, and 1990 and 2007. The subset of cases that began since 2000 is given additional study. Findings include: since 1990 offenders are more likely to be naturalized citizens, and to have foreign attachments, connections, and ties. Their espionage is more likely to be motivated by divided loyalties. Twice as many American espionage offenders since 1990 have been civilians than members of the military, fewer held Top Secret while more held Secret clearances, and 37% had no security clearance giving them access to classified information. Two thirds of American spies since 1990 have volunteered. Since 1990, spying has not paid well: 80% of spies received no payment for espionage, and since 2000 it appears no one was paid. Six of the 11 most recent cases have involved terrorists, either as recipients of information, by persons working with accused terrorists at Guantanamo Bay, Cuba, or in protest against treatment of detainees there. Many recent spies relied on computers, electronic information retrieval and storage, and the Internet. The current espionage statutes have to stretch to cover recent cases that reflect the context of global terrorism.

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

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE	**Form Approved** **OMB No. 0704-0188**	

1. REPORT DATE: 13-03-2008	2. REPORT TYPE Technical Report 08-05	3. DATES COVERED Jan 1947 to July 2007

4. Changes in Espionage by Americans: 1947-2007	5a. CONTRACT NUMBER: 5b. GRANT NUMBER: 5c. PROGRAM ELEMENT NUMBER:
6. AUTHOR(S) Katherine L. Herbig	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 PERSEREC: Technical Report 08-05
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): PERSEREC 11. SPONSORING/MONITOR'S REPORT NUMBER(S): 08-05

12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited

13. SUPPLEMENTARY NOTES:

ABSTRACT: Espionage by Americans is the worst outcome of insider trust betrayal. The Defense Personnel Security Research Center (PERSEREC) monitors and analyzes espionage by Americans in order to improve understanding of such trust betrayal by a tiny minority of citizens. This is the third in a series of technical reports on espionage based on the PERSEREC Espionage Database, files of information from the press, and scholarship on espionage. The focus of this report is on changes and trends in espionage by Americans since 1990, compared with two earlier cold War periods. Findings include: offenders since 1990 are more likely to be naturalized citizens, and to have foreign attachments, connections, and ties, and therefore they are more likely to be motivated to spy from divided loyalties; money has declined as a primary motive for espionage although it is still common, and since 2000 no American is known to have received payment for spying; many recent spies have relied on computers, electronic information retrieval and storage, and the Internet. The most recent cases suggest that global terrorism is influencing the crime of espionage by Americans, and that espionage statutes need revision.

14. SUBJECT TERMS: espionage, security violations, spy, spying, espionage offenders

15. SECURITY CLASSIFICATION OF: UNCLASSIFIED			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 113	19a. NAME OF RESPONSIBLE PERSON: James A. Riedel, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-657-3000

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

PREFACE

The Defense Personnel Security Research Center (PERSEREC) was established in 1986 in the wake of numerous instances of espionage by Americans, culminating in the discovery of the extremely damaging espionage of John Walker and Jerry Whitworth the year before. Over the 20 years that PERSEREC has been working to improve the effectiveness, efficiency, and fairness of the DoD personnel and industrial security systems, the phenomenon of trust betrayal has remained an important research focus. This is the third in a series of unclassified reports based on information collected in the PERSEREC Espionage Database[1]. Materials on espionage and espionage-related offenses, including attempted espionage, conspiracy to commit espionage, and theft or collection of closely held national defense information with intent to commit espionage, have been coded into the PERSEREC Espionage Database since 1986. The automated database now holds data on 173 individuals whose activities span the 60 years from 1947 to 2007. Additionally, PERSEREC has built a collection of files based on press accounts, scholarly articles, and books documenting these cases. The three reports in this series (published in 1992, 2001, and the current report in 2008) are based on materials in the PERSEREC Espionage Database and on these files. Publishing unclassified reports facilitates a broad public distribution of analytical products about espionage, which furthers one of PERSEREC's goals, improving security education and awareness.

This report updates and expands on the two previous unclassified PERSEREC reports in the series. It also has a companion report, which is classified Secret, entitled *Espionage Indicators 1985-2005: A Review of Classified Data Sources*, by Lynn F. Fischer and John E. Leather (2007). The DoD Counterintelligence Field Activity (CIFA) sponsored the research that resulted in the current report and its classified companion. The intent in simultaneously developing two reports was to explore whether locating and collecting Secret-level data on instances of trust betrayal would add significant insights that were unavailable to an analysis based on open sources. Since PERSEREC's research focus is on the personnel security system, failures of that system link us to counterintelligence, and studies of counterintelligence have been a related research effort for PERSEREC. The opportunity offered by CIFA's support of these two reports to mesh PERSEREC's ongoing research on trust betrayal with research on counterintelligence indicators based on Secret sources has been successful, and may lead to other useful collaborations.

James A. Riedel

Director

[1] The PERSEREC Espionage Database contains some information that is For Official Use Only (FOUO), and therefore the database itself is FOUO. The particular information used in this report was unclassified, and this report is unclassified.

EXECUTIVE SUMMARY

This is the third report on espionage issued by the Defense Personnel Security Research Center (PERSEREC). It is based on the PERSEREC Espionage Database, which although largely derived from open sources, contains information that is For Official Use Only (FOUO). Although the Database is FOUO, this report relies on open sources and is approved for public release. The Database now includes 173 individuals in cases that range from 1947 through 2007.

This report compares three groups of espionage offenders defined by when they began espionage activities, not by when they were uncovered or arrested. The first two groups reflect a context in the Cold War between the United States and the Soviet Union, while the third group's context is the post-Cold War period. The three groups are: (1) those that began between 1947 and 1979; (2) those that began between 1980 and 1989; and (3) those that began since 1990. A subset of the last group, the 11 individuals who began since 2000, receives additional analysis.

The following summarizes a selection of the main findings in this report on changes and trends in known espionage by American citizens from the beginnings of the Cold War through mid-2007. It is likely more instances of espionage by Americans have yet to be detected. Examples drawn largely from cases in which individuals began espionage between 1990 and 2007 illustrate the findings in this report.

Personal Attributes

Most espionage by Americans is committed by men, but there have also been several women in each of the three cohorts studied in this report. Before 1990, most spies were white, while since 1990 less than half have been white. Since 1990 American spies have been far older than earlier cohorts: 83% were 30 years or older, and 46% were more than 40. It appears there has been a "graying" of the American spy in the recent past. Recent spies have had more years of schooling and held more advanced degrees than earlier cohorts. Recent spies are twice as likely to be married as single, and have been predominantly heterosexual.

Foreign Influences, Foreign Preferences, and Divided Loyalties

While before 1990, roughly 80% of American spies were native-born citizens, since 1990 the percentage of native-born offenders has fallen to 65%, while the corresponding percentage of naturalized citizens rose to 35%. Also since 1990, the percentage of American spies with foreign attachments (relatives or close friends overseas) increased to 58% and those with foreign business or professional connections jumped to 50%. From less than 10% before 1990 who had cultural ties to foreign countries, that percentage with foreign cultural ties increased to 50%. Divided loyalties, defined here as holding and acting on an allegiance to a foreign country or cause in addition to or in preference to allegiance to the United States, increased dramatically since 1990. Compared to the two earlier periods, in which divided loyalties were the sole motive for espionage by less than 20%, since 1990, 57% of Americans were motivated solely by divided loyalties. Increasingly, divided loyalties are a factor in motivating American espionage.

Employment and Clearance

During the two Cold War periods, equal numbers of civilians and members of the military engaged in espionage, while since 1990, 67% of spies have been civilians and only 33% have been members of the uniformed military. More individuals with jobs not typically associated with espionage, including a boat pilot, housewives, a truck driver, and two translators, have recently engaged in espionage. Since 1990, more persons have held Secret-level access, and fewer persons have held Top Secret access compared to the two Cold War periods. The proportion of those individuals who held no security clearance has increased steadily over time: from 20% before 1980, to 28% during the 1980s, to 37% since 1990. These individuals have used a variety of means to access protected information, including theft of information, reliance on others with access, stealing classified or sensitive information, or passing unclassified but sensitive information. The history of the evolution of the espionage statutes in the United States, and ambiguities with regard to their references to “national defense information” and “classified information,” explain why more people with no security clearance have been prosecuted for espionage.

Characteristics of Espionage

While before 1980, 90% of American spies succeeded in passing information, during the 1980s only about 60% of attempts at espionage were successful. Since 1990, the proportion that succeeded again has increased to 84%. Since 1990, 40% of spies were caught immediately or in less than 1 year, but for those who persisted, the duration of their espionage has been longer compared to the 1980s, with 41% spying for between 1 and 5 years, and 19% persisting for more than 5 years. The pattern established during the 1980s, in which two thirds of American spies volunteered and one third were recruited into espionage, has persisted since 1990: in the recent period, 67% volunteered to commit espionage. Among those recruited since 1990, almost two thirds were recruited into espionage by a foreign intelligence service. During the 1980s, when the Soviet Union was the main customer for American intelligence, 40% of American spies began their espionage by making contact with a foreign embassy. Since 1990, the use of embassies has decreased, while more individuals have chosen a new communications innovation: 13% of volunteers since 1990 turned to the Internet, including seven of the 11 most recent cases since 2000 that used the Internet to initiate offers of espionage.

The Soviets were the ultimate recipient for the information from 87% of individuals between 1947 and 1979, as they were for 75% of those during the 1980s. With the collapse of the Soviet Union in 1991, few Americans—only 15%— have sent information to Russia (the successor state) and no one passed information to former Eastern Bloc countries. Asian and Southeast Asian countries have become more common recipients of information from American espionage: from 5% in the early period, the proportion increased to 12% in the 1980s, and to 26% since 1990. Since 1990 there has been a notable increase in Central and South American countries as recipients of American information, especially Cuba.

Five Americans are known to have, or in one case are alleged to have, volunteered to spy for Al Qaeda or related terrorist groups since the mid-1980s.

Consequences of Espionage

Since 1990, American spies have been poorly paid. The proportion of those who received no payment at all increased from 34% before 1980, to 59% during the 1980s, and to 81% since 1990. Two factors seem responsible for this striking trend: during the 1980s, more spies were intercepted before they were paid, while since 1990 more spies have acted from divided loyalties and have refused payment. Although Americans have made less money at espionage over time, their chances of doing time in prison have increased. From 22% who served no time in prison in the period before 1980, only 7% and then 6% escaped prison terms in the later two periods. Over the three cohorts, there has been a shift in average prison terms to shorter sentences

Motivations

Since 1990, money has not been the primary motivation for espionage. While getting money was the sole motive for 47% of the first cohort and for 74% of the second cohort, since 1990, only 7% (which represents one individual) spied solely for the money. Money remained one of multiple motives in many cases in many recent cases as well.

Spying for divided loyalties is the motive that demonstrates the most significant change of all motives since 1990, with 57% spying solely as a result of divided loyalties. The third most common motive for Americans to commit espionage is disgruntlement. The proportion of Americans whose spying was prompted from disgruntlement was 16% in the early period, dropping to 6% in the 1980s, and rising again to 22% in the recent period. Smaller percentages of American spies held four other typical motives for espionage: ingratiation, coercion, thrills, and recognition or ego. Before 1980, foreign intelligence services applied coercion to recruit agents using blackmail that threatened relatives overseas, or entrapping Americans in sexual blackmail scams. No instances of coercion as a sole or primary motive appear in the database after 1980. A few individuals in each cohort have spied for the thrill of getting away with espionage or from the need to gain recognition and indulge their egos. Ambition for career advancement is notable as a motive in several of the most recent cases since 2000.

Vulnerabilities that Increase the Risk of Insider Threat

The 126 individuals in this study who are known to have held security clearances and signed nondisclosure agreements contracting with the United States government not to reveal classified or sensitive information are exemplars of the insider threat. The personnel security system attempts to screen out individuals who may prove less than loyal, trustworthy, and reliable using standards defined in the 13 *Adjudicative Guidelines.* Much of the data on security-relevant issues in the lives of espionage offenders is missing from open sources, but tentative trends for some security-relevant issues can be described.

Allegiance. Since 1990, the proportion of American spies demonstrating allegiance to a foreign country or cause more than doubled to 46% compared to the 21% in the two earlier cohorts, reinforcing the sense that globalization has had a noticeable impact and that the influence of foreign ties has become more important since 1990. Among those with competing commitments to another country or cause was the small proportion devoted to Communism: Communism claimed 14% of individuals before 1980, only 4% during the 1980s, and again 14% (five individuals) since 1990. The latter five persons spied for Cuba or for North Korea.

Misuse of Drugs or Illegal Drug Use. From 15% of spies between 1947 and 1970 known to have used misused drugs or used illegal drugs, the proportion jumped to 41% during the 1980s when the spy population shifted to younger, low-ranking military men. Since 1990, only one of the 37 individuals is known from open sources to have used illegal drugs,

Alcohol Abuse and Gambling. From a high of 30% between 1947 and 1979, the proportion of those known to be suffering from alcohol abuse declined to 24% during the 1980s, and to only 8% since 1990. Gambling addiction among American spies also declined over time to no instances in the group that began their espionage since 1990.

Foreign Influence, Foreign Preference, and Outside Activities. Variables capturing concern about foreign ties of various sorts are discussed in a separate section, but they are included in the discussion of *Adjudicative Guidelines* because three of the 13 guidelines focus directly on these issues (they are Foreign Influence, Foreign Preference, and Outside Activities), directing the attention of adjudicators to these concerns. The percentage of espionage offenders who had foreign relatives declined starting in the 1980s, while the percentage of those with foreign connections (business and professional associates) and foreign cultural ties remained roughly comparable at less than 20% across the two earlier periods. Since 1990, the percentage of those with foreign relatives increased to 41%, while about half of the 37 individuals had either foreign connections or foreign cultural ties, or both.

Financial Considerations. Roughly 12% of individuals in each of the three groups considered here lived a financially irresponsible lifestyle as reported in open sources. Two individuals in each cohort declared bankruptcy. Among financial problems Debt was the most common theme in each group: roughly one third of individuals in each time period resorted to espionage in part because of their debts.

Greed, on the other hand, figured less often in cases, in only 6% of cases before 1979 and in 11% of cases in the later two periods.

Life Events as Triggers for Espionage

Studies of espionage based on personal interviews with offenders suggest a pattern in which personal disruptions or crises precede, or “trigger,” an individual’s decision to commit espionage. Crises could be positive or negative, and include divorce, death, starting a new relationship, or exhibiting radically changed behavior. Commentators have speculated that if help or timely intervention had been offered in these cases, the crime might have been averted. There is a larger proportion of missing data for these variables than most others. It was determined that 57 of the 173 individuals in the PERSEREC Espionage Database, or 33%, had experienced one or more of these crisis events in their lives during the 6 to 8 months immediately before attempting espionage.

Prevalence of Spies

A chart depicts the number of spies known to be actively engaged in espionage in any given year between 1950 and 2007. It shows an increase to a peak in 1985, followed by a falling off in the numbers of active spies since 1985. It is a safe assumption that not all espionage by Americans has yet been detected, and of those who have been detected, it is clear that not all have been prosecuted, and those would not be included in the database. Since policies on prosecution of espionage have vacillated over time, the chart may reveal more about espionage prosecutions than about espionage itself.

The Most Recent Espionage by Americans

The 11 most recent instances of espionage-related activities by American citizens, those begun since 2000, are discussed in some detail. These cases include: Timothy Smith, Kenneth Ford, Jr., Ariel Weinmann, Lawrence Franklin, Leandro Aragoncillo, Ryan Anderson, Hassan Abujihaad, Ahmed Mehalba, Almaliki Nour, Shaaban Shaaban, and Mathew Diaz.

Patterns in the Most Recent Espionage by Americans

Much has changed over the first decade of the 21st century in the context, motives, customers, and means available to commit espionage. The 11 most recent cases that are discussed in this section are a subset of the larger cohort that began spying between 1990 and 2007. These cases tentatively suggest some directions espionage by American citizens may take, in turn suggesting counterintelligence approaches for the future. Keeping in mind the instability of any conclusions based on only 11 cases, these most recent cases of espionage by Americans demonstrate the following patterns.

More were naturalized citizens, and more had foreign attachments (relatives or close friends), foreign business connections, or foreign cultural ties. They were almost equally divided between civilians and uniformed members of the military. They were mostly volunteers; nine of 11 individuals volunteered. There were twice as many non-whites as white persons. Unlike the larger cohort that began spying since 1990, most of these individuals held security clearances.

A shift to terrorist recipients, or potential recipients, can be seen in that six of the 11 recent cases involved terrorist groups. A shift is apparent from earlier customers, prominently Russia, toward Middle Eastern customers during the Iraq War. For the first time, espionage has been successfully prosecuted against an American citizen for transmitting classified information to an American organization, in this instance, a legal defense group focusing on Guantanamo Bay detainees.

It appears that in none of the 11 most recent cases did the individual receive money as payment, although money was sought as one of several motives in five instances in which individuals did not succeed in being paid. The most common motivation among the 11 individuals was divided loyalties. Prison sentences for the nine of 11 individuals sentenced reverts to earlier patterns evident before 1990, and have been at least as severe as past sentences.

Disgruntlement was the second most common motive among cases since 1990, and ingratiation with persons who could offer status, favors, or power was the most common secondary motive. Acting from ambition, a form of seeking recognition or gratifying ego, and more stockpiling classified information for future use are two distinctive elements that appear in several of the 11 recent cases. Four individuals among the 11 recent cases had serious mental or emotional problems that contributed to their attempts to steal or pass classified information.

Ten of the 11 individuals used the computer in espionage, and two thirds of them, seven of 11, used the Internet, illustrating the transformation in information creation, storage, retrieval, and transfer in society is also being applied to espionage.

A Context for Espionage that Includes Global Terrorism

Before the dissolution of the Soviet Union in 1991, the contest between the West and international communism framed the context for espionage by Americans. Seen first in the 1980s and accelerating in later decades, terrorism began to replace communism as a cause that makes use of espionage. The phenomena of terrorism and espionage more often appear together in cases since 2000. Like terrorists, who have shifted to reliance on the Internet for communications in order to reach a global audience, recent espionage by Americans more often relies on the Internet and sophisticated use of information retrieval and storage.

The context of global terrorism adds another layer of complexity to the application of espionage statutes that date from 1917, and whose last major update by Congress was in 1950. Recent espionage cases involving stateless transnational groups illustrate the strain of how to sort out and apply to the current crime of espionage ambiguities in the current statutes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TABLES IN APPENDICES

INTRODUCTION

Espionage by Americans has been an important focus of research at the Defense Personnel Security Research Center (PERSEREC) since it was founded in 1986 in the wake of John Walker's arrest for spying. As one of the initial projects, PERSEREC developed a database of Americans involved in espionage against the United States since 1945. In 1992 the first report was published on espionage by 117 individuals, entitled *Americans Who Spied Against Their Country Since World War II* (Wood & Wiskoff, 1992). The goal of the ongoing project has been to analyze cases in terms of themes and trends that would further understanding of the phenomenon of espionage as an instance of trust betrayal, which is why it has focused on American citizens.

Since the first report was published in 1992, further instances of espionage by American citizens came to light, and these were entered into the PERSEREC Espionage Database. A second, updated report that incorporated additional cases and expanded the analyses was published in 2002, entitled *Espionage Against the United States by American Citizens, 1947 – 2001* (Herbig & Wiskoff, 2002). In this second report, the parameters of the database, and of the report on which it was based, were redefined to encompass Cold War cases and those that took place in the aftermath of the Cold War. A starting point of 1947 was designated in the second report, because 1947 was a time when the Cold War escalated in the conjunction of three crucial elements of American foreign policy: the Truman Doctrine, the Marshall Plan, and the passage of the National Security Act. This starting point allowed the inclusion of cases of espionage from the late 1940s that resembled those in the 1950s, and the exclusion of cases that were more like those that had occurred during the Second World War. The second study covered 150 individuals involved in espionage cases in the period 1947 through 2001.

This is the third report on espionage based on PERSEREC's Espionage Database. New cases since the second report was published in 2002 have been evaluated and entered into the PERSEREC Espionage Database, and some of the information added is For Official Use Only, which has made the PERSEREC Espionage Database itself FOUO, though this study remains unclassified. The database now includes 173 individuals in cases that range from 1947 through 2007. Unlike the two previous reports, the analyses in this report are based on when individuals began espionage-related activity, not when they were caught or arrested. Coincidentally, the period at which the second report cut off was some months before the terrorist attacks of 9/11/2001, so the current report considers how the context of espionage may have changed as a result of responses to global terrorism since 2000, and in particular since 9/11.

The PERSEREC Espionage Database has been and continues to be based largely on open-source materials available in scholarly articles and books, or in the press, with a small proportion of FOUO information. Focusing largely on open sources and producing unclassified reports allows the broad distribution of PERSEREC's reports on American espionage to any government agency and to the public interested in following specific cases or learning more about espionage in general. The 173 individuals in PERSEREC's Espionage Database were convicted or prosecuted for espionage, conspiracy to commit espionage, attempting to commit espionage, or for whom evidence of espionage or intent to commit espionage exists, even though for various reasons the person was not or has not yet been convicted of those crimes. This latter category includes people who defected before they were prosecuted, who died or committed suicide before they could be prosecuted, who were given immunity from prosecution, or who plea-bargained for lesser charges. Prosecutors often agree to plea bargains in espionage cases in exchange for information, because evidence required by some espionage statutes is lacking, or to protect counterintelligence methods or classified information from being discussed in open court. Lesser charges in plea bargains typically include conspiracy to communicate national defense information to a foreign government, acting as an agent of a foreign government, theft of government property, conspiracy to gather information knowing it would be useful to a foreign government, or even simple mishandling or storage of classified documents.

Outcomes of espionage cases are influenced not only by the charges against the offender and the plea bargaining undertaken on his or her behalf, but also by choices and policies on prosecution of espionage-related offenses. The 2002 PERSEREC report on espionage discussed trends in prosecution policies in some depth (Herbig & Wiskoff, 2002, pp. 6-12). In cases since 2001, a noticeable trend in prosecutions has been the increasing numbers of offenders who are not charged with espionage, but with acting as unregistered agents of a foreign power. The espionage statutes demand more stringent evidence of mental states and intentions for conviction than does acting as an agent of a foreign power, which may explain why the proportion of cases since 2000 that have been charged with acting as an agent of a foreign power is twice that in any earlier decades. Therefore, a fifth criterion for inclusion in PERSEREC's espionage studies has been added to the four that were operative in previous reports.

Current criteria for inclusion as a case in the PERSEREC Espionage Database are:

(1) Individuals convicted of espionage or conspiracy to commit espionage, or for attempting espionage, or for admitting that they intended to commit espionage,

(2) Individuals prosecuted for espionage but who committed suicide before the trial or sentencing could be completed,

(3) Individuals for whom clear evidence of espionage (actual or attempted) existed, even though they were not prosecuted. This category included cases involving defections, deaths at early stages in an investigation, and those administratively processed (e.g., allowed to retire, given immunity, exchanged, or discharged from the military),

(4) Individuals for whom clear evidence of actual or attempted espionage exists, who were initially charged with espionage-related crimes, but who were prosecuted for an offense other than espionage, such as mishandling classified information, as a result of plea bargaining,

(5) Individuals who were charged with acting as unregistered agents of a foreign power, and for whom evidence exists that they collected and intended, attempted, or succeeded in passing information to that foreign power.

METHODOLOGY

Information was compiled from newspaper and magazine accounts, biographies, general published works on espionage, and collections of case histories compiled by other researchers. On-line research tools, such as Lexis-Nexis, were consulted, as were Internet search engines that provided additional leads on information about the more obscure cases. Missing information was sought in the classified investigative files of several federal agencies that would confirm what was know, but except for a small proportion of information designated FOUO, for the most part unclassified information has been maintained in the database.

As in the earlier iterations of PERSEREC's Espionage Database, five categories of information were gathered on individuals identified for inclusion: biographical, employment and security clearance, characteristics of espionage, motivation, and consequences. Within these categories, variables were selected that would be available largely from open sources and that would provide a rich array of background data on spies. Included were personal and demographic information, aspects of the job environment, access to classified information, how they first got involved with espionage, how their careers as spies evolved, their mode of operation as spies, and how their spying careers ended. Information was collected on whether they volunteered or were recruited, and if recruited, by whom; on their motivations for committing espionage; and details on their indictment, conviction, and sentence. Some variables were included for identification and documentary purposes only and were not used for analysis. Some were qualifying descriptors for other variables, e.g., *foreign relative qualifier* provides details about the previous variable, *foreign relative*, which is just coded Yes, No or Unknown. More details on the coding procedures and considerations in the PERSEREC Espionage Database can be found by consulting the second report (Herbig & Wiskoff, 2002).

The 173 individuals and their activities that are recorded in the PERSEREC Espionage Database is a very small number of instances of any phenomena on which to apply statistical analysis. Descriptive statistics, in a comparison of frequencies, are the simple analytical tools used here on such small numbers. While undoubtedly there are more instances of espionage by Americans that have not been made public, and still more that have not been uncovered, these 173 represent all the known instances described in open sources that meet the criteria for inclusion defined here.

RESULTS AND DISCUSSION

This report differs from the earlier two in the series of PERSEREC espionage studies in that it is structured as a comparison across time periods based on when people began espionage-related activities, not as a comparison by selected traits. Rather than focusing analyses on whether individuals volunteered or were recruited, whether they were civilians or military, or whether they passed information or were intercepted, as in the earlier two, this report focuses on how characteristics and patterns have changed over time by comparing those traits across three time periods.

An assumption underlies the decision to structure the analysis by focusing on when a person began espionage, which is that in important ways, an individual's choice of action is influenced by the context of the time and place in which the person lives. On the one hand, the way in which it was possible to commit espionage in 1955 differed quite dramatically from the way espionage could be committed in 1985, and it was different again in 2005. On the other hand, basic elements of the crime of espionage persist across any period. One analysis argues that opportunity, conception, motive, lack of internal constraints, and ineffective external constraints are the necessary dimensions to commit espionage (Herbig, 1994). It is because such basic elements can be found in any act of espionage that one instance can be compared and contrasted with other instances to derive analytic categories and patterns that will be instructive across cases from any period. Yet it is equally important in an analysis of espionage to capture changes over time, and this is the goal here.

Two events define the time periods in which espionage has been analyzed in this study. One event is the collapse of the Soviet Union at the beginning of the 1990s (The collapse was slow-motion, from the fall of the Berlin Wall in November 1989 to dissolution of the Soviet Union as a government in December 1991); the other defining event is the rising incidence of terrorist attacks during the 1990s and accelerating since the turn of the millennium in 2000, culminating with the attacks on the World Trade Center and the Pentagon by Al Qaeda on 9/11/2001. Before the Soviet Union fell apart, it competed with the United States for more than four decades as our Cold War adversary, and it was the main customer for American information from spies. Having one main adversary and customer for American intelligence, and having it be the Soviet Union, shaped the context for espionage in the first two periods of this comparison. After the 9/11 attacks focused attention on the growing threat from terrorism, it tardily became apparent that Islamic terrorists organized in networked global cells posed a new, transnational intelligence threat, one whose challenges could be quite different from the Cold War parameters of two competing superpowers. Rather than repeat the analyses found in the previous two PERSEREC espionage reports, here the implicit question asked is "What has changed in espionage by American citizens since the fall of the Soviet Union after 1990 and with the rise of Islamic jihadism after 2000?"

RESULTS AND DISCUSSION

The individuals studied in this report have been categorized into three time periods by when they began their espionage-related activities, not by when they were uncovered or arrested. This allows for consideration of what impact the historical context of issues and pressures in a given period had on the person's decision to spy, alongside the personal context of his or her decision at that time. Comparisons are made across three groups, defined as those who began espionage-related activity between 1947 through 1979, those who began between 1980 through 1989, and those who began between 1990 through mid-2007. This scheme reflects insights from PERSEREC's two earlier espionage studies. The first two groups are Cold War cases, while the third group begins in the post-Cold War period, during the process of the disintegration of the Soviet Union. Cases that began in the 1980s have been separated out because espionage in those cases present distinct differences from the earlier Cold War decades.

This report is similar to the earlier two in its attempt to identify and highlight the counterintelligence implications of the cases of espionage discussed. Information was collected, if it was available, on personal traits that could serve as triggers for espionage, security concerns as defined by the *Adjudicative Guidelines* for access to classified information, indicators of possible espionage underway such as unexplained affluence, and details on motivations. Open sources are often deliberately vague on counterintelligence details and on the fine points of more obscure spies' lives, but all available open-source information was sought and collected as a starting point for counterintelligence analysis.

In these analyses, results are usually first reported in tables. The text accompanying the tables draws attention to highlights of the results rather than trying to describe all of the results. Discussion is integrated into each topical section and includes implications, examples of cases, and other observations. Examples and illustrations are drawn from the information available in PERSEREC's files of articles on individuals who are coded in the database. Most of the examples summarized here are drawn from the group of individuals who began espionage-related activities between 1990 and 2007. In addition, several individuals who were arrested during that period but who had begun their activities earlier are also described, either because they are especially apt examples or because their espionage is deserving of more study. On the one hand, the examples have been developed into brief thumbnail sketches of cases rather than mere references illustrating a trait in order to broaden public awareness of espionage. On the other hand, some of the most damaging instances of espionage that have already been analyzed in depth in publicly available sources, such as Robert Hanssen or Aldrich Ames, are not described again here. For a complete list of the names and several selected variables of cases coded in the PERSEREC Espionage Database that were the basis of this report, see Appendix A.

PERSONAL ATTRIBUTES

Table 1
Personal Attributes

Characteristics	1947-1979		1980-1989		1990-2007	
	n=66	*%*	*n=70*	*%*	*n=37*	*%*
Gender						
Male	63	95	63	90	32	86
Female	3	5	7	10	5	14
Race or ethnicity						
White	59	89	59	84	17	46
Black	5	7	2	4	4	11
Arab	0	0	1	1	3	8
Asian	1	2	4	6	4	11
Hispanic	1	2	3	4	9	24
Native American	0	0	1	1	0	0
Age when espionage began			*(n=69)*		*(n=35)*	
Less than 20	3	5	6	9	0	0
20 to 29	24	36	34	49	6	17
30 to 39	22	33	12	17	13	37
40 or more	17	26	17	25	16	46
Education, in years	*(n=64)*		*(n=65)*		*(n=20)*	
10 years	4	6	5	7	0	0
12 years	23	36	24	37	7	35
14 years	13	20	13	20	1	5
16 years	17	27	7	11	5	25
18 years	7	11	16	25	7	35
Marital status when espionage began			*(n=65)*		*(n=32)*	
Married	46	70	31	48	21	66
Single	16	24	26	40	7	22
Separated or divorced	4	6	8	12	4	12
Sexual preference	*(n=59)*		*(n=51)*		*(n=32)*	
Heterosexual	55	93	49	96	32	100
Homosexual	4	7	2	4	0	0

Table 1 compares various personal attributes across the three time periods to explore how the demographic characteristics of American spies may have changed. Across the six decades of this study, espionage by Americans has been a crime committed mostly by men, but there has been a small but steady increase in female participation. In the cohort of cases since 1990, the proportion of women increased to 14%. Since 1990 five women began spying; they include Maria del Rosario Casas Ames, Virginia Baynes, Linda Hernandez, Geneva Jones, and Katrina Leung. Leung's prosecution was dismissed for prosecutorial misconduct.

Aldrich Ames' wife Maria became a witting accomplice late in her husband's espionage career, a career that lasted from 1985 to 1994. She began to accompany him on drops, openly enjoyed the financial fruits of his crime, and plotted with him on how best to hide the money ("Spy suspects," 1994; Johnston, 1994). Baynes, Hernandez, and Jones were active accomplices who collected information for their male partners. Baynes, a secretary for the Central Intelligence Agency (CIA) in Manila, the Philippines, in the early 1990s, and Jones, a secretary for the State Department in Washington, DC, during the same period, each held the classified access on which they and their partners relied (Defense Personnel Security Research Center, 2004; Cummings, 1994). Hernandez was a Cuban foreign agent working alongside her husband, Nilo Hernandez, in the south Florida exile communities, but the couple only passed publicly available information back to Cuba (Rosenberg, 1998; Davison, 1998). Leung began working for the Federal Bureau of Investigation (FBI) in 1982 as a source of information about China, but her loyalties were turned by the Chinese in 1990 and she began passing information to China that she surreptitiously took from her FBI handler, J.J. Smith. She seduced both Smith and another FBI handler and maintained both of them as long-term lovers. Leung was probably a damaging foreign agent, but ambiguities in a plea bargain by the prosecutors led a federal judge to throw her trial out of court in January 2005, and Leung pled guilty only of lying to the FBI and tax evasion (Rosenzweig, 2005; Geis, 2006; Department of Justice Office of the Inspector General, 2006; LeFebvre, 2005).

The racial and ethnic composition of American spies reflects some recent expansion in opportunities for non-Caucasians to participate in responsible positions with access to classified or sensitive information. Most spies before 1990 were white, but since 1990 less than half have been white (46%). Among American citizens who were black, or of Arab or Asian descent, representation in each of those categories of espionage more than doubled since 1990, and espionage by Hispanics increased to one quarter of the total.[2] The latter reflects the activities of Cuban intelligence in particular in sending agents into the United States, such as the five individuals who were naturalized American citizens among the "Red Avispa" cases, and the advantage taken by Cuba of overtures by volunteers in the cases of Mario Faget,

---

[2] Every 10 years, the United States Census Bureau wrestles with how to categorize "race" among Americans who are often racial mixtures, and who confuse ethnicity and race when they self-report. The 2000 census defined the following categories as racial groups using these terms: White, Black or African American, American Indian and Alaska Native, Asian, Native Hawaiian and Other Pacific Islander, and Some Other Race, which the Census Bureau thought should apply to persons of Hispanic origin since, they explained, Hispanics could be any race (Grieco & Cassidy, 2001). Consistent racial categorizing is a quagmire. This database field is coded with racial or ethnic terms that reflect the 173 individuals being described. White, Asian, Native American, and Black are commonly used racial categories, while Arab and Hispanic are ethnic or even linguistic categories, but they describe a person's general cultural heritage.

Ana Montes, and Carlos and Elsa Alvarez, (Rosenberg, 1999 [Red Avispa]); Bragg, 2000 [Faget]; Golden, 2002 [Montes]; Weaver, 2007 [Alvarez].

The age at which individuals began espionage has changed markedly across the three time periods. The 66 individuals who began spying between 1947 and 1979 were fairly evenly divided between those in their 20s, 30s, and 40s. Americans who began espionage during the 1980s were younger, and therefore were less experienced in work and in life in general, which apparently led to their being caught in attempts at espionage more often than earlier or later cohorts. Almost 60% of the 1980s group was less than 30 years old. In contrast, the recent cohort that began spying since 1990 is older than either of the earlier groups. Eighty-three percent of these 37 individuals were 30 years or older, and almost 46% were more than 40. It appears there has been a "graying" of the American spy since 1990, though the 11 individuals in cases since 2000 again divide evenly among age cohorts as did the earliest cohort.

American spies have spent more time in school over time. Slightly more than 33% of individuals in each of the three cohorts were high school graduates, but the percentage of those with master's degrees or other postgraduate professional education has increased to 60% in the recent cohort, while for the previous two groups that advanced level of education was typical for only about 30%.

Patterns in the marital status of Americans who committed espionage reflect the increasing incidence of divorce in American society over the last 30 years. Divorce doubled among spies in the 1980s when compared to the earlier group, and divorce remained at that level, 12%, into the 1990s. The 1980s stand out as anomalous because more young, white, native-born members of the military volunteered to spy for money and were often caught at it, and this is reflected in the marital status of the 1980s cohort: there is a drop of 25% in the number of married individuals when compared to earlier decades, and a concomitant increase of 15% in those who were single (Herbig & Wiskoff, 2002).

Lastly in this table, sexual preference is reported if there was any indication of it in the open source materials consulted. There are more missing data for this variable, but it appears that heterosexuals engage in espionage at rates that reflect their percentage in the general American population, that is, between 94 and 97% of the total (Black, Gates, Sanders & Taylor, 2000). Rates of espionage by homosexuals in the two earlier periods, 7% and 4%, and the absence of any instances of known homosexuality among the 37 individuals in the recent cohort since 1990, bear out the conclusion that homosexuality cannot be considered a particular vulnerability of security concern leading to espionage.

FOREIGN INFLUENCE, FOREIGN PREFERENCE, AND DIVIDED LOYALTIES

Table 2
Foreign Influences

Characteristics	1947-1979		1980-1989		1990-2007	
	n=66	***%***	***n=70***	***%***	***n=37***	***%***
Citizenship						
Born in U.S.	52	79	59	84	24	65
Naturalized	14	21	11	16	13	35
Had foreign attachments						
Yes	35	53	24	34	21	58
No or unknown	31	47	46	66	16	42
Had foreign connections						
Yes	10	15	12	17	19	51
No or unknown	56	85	58	83	18	49
Had foreign cultural ties						
Yes	0	0	7	10	18	49
No or unknown	66	100	63	90	19	51

Table 2 suggests that since 1990, globalization and immigration patterns have been shaping American espionage in important ways. The four variables in this table show trends toward less homogeneity in the American population, and this is reflected among Americans who spy. There is also more contact with foreigners among persons who used their access to classified or sensitive information for espionage. Roughly 80% of espionage offenders before 1980 were native-born, and that percentage rose to 84% during the 1980s with an influx into espionage of young, white, male, native-born members of the military. Between 1990 and 2007, the percentage of native-born espionage offenders fell to 65%, while the corresponding percentage of naturalized citizens rose to 35%. A recent example of attempted espionage by a naturalized citizen and successful businessman is the case of John Joungwoong Yai, arrested early in 2003, who sent only publicly available information to North Korea for at least 3 years while he plotted to get access to classified information for himself and worked to plant young Koreans in jobs that would have access to classified information to serve as his collectors. Yai communicated with and took taskings from his North Korean handlers in coded messages by fax, email, and in meetings with them in Europe, China, and North

Korea where they paid him for his efforts. He pled guilty to acting as an agent of a foreign power and to several counts of customs violations for failure to declare his earnings on reentry into the United States from meetings with his handlers. In February 2003, Yai was sentenced to 2 years in prison (Krikorian, 2003; Federal Bureau of Investigation, Affidavit, 2002).

The three variables on foreign contact shown in Table 2 attempt to capture different kinds of ties with countries other than the United States: (1) Foreign attachments were coded for persons with relatives or close, long-term friends abroad; (2) Foreign connections were defined as business or professional associates abroad; (3) Foreign cultural ties were coded as those with evidence of ongoing relatedness to another country, such as making repeated visits, sending money back, participating in native associations or clubs, and speaking that foreign language at home. A person with foreign attachments or connections was usually also coded as having foreign cultural ties if there were indications that the person actively kept up such ties, so foreign cultural ties is the most comprehensive of the three variables, and an individual may be coded in more than one variable.

The number of American espionage offenders with foreign attachments fell during the 1980s, to one third, from the earlier proportion of slightly more than one half with such attachments. During the recent period since 1990, the percentage with foreign attachments increased to more than half, to 58%. The other two variables, foreign connections and foreign cultural ties, also show an abrupt rise since 1990: from less than 20% of offenders with foreign connections before 1990, the percentage jumped to more than 50% in the recent period. From none to 10% who had cultural ties to foreign countries before 1990, the percentage jumped to almost 50% who had such ties since 1990. As the process of globalization continues, economics opens and makes more accessible world markets, while the communications revolution supports access to and ongoing relationships with persons overseas. Societies become more integrated with one another, and this is generating more roles for interaction and connection than had existed in earlier periods (Treverton, 2005). Espionage by Americans reflects those larger trends.

The counterintelligence concern over persons with foreign ties having eligibility for access to classified or sensitive information is the potential for divided loyalties, that is, an allegiance to another country or cause in addition to the United States, a preference for interests other than those of the United States, and the possibility for a betrayal of American interests that divided loyalties could cause. Awareness that a person with access to national security information could secretly harbor and act on loyalty to a competing country or cause—the cause at the time was international Communism—has haunted American federal personnel security policy since 1953 with the founding Executive Order 10450. That order required that when hiring a federal employee, background information must include whether a person could be coerced into betraying information through pressure on overseas relatives or by blackmail, and whether a person was “performing or attempting to perform his duties, or otherwise acting, so as to serve the interest of another government in preference to the interests of the United States” (Executive Order 10450, 1953).

Since 1953, eligibility policies for access to classified information have been repeatedly refined in order to apply this goal of discerning divided loyalties by weighing evidence that would reveal such a potential. The current policy on personnel vetting for access, *Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, based on Executive Order 12968 as amended, was issued in December 2005. These now guide adjudicators across the federal government when they evaluate security concerns in 13 areas about applicants for access to classified information. Four of the *Adjudicative Guidelines* concern potential divided loyalties, which make it the issue with the most guidelines: they are allegiance to the United States, foreign influence, foreign preference, and outside activities.

Furthermore, the attacks of 9/11 have reoriented and focused attention on issues of divided loyalties and how they could threaten national security. One element in the new security environment, exacerbated by the wars in Iraq and Afghanistan, has been a need for many more individuals with skill in languages that have rarely been taught in American schools (Department of Defense, 2005). This need puts a premium on immigrant and naturalized native speakers (“heritage Americans”), and as their numbers with access have increased, concern has increased about how to predict their loyalties. A second element in the post-9/11 environment has been the recasting of the 1950s concern about Communist sympathies into concern about an applicant’s sympathies with global terrorist groups or jihadist causes. As a result, adjudicative policies and investigative standards are again under study for potential revision in an effort to make the background investigators more effective collectors of information and the adjudicators more discerning of issues of divided loyalties (Heuer, 2007; Krofchek & Gelles, 2005; Foreign Associations Ad Hoc Working Group, 2006).

Table 3
Incidence of Divided Loyalties as a Motive for Espionage

Characteristics	**1947-1979**		**1980-1989**		**1990-2007**	
	n=66	*%*	*n=70*	*%*	*n=37*	*%*
Persons with a sole motive	43	65	35	50	14	38
Divided loyalties was the sole motive (ex.: 7/43 = 16%)	7	16	4	11	8	57
All other sole motives (ex.: 36/43=84%)	36	84	31	89	6	43
Persons with multiple motives	23	35	35	50	23	62
Divided loyalties was among multiple motives (ex.: 8/23 = 35%)	8	35	10	29	12	52
Divided loyalties was primary among multiple motives (ex.: 6/23 = 26%)	6	26	5	14	9	39

The proportion of American espionage offenders whose motives included divided loyalties has increased considerably in the recent period.[3] Table 3 shows that in the recent period more individuals held divided loyalties than in the two earlier periods for all three variables. Among persons whose motive was solely divided loyalties (16% before 1980 and 11% between 1980 and 1989), the proportion of these individuals jumped to 57% since 1990.

Among persons who demonstrated multiple motives, the proportion of those whose motives included divided loyalties was 35% in the first group, declining slightly to 29% in the second group; it then increased to 52% since 1990. For individuals whose primary motive among multiple motives was divided loyalties, percentages for the earlier groups of 26% before 1980 and 14% between 1980 and 1989 contrast with an increase to 39% since 1990. Among American espionage offenders, divided loyalties are increasingly prompting their acts of betrayal.

An example of an American spy acting from divided loyalties who had many ties to another country is Robert Chae-gon Kim. He was arrested in September 1996, and charged with passing classified documents to a South Korean naval attaché stationed in Washington, DC. Kim worked as a civilian computer specialist analyzing international ship traffic in the Office of Naval Intelligence, in the same Suitland, MD, office in which Jonathan Pollard had worked and spied for Israel a decade earlier. Kim offered his services as a spy to South Korean officials, and also worked with his brother on a scheme to reverse-engineer a military computer system and sell it to the South Korean government, for which he took out export licenses before he was arrested. Kim pled guilty to conspiracy to commit espionage and was sentenced in July 1997 to 9 years in prison, to be followed by 3 years of supervised release. He served 7 years in prison, and returned to his home to Virginia; meanwhile the South Korean media had already lionized Kim. In South Korea people took up collections to pay him, the mistreated “patriot”—who was still an American citizen—a generous salary for each of the years he had spent in prison, and encouraged him to return “home” to Korea as soon as he served out his probation (Scofield, 2004; Johnston, 1996).

Not all American espionage offenders motivated by divided loyalties have been naturalized citizens with relatives or business connections abroad. An example is Frederick Christopher Hamilton, who served as a Defense Intelligence Agency (DIA) research technician in the American defense attaché’s office in Lima, Peru, from 1989 until 1991. Fluent in both Spanish and Portuguese, Hamilton allowed himself to be cajoled into handing over to Ecuadorian officials classified Secret intelligence reports evaluating the Peruvian military, which revealed sources and methods. He

[3]Motives were coded in the PERSEREC Espionage Database with the intent to capture all known motives of an individual, to make a judgment on what was the primary motive, to make a ranking of secondary motives, and to determine what if any were “continuing” motives, that is, motives that were not present at first but that kept the individual at espionage once engaged in it. Since each person may have one or more motives coded, there are more instances of the various motives than there are individuals in the database.

believed his actions would avert a war between Ecuador and Peru. His concern for these South American countries, coupled with a susceptibility to flattery, led Hamilton to hand over the highly sensitive reports. He pled guilty in a plea bargain in February 1993 to two counts of unlawfully communicating classified information to a foreign power, and was sentenced to 3 years in prison (Gertz, 1993).

EMPLOYMENT AND CLEARANCE

Table 4
Employment and Clearance

Characteristics	1947-1979		1980-1989		1990-2007	
	n=66	*%*	*n=70*	*%*	*n=37*	*%*
Civilian or uniformed military						
Civilian	32	48	35	50	26	70
Uniformed military	34	52	35	50	11	30
Rank of uniformed military	*n=33*		*n=33*		*n=9*	
E1 – E3	3	9	10	30	2	22
E4 – E6	16	49	18	55	3	34
E7 - WO	10	30	3	9	2	22
Officer	4	12	2	6	2	22
Type of employment during espionage					*n=35*	
Uniformed military	34	52	35	50	11	31
Civil servant	14	21	14	20	12	34
Government contractor	7	10	8	11	3	9
Job unrelated to espionage	11	17	13	19	9	26
Occupational field when espionage began					*n=36*	
Communications/intelligence	25	38	22	31	6	16
General/technical	10	15	23	33	10	28
Scientific/professional	16	24	12	17	6	17
Functional support/administrative	12	18	9	13	5	14
Miscellaneous	3	5	4	6	9	25
Security clearance when espionage began	*n=61*		*n=67*		*n=35*	
Top secret SCI	10	16	10	15	6	17
Top secret	28	46	19	28	7	20
Secret	10	16	16	24	9	26
Confidential	1	2	3	5	0	0
None held during espionage	12	20	19	28	13	37

In Table 4 variables are compared relating to changes in occupations and levels of security clearance among American espionage offenders over the past six decades. The first factor that has changed in the recent period is the proportion of uniformed military personnel compared to civilians who committed espionage-related offenses. While in the first two periods this proportion was evenly divided between civilians and military, since 1990 there have been more than twice as many civilians as members of the military, with 70% civilians and 30% uniformed military. The pattern of distribution in rank among military offenders shows a shift to the lower ranks during the 1980s as more young enlisted men tried espionage, and a return to a more evenly distributed ranking among the nine military offenders since 1990. Comparing types of employment, the uniformed military dropped from one half to one third of offenders since 1990, the proportion of government contractors remained the same at roughly 10%, and the proportion of civil servants and of those whose jobs were unrelated to their espionage both increased over time.

Shifts in the occupational fields in which espionage offenders have been employed suggest a trend toward the broadening of categories of information that are classified or considered sensitive. The proportion of communications and intelligence specialists has decreased by half from the earliest period to that beginning in 1990, while individuals in general and technical fields doubled between the first and second periods to roughly one third of the total and have remained at that level since 1990. The proportions of those in scientific or professional fields and those in support or administration have remained about the same over time, but the percentage of persons in miscellaneous jobs has increased from 5 or 6% in the earlier periods to 25% since 1990.

It is suggestive to consider how persons engaged in an increasingly broad range of occupations since 1990 have been able to commit espionage-related crimes. To illustrate the increase in miscellaneous types of employment since 1990, Table 5 lists the types of employment, or lack thereof, which have been coded under “miscellaneous” in the PERSEREC Espionage Database.

Table 5
Miscellaneous Occupations of Espionage Offenders

1947-1979	1980-1989	1990-2007
1. unemployed	1. unemployed	1. boat pilot
2. drug dealer	2. unemployed	2. housewife and student
3. retired	3. housewife	3. Taekwondo instructor
	4. occupation unknown	4. unemployed
		5. housewife
		6.entrepreneur and organizer
		7. truck driver
		8. shop owner
		9. Arabic translator
		10. Arabic translator

The last variable reported in Table 4 is trends in the level of security clearance held when the offender began espionage. The proportion of those with access to Top Secret-Sensitive Compartmented Information (TS-SCI) has held steady over the six decades of this study at 15 to 17%. The proportion of those with Top Secret access has declined over time, from 46% in the first period, to 28% and then to 20% in the latter two periods. The number of individuals holding Secret level access has increased over time from 16% before 1980 to 24% during the 1980s, to 26% after 1990; the Confidential category, never held by more than a few persons in the database, has shrunk to nothing after 1990 as the Confidential classification has fallen into disuse.

The potentially most interesting finding about this variable is the proportion of those individuals who held no current security clearance and had no authorized access to classified information when they committed espionage-related offenses. This group increased from 20% before 1980, to 28% during the 1980s, and to 37%— more than one third of the total—since 1990.

Three elements are required in order to grant eligibility for a security clearance and to receive access to classified information: (1) demonstrating eligibility in a process that includes a background investigation and an adjudicative decision under the authority of a government agency head; (2) the signing of a nondisclosure agreement that legally binds the clearance holder in a contract to uphold the security requirements for the information; and (3) having a need to know specific classified information as determined by a local agency that holds that information (Executive Order 12958, as amended, 2003). Yet it is wrong to assume that espionage-related offenses have been or can be committed only by security clearance holders, or that compromised information that earns an espionage-related prosecution has to be classified. Table 6 lists the names of 44 individuals who held no security clearance at the start of espionage activity, but who have been prosecuted for espionage-related offenses. Also shown in Table 6 are the decades in which the individuals began their activities, either the method of access they used or the type of information they betrayed, and the outcome or sentence they received. Seven of these 44 individuals had had security clearances and access to classified information at some time in the past; the remaining 37 had not held security clearances and did not themselves have access to classified information.

Table 6
Espionage Offenders with No Security Clearance When Espionage Began

Decade Began Espionage	Name	Method of Access or Type of Information in the Case	Outcome or Sentence
1940s	Rees, Norman	Passed unclassified information	Suicide
1950s	Borger, Harold	Accomplice with access	2.5 years in prison
	Cascio, Guiseppe	Accomplice with access	20 years in prison
1960s	Harris, Ulysses	Accomplice with access	7 years in prison
	Sattler, James	Accomplices with access	Defection
1970s	Lee, Andrew	Accomplice with access	Life in prison
	Harper, James	Accomplice with access	Life in prison
	Clark, James	Accomplice with access	12 years 8 months in prison
	Stand, Kurt	Accomplice with access	17 years and 6 months in prison
	Tumanova, Svetlana	Passed unclassified information	1.5 years in prison
	Alvarez, Carlos	Passed unclassified information	5 years in prison and 3 years probation
	Barnett, David	Relied on memory of classified information	18 years in prison
1980s	Pickering, Jeffrey	Stole classified information	5 years in prison
	Jeffries, Randy	Stole classified information	3 years in prison
	Kota, Subrahmanyam	Stole classified information	1 year in prison and 3 years probation
	Wilmoth, James	Stole classified information	35 years in prison reduced to 20 years
	Wolff, Jay	Stole classified information	5 years in prison
	Davies, Allen	Relied on memory of classified information	5 years in prison
	Slavens, Brian	Relied on memory of classified information	2 years in prison
	Howard, Edward	Relied on memory of classified information	Defection
	Smith, Richard	Relied on memory of classified information	Released
	Pelton, Ronald	Relied on memory of classified information	Life in prison
	Buchanan, Edward	Claimed access to classified information	2 years and 6 months in prison

Decade Began Espionage	Name	Method of Access or Type of Information in the Case	Outcome or Sentence
	Irene, Dale	Accomplice with access	2 years in prison
	King, Donald	Accomplice with access	30 years in prison
	Tobias, Bruce	Accomplice with access	5 months in prison
	Chiu, Rebecca	Accomplice with access	3 years in prison, renounce U.S. citizenship and deportation
	Pizzo, Francis	Accomplice with access	10 years in prison
	Pollard, Anne	Accomplice with access	5 years in prison
	Mortati, Thomas	Accomplices with access	1 year and 8 months in prison
	Alvarez, Elsa	Passed unclassified information	3 years in prison and 1 year of probation
1990s	Ames, Rosario	Accomplice with access	5 years in prison
	Brown, Joseph	Accomplice with access	6 years in prison
	Leung, Katrina	Accomplice with access	Released as a result of prosecutorial misconduct
	Yai, John	Passed unclassified information	2 years in prison and $20,000 fine
	Guerrero, Antonio	Passed unclassified information	Life in prison
	Hernandez, Linda	Passed unclassified information	7 years in prison
	Hernandez, Nilo	Passed unclassified information	7 years in prison
	Santos, Joseph	Passed unclassified information	4 years in prison
	Alonso, Alejandro	Passed unclassified information	7 years in prison
	Groat, Douglas	Relied on memory of classified information	5 years in prison and 3 years of probation
	Sombolay, Albert	Stole restricted, but not classified, information and equipment	34 years in prison
2000s	Shaaban, Shaaban	Claimed access to classified information	13 years in prison
	Smith, Timothy	Stole classified information	3 years and 10 months in prison

How did they do it? Table 6 lists six scenarios for access used by those with no current security clearance at the time of their espionage-related activities. Some relied on family or friends who did have access, serving as their accomplices. One example is Rebecca Laiwah Chiu, wife of Chi Mak, sister-in-law of Tai Mak and his wife, their son Billy's aunt—five members of the Chi Mak extended family convicted of working together to commit various violations of export control laws and to acting as agents of a foreign power, China. Chi Mak admitted that he had been sending information on military technology to China since 1983 while working as an electrical engineer on U.S. Navy contracts, most recently at Power Paragon, a defense contractor in Anaheim, CA. Thousands of pages of documents on sensitive military research and development that had been stolen from his workplace were found in Mak's home (Reza, 2007a). Among the technologies the ring compromised to China were advanced propulsion systems for both submarines and warships that reduced the detectable noise they produce and information on new technologies in the Navy's next generation of destroyers and aircraft carriers (Gertz, 2007). Lawyers wrangled for a long time in court over the nature of the documents and files Mak stole and sent to China, since although many were marked NOFORN, the documents were not marked classified, despite Mak holding a Secret clearance.[4]

Initial charges of espionage were dropped in favor of charges of illegal export and foreign agency because the defense established that the particular documents in the case were not classified. Testimony at Mak's trial offered insight into the pattern of China's uniquely patient approach to espionage: "It depends on a multitude of relative amateurs," counterintelligence officers testified, "Chinese students and visiting scientists, plus people of Chinese heritage living in the United States. Each individual may produce only a small bit of data. But collectively the network might vacuum up an extensive amount of sensitive military and economic information" (Grier, 2005). Searches of the Mak home found torn-up lists of specific technologies typed in Chinese characters, apparently taskings of what Mak's Chinese handler wanted to see next from the ring (Flaccus, 2007a).

Mak and his wife Chiu became naturalized American citizens in 1985, while their three relatives in the case remained resident aliens. The brother, Tai Mak, and his wife acted as couriers and go-betweens, flying to China with documents from Mak

[4] The Mak ring case illustrates the disappearing distinction between national defense information and technical research information controlled by corporate contractors who develop defense applications of all sorts for the United States government. Several related issues make the distinction between passing national defense information and sharing or selling corporate research information difficult: some technologies are "dual use" and at some stage can be applied to defense weapons systems or to civilian projects; some technologies that are in early stages of development are not yet designated as defense-related, and therefore not classified, in order to facilitate the exchange of information with other companies and agencies, yet when mature such technologies will become defense-related and classified. Selling them off at an early stage may not be espionage, while selling them at a later stage may be. China's information-gathering program among defense contractors is cited as particularly effective, as are many others. The nest of conceptual and legal issues in the increasingly close conjunction of economic espionage and national defense espionage requires further research and analysis (Hawkins, 2007; Mazzetti & Lewis, 2007; Meyer, 2007; Cho & Cha, 2007).

on compact disks encrypted by their son. A jury found Mak guilty in May 2007 of conspiracy to export controlled defense technology to China, acting as an agent of a foreign power, attempting to violate export control laws, and lying to the FBI (Flaccus, 2007b). Chiu's witting participation in the collection and transmittal of information, and her awareness of its illegality, was documented by the FBI through electronic surveillance in the Mak home for months. She pled guilty just before her trial was to start in a plea bargain to acting as an agent of China without registering, and was sentenced to 3 years in prison. She also agreed to renounce her American citizenship and be deported to China once she is released (United States District Court for the Central District of California, Grand Jury Indictment, 2005; Reza, 2007b). Sentencing for Chi Mak was scheduled for the fall of 2007, but as of March 2008 it had not yet occurred.

A number of American citizens convicted of espionage-related offenses acted as agents of a foreign power by collecting information that was not classified but which could be procured by observation or by mining public sources. The government objected to such information being compiled and deliberately passed into the hands of a foreign intelligence service or a government research agency by persons acting as an agent for them. An example of this is the prosecution of the Cuban spy ring operating in southern Florida from 1992 until the arrest of 10 of its members in September 1998. Five of the 10 were American citizens, and therefore are subjects in this study. The ring, nicknamed the Wasp Network (in Spanish "La Red Avispa"), was led by three Cuban nationals who were officers in Cuban military intelligence; the five Cuban-American agents recruited to make observations and report to the ringleaders were trained in Cold War era espionage techniques and methods—including code names, encryption pads, fake identification documents hidden in book covers, shortwave radios, and pages of secret codes on dissolving paper (Rosenberg, 1999). The information they passed, however, was from direct observations and public knowledge, and was unclassified, despite the agents' best efforts to get jobs inside military installations that would give them better access (Davison, 1998). They sent hundreds of reports on movements, exercises, visible forces, and plane patterns as seen near MacDill Air Force Base near Tampa, FL, Naval Air Station Key West, FL, and Southern Command headquarters in Miami, FL. They also tried to infiltrate Cuban émigré groups to spy on their intentions toward Cuba (Pressley, 1998; Rosenberg, 1999). Four of the five Americans took plea bargains, pled guilty to acting as agents of a foreign power, and served 4 to 7 years in prison. Antonio Guerrero stood trial with four Cuban nationals, and he was found guilty of conspiracy to commit espionage, despite the fact that no classified information was involved in these cases. He was sentenced to life in prison in late December 2001 (Borger, 2001; "Five Cubans convicted," 2001).[5]

[5] A federal appeals court overturned Antonio Guerrero's life sentence in August 2005, along with the sentences of the four Cuban nationals whose trials date from the same period, on the grounds that these defendants could not have received a fair trial in southern Florida with its population of anti-Castro immigrants and the inflamed climate of public opinion at that time. The five remain in prison in 2007 as likely flight risks, while federal prosecutors decide whether to mount another

Some people simply stole classified information and intended or attempted to profit from the theft. Others stole information or objects that were closely held or restricted from public distribution by the government, but were not actually classified. Albert Sombolay, an Army cannon crewman stationed in Germany in 1990, was an example of someone who provided restricted, but not classified, materials to a foreign government. He provided deployment information on U.S. forces, military ID cards, and examples of protective equipment against chemical warfare to the Jordanian embassy in Brussels, promising them that when he was deployed to Saudi Arabia shortly during Operation Desert Storm, he would videotape American positions and equipment and send the tapes to them. He also offered these services to the Iraqi embassy in Bonn, West Germany, which did not respond. Sombolay was a native of Zaire who became a naturalized citizen in 1978 and joined the U.S. Army in 1985. Although he claimed to support the "Arab cause" in the first Gulf War, money and disgruntlement were stronger motives for his efforts to sell his stolen equipment and information. Sombolay pled guilty to espionage and contacting the enemy, and was sentenced to 34 years at hard labor ("U.S. soldier convicted," 1991; Holthaus, 1991; Brodie, 1991). A more recent example of theft of classified information for sale is Timothy Smith, whose case is discussed in more detail below. Smith stole computer diskettes from an officer's desk, intending to sell the information to customers he expected to find on the Internet (Skolnik, 2000).

Others relied on their memories of information they had worked with previously once they no longer had access to that classified information. Ronald Pelton is an example of this method, in a case that dates from the 1980s. Pelton telephoned the Soviets in 1980 offering to sell them information in order to deal with his bankruptcy. Over a series of meetings, he shared his broad knowledge of National Security Agency (NSA) intelligence activities gleaned from years of employment at the agency. Pelton's debriefings by the Soviets involved no documents; he relied on his remarkable memory to relay the details of communications intelligence operations that allowed the Soviets to counter information channels that had cost U.S. intelligence agencies "hundreds of millions of dollars" to initiate (Engelberg, 1986).

Douglas Groat offers an example from the 1990s of a spy who relied on his memory of information to which he had access in the past when he had held a security clearance. Groat had worked for the CIA for 16 years as a burgler—one of the agency's operatives whose very secretive job was to break into foreign embassies abroad and steal codes, cipher systems, and computer chips used to secretly communicate with their nations' capitals (Weiner, 1998b). Groat became increasingly disgruntled and resentful about his treatment and lack of promotion at CIA. In 1993, he was suspended from the agency and cut off from access to

---

trial. Meanwhile "The Cuban Five" have become heroes in Cuba, supported by groups that demand their release, and they have become a cause for pro-Cuba groups in the United States (Yanez, 2005; Weaver, 2005; Williams, 2005).

classified information. The CIA did offer him a substitute job and a settlement, however, from fear that unless he kept his silence, he could destroy the sensitive operations in which he had been involved. Groat rejected the offers, left his wife, and spent 3 years traveling the West alone in a recreational vehicle, while he conducted telephone negotiations with the agency and the FBI over his demands for enormous payments, reinstatement, hearings, and immunity. In 1997, Groat went to two foreign embassies in the Washington, DC, area and revealed what he knew from personal experience about the CIA's methods of "targeting and the compromise of the cryptographic systems" they used (Weiner, 1998b, 1998a). He was arrested in April 1998 and charged with espionage. In September he accepted a plea bargain in which the espionage charges were dropped, and instead he pled guilty to extortion for threatening to reveal more secrets unless he were paid $1 million. He was sentenced to 5 years in prison, and allowed to keep his CIA pension (Weiner, 1998c; "National news briefs," 1998).

Finally, two individuals claimed that they had access to classified information, and tried to make money on their claims, when in fact they did not have access. Still they were prosecuted and convicted of espionage-related offenses. Edward Buchanan is the only instance of someone who began laying the groundwork for committing espionage while his TS/SCI clearance was still being processed, before he had any access. Airman Buchanan was still in training at Lowry AFB, CO, in April 1985 when he began sending letters to the East German and Soviet embassies in the United States offering to sell them classified information. He followed up with phone calls. The Air Force Office of Special Investigations (AFOSI) set up a sting, and AFOSI agents met Buchanan pretending to be Soviets. Buchanan told them he wanted to set up a long-term and profitable relationship selling secrets, and he "sold" the agents unclassified data from an electronics magazine for $1000. He was arrested at the scene. Interviews revealed that Buchanan was painfully immature and naïve; once he had his access to classified information, he intended to commit espionage long enough to make the money he needed "to live comfortably," then he planned to defect and live in the Soviet Union.[6] He was court-martialed and sentenced to 2½ years in prison, forfeiture of all pay and allowances, and a dishonorable discharge (Crawford, 1998).

The other individual who claimed an access he apparently did not have is Shaaban Shaaban, whose case is discussed in more detail below. He offered to sell the names of all CIA agents working undercover in Iraq to Saddam Hussein's intelligence agents in 2002. Despite failing to produce any names, Shaaban was convicted in 2006 of acting as an agent of a foreign power and various other charges, and was sentenced to 13 years in prison (Corcoran, 2006b).

[6] This childlike fantasy is strikingly similar to the plans Ariel Weinmann made for himself in 2000. See the case description for Weinmann below.

Table 7
Frequency of Methods of Access for Espionage Offenders with No Current Clearance

Method of Access or Type of Information in the Case	n=44	%
Accomplice with access	18	41
Passed unclassified information	10	23
Relied on memory of classified information	7	16
Stole classified information	6	14
Claimed access to classified information	2	4
Stole restricted, but unclassified, information and equipment	1	2

Table 7 compares the frequency of the six methods by which individuals with no access themselves to classified information managed to commit espionage. Relying on an accomplice who did have access was the most common situation, accounting for 41% of the instances. Passing unclassified but sensitive information accounted for the second most common category, in 23% of the cases. Relying on memory based on past access described seven cases, 16%, stealing classified information without having access accounted for six cases, 14%, falsely claiming access accounted for two cases, and stealing restricted, but not classified, information and equipment characterized one case.

Individuals can commit espionage without themselves having access to classified information, in the various permutations discussed here, in part because of legal ambiguities in the espionage statutes of the United States. The laws have evolved from the early 20th century without benefit of reconciliation between the existing and the new. Statutes now governing espionage date from the first effort to protect the government's secrets in the Defense Secrets Act of 1911. The Espionage Act of 1917 adopted the approach taken in 1911, incorporating many of its key phrases. Most of the 1917 act in turn has been incorporated without many revisions into 18 U.S. Code 793, the core statute for dealing with espionage. The last revisions in wording made to section 793 were in 1950 with the Internal Security Act; also in that act 18 U.S. Code 794 was added. Over the nearly 100 years of use and interpretation, the legal framework for espionage has grown complicated and potentially contradictory. New provisions have been added to deal with new contingencies, but little restructuring of the original framework was done, nor were attempts made to reconcile new provisions to existing statutes (Edgar & Schmidt, 1973).

The language that comes down from the 1917 act makes it a crime to disclose or attempt to disclose national defense information to the injury of the United States or to the advantage of a foreign power. It does not specify classified information, since classification of information was not standardized and widely used until during World War II, starting with an executive order in 1940 (Elsea, 2006a). Subsequent laws added protection for intelligence sources and methods, information about nuclear energy or nuclear weapons, patents the government determined should be controlled, codes and cryptographic information and methods, communications information and methods, and more. The Economic Espionage Act of 1996 added protection for "trade secrets." Some of the later statutes retained the language of the 1917 Espionage Act by referring to the protection of national defense information, while other provisions referred to classified information (Elsea, 2006b). Appendix B lists the main espionage-related statutes by title and reference, but as many observers have noted, the scattered, overlapping, and contradictory statutes governing espionage activities cry out for reorganization and revision by Congress (Epstein, 2007; Barandes, 2007). This discussion points up the fact that some persons who held no security clearance and had no current access to classified information have been convicted of espionage-related offenses, and that it is quite possible to be convicted of espionage–related offenses for collecting and passing unclassified information. Foreign agents are often recruited and sustained in countries of interest to collect publicly available information. The distinction between the broader category of "national defense information" and the narrower category of "classified information" is necessary to keep in mind in studying espionage and its related offenses.

CHARACTERISTICS OF ESPIONAGE

Table 8
Characteristics of Espionage

Characteristics	1947-1979		1980-1989		1990-2007	
	n=66	***%***	***n=70***	***%***	***n=37***	***%***
Intercepted or passed information						
Intercepted	6	9	29	41	6	16
Passed information	60	91	41	59	31	84
Duration						
Intercepted	6	9	29	41	6	16
Less than 1 year	14	21	10	14	9	24
1 to 4.9 years	23	35	16	23	15	41
5 or more years	23	35	15	22	7	19
Volunteer or recruit	*n=65*				*n=35*	
Volunteer	34	52	46	66	22	63
Recruited	31	48	24	34	13	37
Recruited by	*n=31*		*n=22*		*n=13*	
Family	2	7	3	14	1	8
Foreign Intelligence	24	77	10	45	8	62
Friend	5	16	9	41	4	30
Method used to begin espionage	*n=64*		*n=69*		*n=30*	
Contact foreign agent	8	13	10	15	2	7
Contact foreign embassy	17	27	28	41	9	30
Go-between	6	9	3	4	0	0
Other methods	2	3	3	4	2	7
Internet	0	0	1	1	4	13
Recruited	31	48	24	35	13	43
Location where espionage began	*n=64*		*n=69*			
Outside U.S.	26	40	16	23	9	24
U.S. east coast	28	44	24	35	18	49
U.S. west coast	5	8	18	26	6	16
Other locations in U.S.	5	8	11	16	4	11
Location where espionage began, outside the U.S.	*n=26*		*n=16*		*n=9*	
Western Europe	21	81	2	12	1	11
Asia and Southeast Asia	3	11	3	19	3	33
Eastern Bloc/Soviet Union	2	8	10	63	0	0
Africa	0	0	1	6	0	0
Middle East	0	0	0	0	2	23
Central and South America	0	0	0	0	3	33

Characteristics	1947-1979		1980-1989		1990-2007	
Number of individuals passing information to recipient regions	*n=65*		*n=65*		*n=36*	
Western Europe	2	3	3	5	2	6
Soviet Union/Russia	42	65	38	58	5	14
Eastern Bloc	14	22	11	17	0	0
Asia and Southeast Asia	3	5	8	12	9	25
Africa	1	1	2	3	1	3
Middle East	2	3	0	0	6	16
Central or South America	1	1	2	3	8	22
Al Qaeda	0	0	1	2	4	11
USA (sent to a legal aid organization for Guantanamo Bay detainees)	0	0	0	0	1	3

Table 8 summarizes variables that describe how selected characteristics of the act of espionage itself by Americans have changed over time. The rate of interception or discovery before information could be passed highlights one of the ways in which the 1980s differed from both the earlier and later periods. While 90% of individuals before 1980 did pass information, during the 1980s only about 60% of espionage attempts were successful in passing information. A larger proportion of young, inexperienced members of the military tried espionage in the 1980s, driving the rate of interception up. After 1990, the proportion of those who did pass information increased again to 84%. A number of factors could underlie their increased rate of success, including the shift to older, better educated individuals among those who began espionage since 1990, and the post-Cold War context in which instead of the Soviet Union as the one main competitor, many different countries target the United States for intelligence, providing more foreign customers for the fruits of espionage by Americans.

Duration of espionage careers by Americans also reflects this pattern in which the 1980s are anomalous. Before 1980, lengths of espionage career broke down roughly into thirds: one third was caught immediately or within 1 year, one third spied for between 1 and 5 years, and one third spied for more than 5 years, sometimes for decades. During the 1980s, this proportion shifted toward a shorter duration, in which 55% were caught before they had spied for 1 year, 23% persisted between 1 and 5 years, and another 22% spied for more than 5 years. Since 1990, American spies as a group again have shifted toward more prolonged espionage careers compared to the 1980s: for the most recent cohort, 40% were caught immediately or within 1 year, another 41% spied for 1 to 5 years, and 19% continued for more than 5 years. As more offenders who began in the recent period are brought to light, these proportions may change.

The pattern over time of whether Americans volunteered or were recruited into espionage does not follow that of the previous two variables. Between 1947 and 1979, roughly half of American spies were recruited, the other half volunteered. During the 1980s, this proportion shifted as more individuals volunteered, and the pattern showed that two thirds volunteered and one third of them were recruited. This pattern has largely persisted into the recent period, with 63% volunteers and 37% recruits (for one individual in the recent period, it is unclear from open sources whether he volunteered or was recruited).

Changes over time in who was recruiting Americans into espionage were also analyzed. The numbers of those known to have been recruited, whether by a family member, a friend, or a foreign intelligence service, are comparatively small. In the early period intelligence services were the predominant recruiters, when these services lured 77% of the 31 recruited spies into espionage. That proportion dropped to 45% of the 22 recruits during the 1980s, when more young military men convinced their buddies to get into the game with them and several notorious family spy rings—notably the Walkers—came to light. Since 1990, foreign intelligence services have again become the recruiting source for the majority of the 13 recruits, with 62% of recruits to their “credit.”

Shifts over time in methods by which individuals began spying reflect the end of the Cold War and the appearance of the Internet. The two most popular methods to initiate an offer to spy have been to contact a foreign intelligence agent directly, or to contact a foreign embassy. During the 1980s, when the Soviet Union was the main customer for American intelligence, 40% of volunteers began their espionage by telephoning or walking into an embassy. Since 1990, the use of embassies has decreased, while more would-be spies have taken advantage of innovations in communications, including the 13% who chose the Internet to initiate their offers of espionage.

In considering the locations in which individuals initiated or were recruited for espionage, certain locations have been more frequent than others. In the early period, more espionage began overseas than in the two later periods; from two fifths of persons who began overseas, the proportion declined in the 1980s, as well as in the recent past, to one quarter. East Coast locations in the United States predominated in both the earlier and latest periods, in nearly one half the instances, while during the 1980s, the choice of locations was more evenly divided between East and West Coasts and other U.S. venues. Intelligence agencies and government and military headquarters are concentrated on the East Coast and around the national capital, and this geographical clustering probably explains the focus for more espionage attempts on the East Coast.

Of those who initiated espionage from locations outside the United States, the shift in venues between time periods is dramatic. Between 1947 and 1979, four fifths of overseas espionage initiatives occurred in Western Europe. During the 1980s the focus shifted to the Eastern Bloc and the Soviet Union, with two thirds acting from those locations. Since 1990, the small subset (nine individuals) of those initiating espionage from overseas has been spread around the globe: three initiated espionage from Asia or southeast Asia, three from Central or South America, two from the Middle East—a first appearance for that region as a location from which to initiate espionage—and only one from Western Europe. Over the three time periods, initiatives from Asian locations have increased steadily from 11% before 1980, to 19% during the 1980s, to 33% in the most recent period.

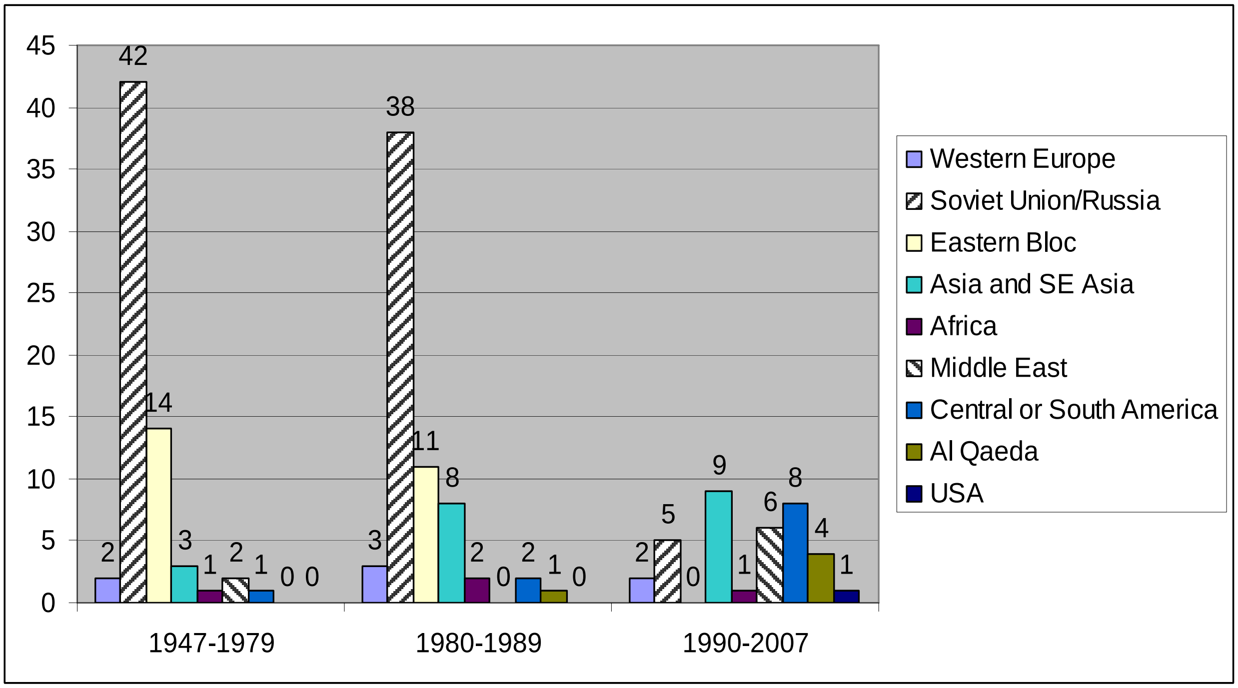

Figure 1 Number of American Spies Sending Information to Various Recipients by Region

The final variable in Table 8 compares the regions or countries to which individuals have sent or tried to send information during espionage. The same information is depicted in chart form in Figure 1. The predominance of the Soviet Union as the customer of choice during the Cold War is obvious during the first two periods, as is its precipitous falling off since 1990. Since most information sent to Eastern Bloc countries during the Cold War also went to the Soviets, it makes sense to combine percentages for the Soviets with the Eastern Bloc countries. Doing this credits the Soviets with being the ultimate recipient for 87% of information from individuals between 1947 and 1979, and the recipient for 75% of individuals during the 1980s. With the final collapse of the Soviet Union in 1991, the percentage of those sending information to Russia dropped to 15%, and to former Eastern Bloc countries, to none.

A few individuals in each period found recipients in Western Europe or in Africa, but percentages sending to these regions have remained small in all three periods. The trend for Asian or Southeast Asian countries to serve as recipients of American intelligence shows a steady increase: from 5% in the early period, it increased to 12% in the 1980s, and to 26% since 1990. The trend for Central and South American countries shows a marked increase since 1990; while only a small percentage appears in the two earlier periods, 22% of individuals chose to send information to that region in the recent past, largely to Cuba.

Al Qaeda first appears as a recipient in the mid-1980s from Ali Mohamed, who joined the U.S. Army in 1986 and stole classified documents, manuals, and training materials that he passed on to henchmen of Osama bin Laden in the United States, during the early phases of bin Laden's organizing a terrorist network (Waldman, Seib, Markov & Cooper, 2001). Four more Americans are known to have tried to spy for Al Qaeda or other related terrorist groups since 2000: Timothy Smith, who stole information intending to contact terrorists online; Ryan Anderson, a Washington State National Guardsman, who tried to contact local terrorist cells over the Internet; Hassan Abujihaad, who is accused of sending U.S. Navy ships' location reports and advice on attack options to an Al Qaeda affiliate in England; and Almaliki Nour, whose contacts in Iraq appear to have included Al Qaeda (Skolnik, 2000 [Smith]; Rivera, 2004 [Anderson]; "Ex-sailor charged," 2007 [Abujihaad]; Goldstein, 2007 [Nour]). These four recent cases with terrorist ties are discussed in more detail later in this report. The growth of a global yet stateless terrorist network has reframed the challenge of countering espionage. In two of these five instances, Ali Mohamed and Hassan Abujihaad, American citizens not only offered to support Al Qaeda by supplying information, but they also explicitly supported the terrorist agenda.

CONSEQUENCES OF ESPIONAGE

Table 9
Consequences of Espionage

Characteristics	1947-1979		1980-1989		1990-2007	
	n=66	*%*	*n=70*	*%*	*n=37*	*%*
Payment	*n=53*		*n=66*		*n=27*	
none	18	34	39	59	22	81
$50 – 999	3	6	7	11	0	0
$1,000 – 9,999	7	13	7	11	2	8
$10,000 – 99,999	15	28	8	12	1	4
$100,000 – 999.999	7	13	4	6	2	7
$1 million or more	3	6	1	1	0	0
Initial prison sentence, in years	*n=65*		*n=68*		*n=33*	
None	14	22	5	7	2	6
.1 – 4.9 yrs	8	12	15	22	12	37
5 – 9.9 yrs	10	15	12	18	9	27
10 – 19.9 yrs	12	19	14	21	2	6
20 – 29.9 yrs	4	6	10	15	2	6
30 – 39.9 yrs	4	6	6	9	1	3
40 yrs	2	3	1	1	1	3
life in prison	11	17	5	7	4	12
Outcomes other than being sentenced to prison at trial	*n=14*		*n=4*		*n=2*	
Discharged	1	7	0	0	2	100
Defected	5	36	2	50	0	0
Granted immunity	2	14	2	50	0	0
Suicide	4	29	0	0	0	0
Died	1	7	0	0	0	0
Exchanged	1	7	0	0	0	0

Table 9 compares three variables related to the consequences for American citizens of being caught betraying the country's trust through espionage. Data on payment received suggests that moneywise, espionage has been increasingly a losing proposition.[7] The proportion of those who received no payment at all increased from 34% before 1980 to almost 59% during the 1980s, and to 81% in the recent period. This reflects several trends. During the 1980s more would-be spies were intercepted—recall from the discussion above that interceptions increased from 9% to 40% in the 1980s—while since 1990 a larger proportion of spies have been acting

[7] The amount of money paid to spies is often hard to determine. Some succeed in hiding or lying about payment they received; for others, authorities prefer to acknowledge only vague figures. Figures available in open sources were coded, and no attempt was made to correct for the changing value of the dollar over time.

from divided loyalties and their commitment to another country or cause, and they have not received money for their work.

Table 9 shows that in most categories of payment, this trend toward declining payment over time can be seen: in all but one category, a smaller proportion of espionage offenders in the later two periods received as much as those in the early period, except for those making less than $1,000, where the number making less than $1,000 doubled in the 1980s. Collapsing the fourth and fifth categories of payment, while 40% of spies between 1947 and 1979 made between $10,000 and $999,000, and three individuals became millionaires, only 18% received that much in the 1980s, and only 11% did so since 1990. There are more missing data for this variable than there are for many others discussed here.

Americans have been making less money at espionage over time, while their chances of doing time in prison have increased. From 22% who served no time in prison in the period before 1980, only 7% in the 1980s, and 6% after 1990 escaped prison terms. There has been a shift in prison terms to the shorter sentences over the three time periods, with “one-month to five-year” and “5-year to 10-year” sentences nearly doubling since 1990 when compared to the earliest period. On the other hand, sentences of life in prison declined from 17% to 7% during the 1980s, but since 1990, life sentences have increased again to 12% of the total.

For those accused of espionage, outcomes other than a trial and prison are occasionally possible. The third variable in Table 9 reports the numbers of individuals who experienced other outcomes. One sizeable category is defections during the Cold War, and another is death before conviction, usually by suicide. Five individuals have been discharged or granted immunity, often for issues with the prosecution’s case or for lack of evidence, and one spy was exchanged.

MOTIVATIONS

Table 10
Motivations of Individuals for Espionage (92 persons held a sole motive; 81 persons held multiple motives)[8]

Characteristics	1947-1979		1980-1989		1990-2007	
	n	%	*n*	%	*n*	%
Money						
Sole motive	20	47	26	74	1	7
Primary among multiple motives	10	43	21	60	9	39
Divided loyalties						
Sole motive	7	16	4	11	8	57
Primary among multiple motives	6	27	5	14	9	39
Disgruntlement						
Sole motive	7	16	2	6	3	22
Primary among multiple motives	5	22	3	9	3	13
Ingratiation						
Sole motive	4	9	1	3	2	14
Primary among multiple motives	1	4	6	17	2	9
Coercion						
Sole motive	4	9	0	0	0	0
Primary among multiple motives	1	4	0	0	0	0
Thrills						
Sole motive	1	3	1	3	0	0
Primary among multiple motives	0	0	0	0	0	0
Recognition or ego						
Sole motive	0	0	1	3	0	0
Primary among multiple motives	0	0	0	0	0	0

Table 10 compares the motivations of individuals to commit espionage over the three time periods considered here. While in an earlier section changes were considered in the incidence of divided loyalties as a motive, here the comparison is made across all the typical motives over time.

Assigning the motivation for committing espionage is often most accurate when motivation is inferred from evidence available while the crime was being committed,

[8] Group 1 (1947-1979): sole motive = 43 persons; multiple motives = 23 persons; total = 66. Group 2 (1980-1989): sole motive = 35 persons; multiple motives = 35 persons; total = 70. Group 3 (1990-2007) sole motive = 14 persons; multiple motives = 23 persons; total = 37. Percentages in this table reflect the number of persons in each time period who had either sole motives or multiple motives. For example, in the group that began espionage between 1947 and 1979, 4 persons had a sole motive of ingratiation, which is 9% of the 43 persons who began in that period who had sole motives.

rather than from the self-justifications of the offender after the fact. Like most criminals, once caught, spies see their own past intentions and the pressures that may have affected their behavior in a changed light. For some individuals, their retrospective justifications are the only evidence available about their motives. Sole motives were coded for persons who appeared to have only the one reason for spying, and if an individual held multiple motives, an attempt was made to rank these motives in their order of importance to the person. Inevitably this was a subjective judgment based on the evidence available from open sources. For each motive reported in Table 10, the number of those with a sole motive is shown first, then the number of persons with multiple motives for whom this was the primary one.

Americans who spied during the first two time periods considered here most often did so for the money. For 47% of offenders in the early period, money was their sole motive, and that proportion jumped up to 74% who spied solely for money during the 1980s. The 1980s were years of considerable public soul-searching over what the influx of mercenary spies said about the state of American values (Lentz, 1985; Molotsky, 1985; Brock, 1987). Possibly the state of American values has improved in the recent past because since 1990, the number of citizens spying solely for money has dropped to one. Among those with multiple motives in which money was primary among them, a comparable pattern holds over the three time periods, with 43% spying primarily for money in the early period, increasing to 60% during the 1980s, and then decreasing to 39% since 1990. One of those cases since 1990 in which the individual was motivated by a combination of desire for money laced by disgruntlement was Brian Regan, a career Air Force signals intelligence analyst who prepared for and attempted to commit espionage starting in 1999.

Regan was working as an analyst at the National Reconnaissance Office (NRO) when he began browsing daily on Intelink, a multiagency classified intelligence network, searching for documents and photos that he could offer to Iraq, Libya, or China. He downloaded or printed off thousands of pages of documents. At the time, he was slipping deeply into debt, running up over $50,000 on his credit cards (United States District Court for the Eastern District of Virginia, Superseding indictment, 2002; Bamford, 2001). At the end of August 2000, he retired from the Air Force, and a few months later he took a job with TRW, Inc., in order to continue to work at NRO as a contractor. On August 1, 2001, Regan received his renewed TS-SCI security clearance and regained his access to Intelink; that very morning he resumed searching for classified documents for his espionage project (Bamford, 2001).

Sometime before he retired from the Air Force, Regan had drafted long, detailed letters to Saddam Hussein and Muammar Gaddafi, offering to provide them with highly classified satellite intelligence about Iraq or Libya, or their enemies, in exchange for $13 million. He filled page after incriminating page with detailed instructions on how to communicate with him so he could remain anonymous, and with assurances about how valuable the information he could provide would be, insisting it would be well worth the money. In his letters, he explained that he was angry about the paltry pension he would receive after 20 years of personal sacrifice serving in the Air Force, while movie stars and athletes made millions (United States District Court for the Eastern District of Virginia, Superseding indictment, 2002). Using computers at his local public library, he searched on the Internet for addresses and phone numbers of foreign embassies in Europe, and he collected spy gear—tape, gloves, a Global Positioning System receiver—for his planned trip to make contact with embassy personnel in Bern, Switzerland, Vienna, Austria, or Paris, France (United States District Court for the Eastern District of Virginia, Superseding indictment, 2002; Markon, 2003a).

Regan was arrested at Dulles International Airport, Dulles, VA, on August 23, 2001 as he was boarding a flight to Switzerland. He was charged with multiple counts of attempted espionage (Schmitt, 2003). After the attacks of 9/11, the government sought the death penalty in his case, but the jury resisted considering the death penalty for attempted espionage, and found Regan guilty of two counts of attempted espionage (with Iraq and China) and one count of gathering national defense information with intent to harm the United States. In May 2003, Regan accepted a plea of guilty and a life sentence, and he agreed to cooperate with further investigation (Markon, 2003b, 2003c). During the summer of 2003, the FBI undertook an elaborate search for the 20,000 pages of documents, CDs, and videotapes that Regan had packaged and buried in 19 locations in state parks in Virginia and Maryland. He had encoded the coordinates of the burial sites so thoroughly that it took cryptographers a month to decrypt them. Even Regan had forgotten several of the locations, and he thrashed around the forests in handcuffs and leg irons with FBI agents toting shovels until they had retrieved all the documents he had hidden (Markon, 2003d).

As discussed in earlier sections, spying for divided loyalties shows the most significant increase over time of all the motives for espionage. Since 1990, the proportion of those motivated to spy solely by divided loyalties has increased from less than 20% in the two earlier periods to 57%, and the pattern for those with multiple motives in which divided loyalties was primary shows a similar increase: from 25% in the early period, the proportion of those whose primary motive among multiple motives was divided loyalties dropped to 14% in the 1980s, and then rose to 39% in the recent period. This suggests that espionage by Americans probably reflects the trend of globalization and its concomitant changes in communications and automated information transfer and storage that have taken place over the past two decades. Data for the group of individuals who began espionage since 2000, discussed below, suggests that this trend may have been accelerating since 2000.

An example of a serious espionage case motivated by divided loyalties is that of Ana Belen Montes, a DIA analyst and an agent for Cuban intelligence for at least 16 years. Montes, whose family moved to the United States from Puerto Rico, was recruited by Cuban intelligence while in graduate school in 1984. At their suggestion, she sought a job with better access to the information her handlers required, that of a Cuba specialist at DIA (Glazov, 2007). Montes appeared to be a "model employee," dedicated and industrious, yet her coworkers noticed her scorn for American policy toward Cuba and other Latin American socialist regimes. Qualms about her attitudes were repeatedly raised, yet decided in her favor by security officials who looked into concerns about her (Glazov, 2007).

The FBI investigated Montes from May into September 2001, watching as she made phone calls from pay phones to her handlers in order to pass codes. They also found her shortwave radio in her closet, and her decoded exchanges with Cuban intelligence still on her computer's hard drive (United States Magistrate Judge, Affidavit, 2001). The FBI arrested her sooner than investigators would have liked, on September 21, 2001, as the plans for the incursion into Afghanistan came together and the government did not want her to pass those plans to Cuba. She was convicted of espionage for passing to Cuban intelligence information on all sources and methods the United States was using to collect intelligence against Cuba, American contingency plans for response to Cuban activities, at least one special access program, and insight into government attitudes and policy preferences at the highest levels of government (Glazov, 2007). She accepted a plea bargain to plead guilty and received 25 years in prison and 5 years' probation in exchange for her cooperation in the investigation. Montes remained defiant and unrepentant of her espionage at her sentencing hearing, saying "I believe our government's policy towards Cuba is cruel and unfair. I felt morally obligated to help the island defend itself from our efforts to impose our values and political system on it" (Golden, 2002).

The third most common motive for Americans to commit espionage is disgruntlement, usually caused by the person's relationships or treatment in the workplace, and the associated desire to take revenge. The proportion of Americans spying solely from disgruntlement was 16% in the early period, dropping to 6% in the 1980s, and rising again to 22% in the recent period. A similar pattern, with a drop in the percentage in the 1980s, tracks for those with multiple motives whose primary one is disgruntlement. Earl Pitts, the second FBI agent to be convicted of espionage,[9] is an example of someone motivated by disgruntlement, although in his case his anger at the FBI was inextricably entwined with his need for money (United States District Court for the Eastern District of Virginia, Criminal complaint, 1996).

Pitts joined the FBI in 1983 after graduating from law school, and married a fellow agent 2 years later. In 1985 he was already simmering with discontent at the bureaucratic ways of the FBI, and chafing at his boring assignments as a junior agent. In late 1987, Pitts was transferred to the New York FBI office, and within 6 months he decided to begin spying for the Komitet Gosudarstvennoy Bezopasnosti (KGB)—out of anger and humiliation at his paltry salary that meant he had a two-hour commute into the city each way, was forced to borrow money from his

[9] Richard Miller was the first.

parents, and ran up debts on his credit cards. The New York City FBI office was notorious as a hard duty station because of the Bureau's refusal to recognize the cost of living in its agents' salaries (Brenner, 1997). Robert Hanssen also worked in the New York City FBI office, and he suffered from a similar rage about his salary that fueled his determination to commit espionage (Ciccarello & Thompson, 2003).

Since Pitts was working foreign counterintelligence against the Soviets at the United Nations, it was relatively simple for him to drop a note to one of his surveillance targets who arranged a meeting with the KGB, at which he offered to spy for them. For 5 years he passed intelligence about FBI surveillance operations to the Soviets, including the FBI's list of all known Soviet intelligence agents operating in the United States (Masters, 1997a). Pitts' contact with the Soviets went quiet in 1992 after the fall of the Soviet Union, but he came to the attention of the FBI 3 years later when his initial Soviet contact became an FBI source and fingered Pitts as a spy (Suro & Thomas, 1996). After an elaborate 16-month FBI sting, Pitts was arrested in December 1996. He pled guilty in a plea bargain to conspiracy to commit espionage and attempted espionage, and was sentenced in July 1997 to 27 years in prison (Hall, 1997; Masters, 1997b). Looking back at his decision to spy, what was salient to Pitts was not the $200,000 he took from the Soviets; it was his disgruntlement with the way the FBI had treated him. He told a reporter that in New York "I was angry all the time….I had an overwhelming need to lash out [at the FBI] and strike out…I wanted to hurt them" (Brenner, 1997).

Smaller numbers of individuals demonstrate the remaining four typical motives for espionage: ingratiation, coercion, thrills, and recognition or ego (this could also be called ambition). Ingratiation with a spouse or other family member, a friend, or a handler was a motive for several persons in each period. A recent example of a case motivated primarily by ingratiation is that of Donald Keyser, who was serving as the Principal Deputy Assistant Secretary of State for East Asian and Pacific Affairs in September 2004 when he was arrested by the FBI for concealing a secret visit to Taipai, Taiwan a year earlier, not listing the trip on a U.S. Customs report form, and lying about the trip during his personnel security reinvestigation in May (Brinkley, Bradsher & Oppel, 2004).

On the day of his arrest, the FBI searched Keyser's residence and found 3,659 hard copy and electronic documents classified Top Secret, Secret, and Confidential that dated from 1980 to 2004. Keyser was a prominent foreign policy analyst, fluent in Mandarin Chinese and an expert on China, Japan, and Taiwan, who had repeatedly served in senior posts in American embassies in the Far East. He had served as advisor to Secretary of State Colin Powell, and had been named Ambassador by President Clinton while he served as the Special Negotiator in Nagorno-Karabakh, Azerbaijan, in 1999. Keyser pled guilty in December 2005 to maintaining an unacknowledged personal friendship with Isabelle Cheng (a 33-year-old Taiwanese intelligence officer living in Washington, DC), traveling with her to Taiwan (which was forbidden by the State Department for someone in his position) while he was ostensibly on an official trip to China and Japan, lying about it, and removing and improperly storing at his home several thousand classified documents. He claimed in the plea bargain that he had passed no classified information to Cheng or her boss, Michael Huang, when he met with them, nor had he been blackmailed by them, though he admitted he could have been (LeFebvre, 2007; Markon, 2006).

As part of his plea bargain, Keyser promised to completely and truthfully cooperate with debriefings and polygraph tests. In June 2006, the prosecutors filed a rare retraction of their plea bargain, stating that Keyser had remained evasive and uncooperative. The government's revised charges vividly documented the sexual infatuation that Keyser had felt for Cheng for several years and their illicit relationship by quoting emails and telephone taps and describing sightings of the couple in compromising situations. The superseding indictment provided documentary evidence of Keyser's eagerness to "help" Cheng and her government by passing along insider information he thoughtfully summarized for her, including official briefings and policy documents about Taiwan and China. He also suggested to Cheng that a colleague of his was ripe for Taiwan's recruitment as a spy. The FBI described Keyser's practice of espionage tradecraft in clandestine meetings and dealings with Cheng and Huang, changing taxis and walking through restaurants to shake anyone tailing him.

Keyser claimed he helped Cheng because he felt U.S. policy was not being accurately conveyed toward Taiwan, but he told her not to admit she had gotten the information from him. "All you need to do is ask," he emailed her, "and I will do my best to reply quickly, fully, and helpfully. *No matter the subject,* whether official or personal. *Anything.*" (United States District Court for Eastern District of Virginia, U.S. v. Donald Willis Keyser, 2006). Keyser was sentenced in January 2007 to 1 year and a day in prison, 2 years of supervised release, and a fine of $25,000 (LeFebvre, 2007; Markon, 2004; Markon, 2006; Gerstein, 2006). Keyser's earlier repeated security violations over several decades, and his casual crossing of the line from diplomatic interaction with foreign officials to an obsessive, furtive affair advanced by his passing State Department intelligence, suggest that he assumed he was above mundane details like the security requirements of his position.

Coercion was used to recruit spies most often in the early period before 1980, when foreign intelligence services engaged in occasional blackmail using relatives overseas, or entrapped Americans in sexual blackmail scams. No instances of coercion as a sole or primary motive appear after 1979. A few individuals spied for the thrill of getting away with espionage, or from their need to gain recognition and indulge their egos or to get ahead in their jobs. More of these cases are discussed below.

VULNERABILITIES THAT MAY INCREASE RISK OF INSIDER THREAT

Eighty percent of the 173 individuals in the PERSEREC Espionage Database held security clearances and access to classified information while they were committing espionage; 20% did not have clearances when they began spying, but as discussed above, some of those used the access of family or friends, and others relied on their memories from earlier access. The 119 persons who are known to have held security clearances and access to classified information when they began espionage-related activities, plus the seven individuals who had held security clearances earlier before they began espionage, all signed nondisclosure agreements in which they agreed not to disclose any information made known to them by their access. The 126 individuals who betrayed the trust placed in them and violated their signed contracts by committing espionage are the exemplars of insider threat.[10]

Considerable expense and effort are focused on screening out unreliable, untrustworthy, or disloyal applicants for a security clearance. Eligibility for access to classified information is defined by criteria in Department of Defense Regulation 5200.2R (Personnel Security Program Regulation, January 1987 as amended), in Executive Order 12968, approved in 1995, implemented in 1997 and revised in December 2005 titled *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, which is also endorsed by the Director of Central Intelligence Directive No. 6/4 ("Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmental Information," July 1998). The *Adjudicative Guidelines* specify guidelines that personnel security adjudicators must consider before granting a security clearance to any civilian or military employee or contractor across any agency of the federal government. The guidelines define issues of concern that raise questions about a person's eligibility for access classified information. The guidelines cover behaviors in the following topics:

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

[10] For 10 individuals, whether they held a security clearance and at what level are unknown.

Several of these criteria, including personal conduct, outside activities, and use of information technology, have been added since 1990; others have been in effect for decades. They have defined the information that is collected by investigators during a background investigation, and the information that is evaluated by adjudicators in deciding whether to grant a person a security clearance. The nexus between these 13 personnel security criteria and the potential to betray the country's trust by committing espionage is not exact, for not every spy fails to live up to one or more of these criteria, but the nexus has been compelling enough over time for these criteria to remain in effect and useful. It is important to anchor in time judgment about the effectiveness of this nexus. While an applicant is still being considered for a clearance, information based on these criteria is evaluated to determine whether the person is likely to be less than loyal, trustworthy, and reliable in the future. People change with time while they have access, however, which is why security programs incorporate continuing evaluation measures, and why they update their information on these criteria in order to capture changes of security concern. The personnel security is not designed to identify spies or prevent espionage (and indeed it has not in several instances) but rather to provide employees that meet the 13 personnel security criteria.

The 126 individuals under consideration here, who illustrate a major dimension of the insider threat, are a tiny subset of the millions of people granted access to classified information over six decades. They are the known instances of betrayals of trust—the "after access" group that proved disloyal or untrustworthy or unreliable although they passed an initial screening, and for some, multiple periodic screenings. Many of them did indulge in behaviors that fall under one of the 13 guidelines and also committed espionage—but as background investigations suggest, millions of other persons with access to classified information also indulge in some of these behaviors and they do not commit espionage. The nexus between the guidelines and security failures is useful but inexact; it allows the filtering out at the front end of many persons who seem likely to present or develop security problems, but it does not usefully "read backwards" in time to predict who will become a spy. The nexus does focus on an applicant's potential for good judgment and reliability, and thus identifies those who may present vulnerabilities for becoming security risks as employees.

All available instances of potential violations of personnel security criteria were coded for the 173 individuals into the PERSEREC Espionage Database, but much information is missing on these behaviors. No claim can be made that because a security-relevant behavior is not mentioned in these sources that it was not present. Serious espionage cases earn intense media scrutiny and provide many personal details about the suspect; the media treatment of obscure cases provides very few details about the person's life. Data in this area are inevitably incomplete and probably underreport the incidence of problem or security-relevant behaviors. In the examples of espionage-related offenses discussed in this report, many issues appear that are identified in the *Adjudicative Guidelines* as security-relevant, including instances of security violations such as taking classified information home, compromises of allegiance, mental illness and instability, sexual affairs with foreign intelligence agents, mounting debts, bankruptcy, greed, misuse of computer systems to collect intelligence for espionage, and foreign influence and preference.

Table 11
Selected Issues of Security Concern among Espionage Offenders[11]

Characteristics	**1947-1979**		**1980-1989**		**1990-2007**	
	n = 66	*%*	*n = 70*	*%*	*n = 37*	*%*
Allegiance to the United States						
To a separate country or cause	14	21	15	21	17	46
To Communism specifically	9	14	3	4	5	14
Drug Involvement	10	15	29	41	1	3
Alcohol Consumption	20	30	17	24	3	8
Personal Conduct: Gambling	12	18	1	1	0	0
Foreign Influence or Foreign Preference (may have more than one type as coded here)						
Foreign Attachments (relatives or close friends)	33	50	15	21	15	41
Foreign connections (business or professional)	10	15	12	17	19	51
Foreign cultural ties	4	6	7	10	18	49
Financial Considerations						
Financially irresponsible lifestyle	8	12	9	13	4	11
Bankruptcy	2	3	2	3	2	5
Debts were one cause of espionage	24	36	28	40	11	30
Greed were one cause of espionage	4	6	8	11	4	11

The data in Table 11 demonstrate that many individuals who committed espionage-related offenses are also known to have violated the criteria for security-relevant behaviors and conditions outlined in the *Adjudicative Guidelines*. Of the variables that relate to the 13 adjudicative criteria, these have the fewest missing data in the PERSEREC Espionage Database.

Allegiance (already discussed in relation to foreign preference above) is a complex phenomenon that is particularly difficult to behaviorally document (Krause, 2002). Evidence was coded as allegiance to a separate country or cause when sources described activities or statements by an individual supportive of that entity and

[11] Percentages of the total persons in each time period are shown for each issue, but because an individual may have more than one issue, percentages do not sum to 100.

detrimental to the United States. This entailed exercising judgment, and observers could differ on them. For both of the early periods, just over 20% of espionage offenders showed allegiance to a separate country or cause. This proportion doubled in the recent period to 46%, reinforcing the finding of globalization's impact and the influence of foreign ties since 1990. Among those with competing commitments was the small proportion devoted to Communism: 14% of those before 1980, only 4% during the 1980s, and again 14% of the total since 1990. Allegiance to the cause of terrorism appears in several recent cases.

The security concern about behaviors such as misuse of drugs or use of illegal drugs, alcohol dependence or abuse, or gambling, is that these could undermine self-control and lead to recklessness, unreliability, or the need to raise cash illegally to support addictions. Some espionage offenders did engage in these behaviors of security concern. From 15% of spies between 1947 and 1970 who are known to have misused drugs or used illegal drugs, the proportion jumped to 41% during the 1980s as the spy population flooded with younger, low-ranking military men. In contrast, only one of the 37 individuals who began spying since 1990 is known from open sources to have misused drugs or used illegal drugs, which may reflect the spread of drug tests for applicants for access and as a continuing evaluation measure.

Immoderate use of alcohol that was severe enough to be reported in case descriptions declined over time among the three groups in this study. From a high of 30% between 1947 and 1979, the proportion of those known to be suffering from alcohol dependence or abuse declined to 24% during the 1980s, and declined to only 8% since 1990. Gambling addiction also declined among espionage offenders, from 18% before 1980 to one individual during the 1980s, and then to no one in the later period.

Variables demonstrating potential foreign influence or foreign preference have been discussed in earlier sections of this report, but they are included in Table 11 because three of the 13 *Adjudicative Guidelines* focus directly on these issues (Foreign Influence, Foreign Preference, and Outside Activities), directing the attention of adjudicators to these concerns. The pattern in the data shows that the percentage of espionage offenders who had foreign relatives has declined starting in the 1980s, while the percentage of those with foreign connections and foreign cultural ties remained roughly comparable across the two earlier periods at less than 20%. Since 1990, the percentage of those with foreign relatives increased to 41%, while about half of the 37 individuals had either foreign connections or foreign cultural ties, or both.

Four variables on the issue of financial concerns were coded in the PERSEREC Espionage Database. The *Adjudicative Guidelines* embody the concern that a person with access to classified or sensitive information who is irresponsible about personal finances may prove unreliable in security responsibilities as well, or that a person with mounting debts, or a greedy disposition, may be tempted to sell valuable information to meet those needs. Roughly 12% of individuals in each of the three time periods being considered here lived a financially irresponsible lifestyle. Only two individuals in each group declared bankruptcy. Among financial problems, debt was the most common theme in each group, since 36%, 40%, and 30% of individuals in each time period resorted to espionage in part because of their debts. Greed without accompanying debt, on the other hand, figured in the motives for espionage for 6% of individuals before 1980, and for 11% both during the 1980s and since 1990.

LIFE EVENTS AS TRIGGERS FOR ESPIONAGE

Studies of espionage based on personal interviews with offenders suggest a pattern in which personal disruptions or crises precede, or "trigger," an individual's decision to commit espionage (Stein, 1994). Researchers have speculated that if help or timely intervention had been offered, the crime might have been averted (Wood & Fischer, 2002). Instances of such triggers were coded in the PERSEREC Espionage Database if they occurred coincident to or shortly before an espionage attempt, roughly during the previous 6 to 8 months. Crises could be positive as well as negative, and were defined as the death or terminal illness of a close friend or member of the family, separation or divorce from a spouse, lengthy physical separation from a spouse, marital discord, a recent engagement or marriage, a new love relationship, an extramarital affair, physical relocation, threatened suicide, or reports by others of sudden radically altered behavior (Ross & Mirowsky, 1979). Most of the data on these life crisis issues for espionage offenders are missing in open sources. Only the most damaging spies merit in-depth journalistic treatment; in most cases only the espionage itself and the consequences are reported. Nevertheless, if these issues were mentioned in the sources available, these data were collected.

Fifty-seven of the 173 individuals in the PERSEREC Espionage Database, or 33%, were found to have experienced one or more of these events in their lives during the months before attempting espionage. Given the proportion of missing data, no comparison across time periods is possible for this issue. Harold Nicholson, the highest-ranking CIA agent accused of espionage, provides an example of someone whose personal crisis seems to have triggered his decision to commit espionage.

Nicholson had risen during a 16-year career with the CIA to station chief and then branch chief levels; his ex-wife and friends described him as devoted to his career, putting the demands of his job first before family, yet especially loving toward his children (Grier, 1997). In 1992, when he moved from his CIA assignment in Bucharest, Romania, to one in Kuala Lumpur, Malaysia, his wife returned to Oregon and filed for divorce. They fought a contentious divorce and child custody battle in court, which resulted in Nicholson gaining custody of their three children in 1994. He became a single father who owed his ex-wife a lump sum payment and monthly alimony payments that took one quarter of his salary (Lacayo, 1996). His

CIA supervisors were aware of his divorce, and they were concerned about the possibility that his personal upheaval could make him vulnerable to recruitment by foreign intelligence (Grier, 1997). Despite the alertness of his supervisors, just months after his divorce was settled, Nicholson arranged a meeting with a Russian contact, explaining to his boss that he might be able to recruit the man (this was also Aldrich Ames' method for initially contacting the Russians). Apparently at that meeting he offered his services as a spy, since the following day he wired a large, unexplained deposit into his savings account (United States Magistrate Judge, Affidavit, 1996). Nicholson then spied for the next 2 years for the Sluzhba Vneshney Razvedki (Foreign Intelligence Service, or SVR), successor to the KGB; almost half of that time he was being watched by the FBI, after he registered deceptive in a series of polygraph tests in late 1995 (United States Magistrate Judge, Affidavit, 1996). He took four trips to East Asia or Europe to meet his handlers, exchange intelligence, and collecting payments.

Nicholson was teaching new CIA recruits in Virginia during the period of his espionage, and he passed along to the Russians the identities of his students who would soon be taking up clandestine positions. He requisitioned a folding camera at his CIA office. When it was delivered to him, he locked his office door and began using it to photograph the piles of classified documents that he had printed out that would be of interest to the Russians (United States Magistrate Judge, Affidavit, 1996). He was arrested on November 16, 1996, at Dulles airport as he was boarding a flight to Switzerland for another meeting with his handlers. He carried with him photographs of 74 classified reports in his luggage (Smith & Hall, 1996). Nicholson pled guilty to conspiracy to commit espionage in a plea bargain, and agreed to cooperate in debriefings. He admitted he had received $300,000 for his espionage, far more than the FBI had realized (Risen, 1997). In June 1997, he was sentenced to 23½ years in prison. A reporter described the explanation of his motives Nicholson gave at his sentencing hearing: "He {said he] sold out the United States for money to give his children a better life after the collapse of his tumultuous marriage" (Risen, 1997). His attorney echoed his client, blaming his actions on the divorce and the need for funds it had caused: "What happened in this case was the result of his decision to deal with a family situation," his attorney offered (Masters, 1997b). On the other hand, the prosecutor noted, "an awful lot of people get divorced and don't spy for the Russians," and instead put Nicholson's betrayal down to greed (Risen, 1997).

It is probable that more of these 173 people faced one or more of these personal crises and that fact is simply unknown to us, given the likelihood of such common crises in anyone's life. The millions of persons with access to classified or sensitive information who did not commit espionage also faced crises and upheavals in their lives. The large proportion of missing data on life crises prevents a claim that persons with access to classified or sensitive information who experience one of these life events are more likely to commit espionage, but the number of instances of espionage in which life seemed to them to be falling apart to the person before he or she acted, or where individuals said they were under unusual pressure and resorted to espionage to relieve it, cannot be dismissed. Pressure does tip some people away from their apparent stability into doing impulsive or desperate things, and espionage is occasionally one of those desperate things. At a minimum, this suggests that managers of employees with access to classified or sensitive information should take seriously their responsibility to be aware of unusual stresses in their employees' lives, and to sensitively monitor and try to assist employees in crisis.

PREVALENCE OF SPIES

Figure 2 depicts how many American citizens in a given year, known from open sources, were actively engaged in espionage.

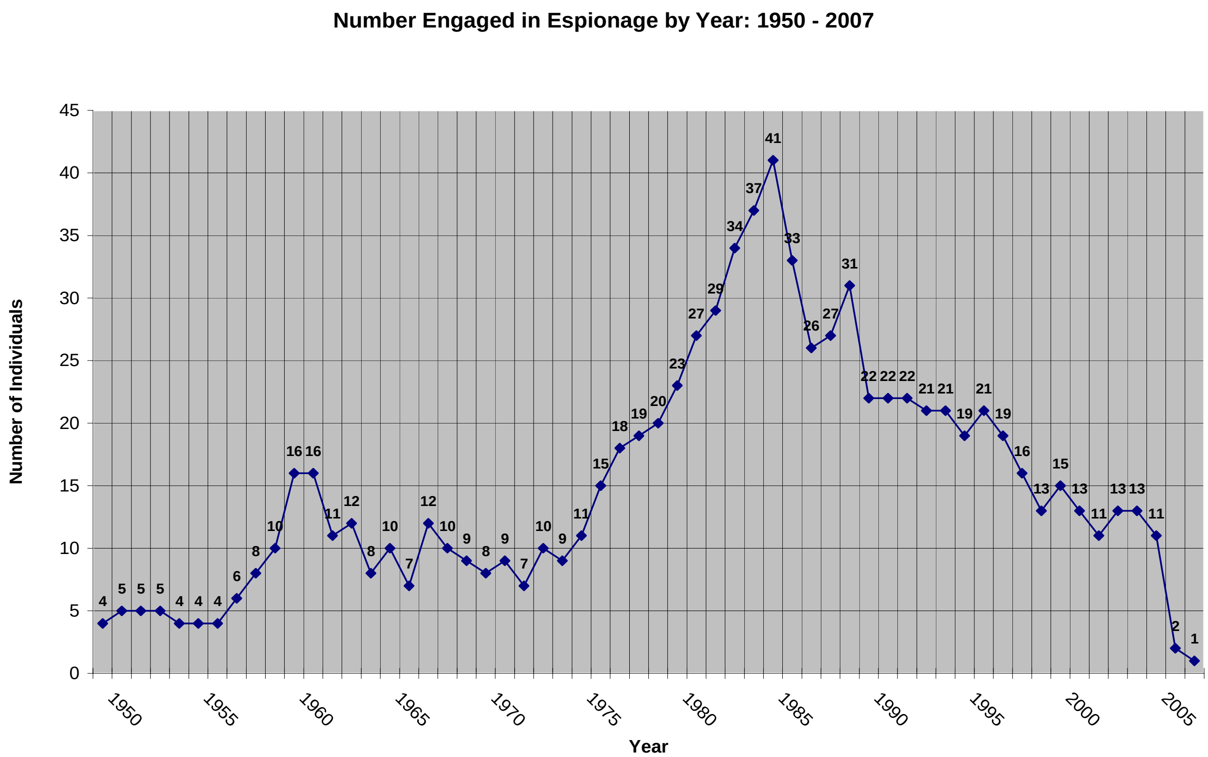

Figure 2 Prevalence of Spies

The chart in Figure 2 is derived by comparing the year in which an individual began espionage activities with the year in which he or she ended those activities. If a person was intercepted before passing information, the person is counted as active once in the year they attempted espionage. Some spies started and stopped several times over their careers, and they are only counted in a given year if they were active in that year. Robert Hanssen, for example, spied during three different time periods: between 1980 and 1981, between 1985 and 1991, and between 1999 and 2001 (Ciccarello & Thompson, 2003). Other spies discontinued their espionage only to be arrested years later, and only their years of actual spying are counted in this chart. Robert Lipka may be the best example of a spy who was caught years after he had stopped his activities.

Lipka stole highly classified reports, communications intercept summaries, and reports of U.S. troop movements from the NSA, where he worked as a communications clerk between 1965 and 1967. He was a 19-year–old Army enlisted man when he began spying for the Soviets, just as the Vietnam War was escalating. Lipka made $27,000 for the documents he wrapped and left in dead drops in the neighborhoods around NSA. Complaining that the KGB did not pay well enough for the risks he was running, he left his job at the NSA that gave him the access he was selling in 1967, and he cut off all contact with the Soviets in 1974 (Smith & Thomas, 1996).

For the next 20 years, Lipka lived quietly in Pennsylvania. He divorced his first wife and remarried, had three children, ran a coin shop for while, and taught high school. In 1993, an FBI agent posing as a Russian intelligence officer knocked on his door and offered to reestablish contact and discuss his past contributions. Lipka said enough in their meetings, along with other evidence turned up in the investigation, to cause his arrest in February 1996. At the time, the FBI claimed that Lipka's ex-wife had come to them and turned him in (he had apparently told her about his spying at the time, and while she had never come forward, she was given immunity from prosecution in the mid-1990s) (Smith & Thomas, 1996). Later it was revealed that Lipka had been implicated by name in the "Mitrokhin files," intelligence files that were smuggled out of the Soviet Union by the former KGB officer Vasili Mitrokhin in 1992 when he defected to London. Those files were shared with the FBI (MacIntyre, 1999). In 1997, Lipka pled guilty in a plea bargain to conspiracy to commit espionage 20 years earlier, agreed to cooperate with debriefings, and was sentenced to 18 years in prison and a $20,000 fine. He admitted betraying his country out of what he said was "pure green greed," and at his sentencing he acknowledged that his whole life had been lived looking over his shoulder, waiting for someone to find him (Wilson, 1997; Duffy, 1997).

The chart in Figure 2 above demonstrates that an increasing number of spies are known to have been active between 1975 and 1990, with the peak of 41 active spies in 1985. This period reflects federal policies that encouraged public prosecution of espionage in order to deter others from the crime, and thus more espionage prosecutions clustered in this period (Herbig & Wiskoff, 2002). The accelerating falling off since 1990 in the numbers of known spies actively committing espionage may reflect one or more possible developments. It may reflect a change in prosecution policies toward a more conservative approach in which fewer espionage arrests are made public, or a shift in resources and attention from counterespionage to counterterrorism. It may demonstrate that counterespionage measures undertaken since 2000 have been increasingly effective; or it may be a warning that there are still more Americans spying that have not been identified, and so do not appear in the chart.

THE MOST RECENT ESPIONAGE BY AMERICANS

Public media have reported on 11 American citizens who began spying, or tried to begin spying, since the turn of the 21st century. In their motives and in their choice of potential customers, they reflect the most current global political and military context. In some obvious ways they differ from those who chose to spy in the two earlier periods. The 11 most recent cases will be discussed here in detail because their activities are not well known and they merit close study. This is a subset of the 37 individuals considered in this study who began espionage since 1990—these 11 persons began their espionage in 2000 or later. Their cases are less familiar and have been studied less than many of the earlier cases in their cohort. Their cases are scrutinized for the new departures they illustrate, as well for the trends or patterns they may suggest in future counterintelligence challenges.

The 11 most recent American spies fall loosely into two groups: the four who stole or collected national defense information to sell it for money, revenge, or self-advancement, and the seven others whose motives included divided loyalties to other countries or causes. Those in the first group resemble many earlier would-be or actual spies, many of whom proved to be ineffectual at espionage and who were soon caught. Those in the second group—who were also for the most part caught before they passed information—point up some issues that make espionage distinctive in the recent period of globalization and global terrorism.

Case Descriptions

Timothy Smith. In the early morning hours of April 1, 2000, Smith stole computer disks from the first officer's desk on the ammunition supply ship *U.S.S. Kilauea.* He was caught in the act, fought briefly against capture, and was subdued. Smith worked as a civilian seaman on the ship, which was docked in Bremerton, WA, during the episode. At first, Smith was charged with espionage, theft of government property, and resisting arrest. A search found five more documents marked Confidential in his storage locker. He told investigators he intended to steal "valuable classified materials" in order to "take revenge on shipmates who had mistreated him," and he would "possibly sell them on the Internet to terrorists." In December 2000, in a plea bargain, Smith pled guilty to theft of government property and was sentenced to time served, 260 days, plus 3 years' probation, and treatment for alcoholism and mental illness. The case illustrates a typical ill-planned, impulsive theft of the most valuable commodity at hand, national defense information, to sell and, at the same time, to get a vaguely defined revenge on his shipmates. The new element in the case was Smith's apparently casual assumption that he could make contact with "terrorists" on the Internet who he assumed would welcome his offer and pay him for his stolen documents (Skolnik, 2000; Horn, 2000).

Kenneth W. Ford, Jr. Ford worked for the National Security Agency (NSA) as a computer specialist from mid-2001 to the end of 2003. According to a press account of his trial, the prosecutor explained that "On his last day of work there, Ford packed up the cardboard boxes with national security documents, left through an unguarded exit and loaded them into his pickup" (Castaneda, 2005). When the FBI searched his home in mid-January 2004 (acting on a tip from Ford's girlfriend), they found several boxes of Top Secret documents piled in the kitchen, and more classified documents in a bedroom safe and under the bed. Ford claimed he had taken the documents home to refer to them in his next job, which was to be with Northrop Grumman on a classified contract. Prosecutors responded that Ford did not have enough information about the new job to know what would be relevant to it, but they did not claim they had evidence that Ford intended or tried to sell the information. Having lost the Northrop Grumman job, a judge warned Ford at a hearing in August 2004 that if he applied for other work with classified materials while on bail, Ford would have to disclose on the Standard Form 86 (SF-86) that criminal charges were pending against him. Ford proceeded to apply for employment at Lockheed Martin, where he filled out an SF-86 claiming that there were no charges pending against him, that he had been falsely arrested by the FBI, and that he had no prior criminal record. His lies on that SF-86 earned Ford a second criminal charge: in addition to unlawful possession of classified information relating to the national defense, he was also charged with making false statements to a government agency.

Ford was convicted of these offenses on December 15, 2005, and sentenced on March 30, 2006, to 6 years in prison, to be followed by 3 years' probation (United States Attorney's Office, 2006). In an otherwise mundane case of stolen classified documents, the ease with which he walked out of NSA with considerable quantities of classified documents is startling. This despite notorious recent examples of trusted employees taking classified materials out the exits of their agencies, including Jonathan Pollard in the mid-1980s, and Brian Regan in the mid-1990s. Ford underlined again in 2004 the need for vigilance and systematic physical security at exits, and better information security to track and account for classified documents.

Ariel Weinmann. Weinmann joined the Navy at age 22, an idealist and outspoken patriot, hoping for a promising naval career that would build on his conventional middle-class start in life. However, a series of disappointments in his first year soured him on military life, and diverted him into ill-considered, increasingly desperate crimes. Once in the Navy, he found there were no openings in the linguist rating he wanted. He settled for a Fire Control Technician rating on a nuclear submarine, but he hated the petty corruption he found in the intensely competitive struggle for advancement, and the indifference he felt the officers showed to the junior men. Next, his fiancée broke up with him, and at her parents' insistence, moved to Switzerland to go to school. Weinmann decided to desert from the Navy that he was coming to hate, and to follow his fiancée to Europe hoping she would take him back. He carefully planned his escape and used his computer skills to leave with saleable assets. Stealing a laptop computer, he downloaded files from classified databases onto CDs he thought would be saleable, and he stored other classified files on external disk drives and memory cards. He took his life savings of $7,000 and deserted. Weinmann left in July 2005 and flew to Vienna, Austria, where he lived for the next 8 months.

Knocking about the city, mocked by acquaintances with whom he shared his amateurish spy plans, eventually he entered the Russian Embassy in Vienna and handed over his four classified manuals for the Tomahawk cruise missile system to the duty officer, who assured Weinmann that he would be back in touch with him. When he realized he had given away his only resource and gotten nothing for it, Weinmann decided to return to the United States, fly from there to Russia, and defect (McGlone, 2006). Since his name appeared on a deserter's list, he was arrested at the Dallas Ft. Worth, Texas, airport on March 26, 2006. At his court martial, he pled guilty in a plea bargain to desertion, espionage charges including failure to secure classified information, making electronic copies of classified information, and communicating classified information to a person not entitled to receive it, as well as larceny for stealing and destroying the laptop. Two other espionage charges relating to attempts he made to sell classified information in Bahrain (before he deserted his sub) and Mexico City, Mexico (on his way back to the United States), were dropped in the agreement. Weinmann was sentenced to 12 years in prison, a dishonorable discharge, and forfeiture of all pay and benefits. He would be eligible for parole in 4 years (Amos, 2006b). In the judgment of an examining psychiatrist, Weinmann was "immature, impulsive, and impatient," unable to respond to life's downturns with resilience, and under the impression that he did not have to follow rules (Amos, 2006a).

Lawrence Franklin. Franklin, 59, was at the opposite end of his career path from Ariel Weinmann. Franklin was a South Asia specialist working the Iran desk in the Office of the Secretary of Defense, International Security Affairs Office. He had earned a Ph.D. in Asian Studies, held a Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance for three decades, and, in addition to his academic and policy roles in the federal government, served as a Colonel in the Air Force Reserve. In the 1990s, he developed a strong disagreement with the trend of American foreign policy toward Iran, and he complained that the National Security Council (NSC) was not taking the Iranian threat seriously enough. Starting in April 1999 and continuing until August 2004, Franklin tried to manipulate foreign policy by sharing classified information with various Israeli contacts, including Naor Gilon, the political officer in the Israeli embassy in Washington, DC, and two lobbyists for the American Israeli Public Affairs Committee, Steven Rosen and Keith Weissman.[12]

---

[12] Steven Rosen and Keith Weissman are themselves being prosecuted for espionage for having received verbal classified information from Lawrence Franklin and passing it along to foreign officials and journalists. Their trial in scheduled for January 2008, and it has provoked lively debate among legal scholars about whether this prosecution represents a correct application of the espionage statutes, since it could be seen to threaten First Amendment guarantees of freedom

The information he passed along verbally in furtive meetings with these individuals, which were held in Washington coffee shops, restaurants, and even at the Pentagon Athletic Club, usually consisted of insights into the secret internal deliberations of U.S. policymakers, but it also included intelligence on potential attacks on American forces in Iraq ("Pentagon man," 2006; United States District Court for the Eastern District of Virginia, Criminal complaint, 2005; United States District Court for the Eastern District of Virginia, Superseding indictment, 2005). Israel, a close American ally, denies conducting espionage against the United States, but starting in June 2003 when the FBI became aware of Franklin's activities, agents began monitoring his movements and communications, collecting evidence. A year later, in June 2004, the FBI confronted Franklin and threatened him with a long prison term unless he "wore a wire" for them in a series of sting operations against other suspects. Franklin's wife is confined to a wheelchair with multiple sclerosis and they have five children. Realizing the grim implications his behavior would have for his family, Franklin agreed to cooperate in the FBI stings against Rosen and Weissman and others, who included the political advisor to the prominent exiled Iraqi politician, Ahmed Chalabi (Markon, 2005b; Black, 2004).

Franklin was arrested in May 2005. At first the press portrayed him as a cooperating player in the investigation, but by the fall the FBI had decided he was withholding information, and they sought a superseding indictment. He pled guilty in early October 2005 to two counts of conspiracy to communicate national defense information to individuals not entitled to receive it (that is, to Rosen and Weissman, both private American citizens, but not to the Israeli official also identified), and one count of unlawful retention of national defense information, after a search revealed 83 classified documents he had stored in his home. Some were documents; some were files on nine computer disks (United States District Court for the Eastern District of Virginia, Criminal complaint, 2005; Markon, 2005a). Franklin was convicted on three counts on January 20, 2006, and later sentenced to 12 years and 7 months in prison and fined $10,000 (Johnston, 2006). In an unusual move, the government also began an espionage prosecution of Rosen and Weissman because they had knowingly received classified information from Franklin, even though they had no clearances or access themselves. The case against them is still awaiting trial in March 2008.

Franklin is an example of what might be called a "professorial" spy. Among those recently arrested, his background resembles both Donald Keyser and Ronald Montaperto, who passed intelligence to two Chinese agents to further his academic

---

of speech and freedom of the press. The District court judge in the case, T.S. Ellis, has issued numerous memoranda opinions leading up to the trial clarifying his assumptions. One important memorandum opinion is his United States v. Rosen, 445 F.Supp.2d 602, 643 (E.D. Va 2006), a thorough discussion of his understanding of the various elements required to convict on espionage. His reading of the precedents will, however, remain operative only in his district, the Eastern District of Virginia, leaving room for other interpretations by other judges of the complex espionage statutes (United States District Court for the Eastern District of Virginia, Memorandum opinion, 2006).

standing and pled guilty to unlawful retention of classified documents in 2006 (Gertz, 2006). Highly credentialed by academia, positioned in influential government policy jobs with years of worldly experience, these individuals decided—each in his own way—that they knew better than the information security regulations or the requirements on reporting foreign contacts and not sharing national defense information with them. In Franklin's case, his self-importance, taking American foreign policy into his own hands by leaking classified information to the Israelis in hopes they in turn would influence the NSC, was bolstered by other motives, including his ambition to get a job with the NSC, for which he asked Rosen to "put in a good word for him" (United States District Court for the Eastern District of Virginia, Superseding indictment, 2005).

Leandro Aragoncillo. Aragoncillo seemed the archetype of successful immigration to America, until he was arrested as a spy. He grew up in the Philippines, immigrated to the United States in 1982, and joined the U.S. Marines a year later After a successful military career that included six good conduct awards, he rose to the rank of gunnery sergeant, and in 1999 was appointed the staff assistant to military advisors in the Office of the Vice President, first under Al Gore, and then under Richard Cheney, where he served until 2002. At a White House function in 2000, President Clinton introduced the Filipino staffer to the visiting President of the Philippines, Joseph Estrada, who pocketed Aragoncillo's business card. Later that year, when Estrada's presidency collapsed in an embezzlement scandal, he had an associate contact the well-placed Aragoncillo in the U.S. Vice President's office and ask for help—could Aragoncillo pass along American intelligence that Estrada could use to save his presidency? According to prosecutors, Estrada appealed to his "Filipino patriotism" (Whelan, 2007; Martin, 2007).

Aragoncillo began collecting, stealing, and passing along classified documents from his office at the White House, sometimes using the fax machine there, or taking them out as files on disks in his gym bag, then emailing the files from his home computer (Gaudin, 2007). When his tour in the Vice President's office ended and he retired from the Marines in 2004, he repeatedly tried to get another job with classified access, applying to the CIA, NSA, and the FBI. In the meantime, Estrada fell from power in a coup and turned to working in opposition to the new Philippine president, Gloria Arroyo. In July 2004, Aragoncillo began a new job as a civilian FBI analyst, and he quickly resumed collecting information for Estrada and a group of conspirators who were seeking to overthrow Arroyo. Aragoncillo ran unauthorized database queries (using the same FBI case management system that Robert Hanssen had exploited) and passed on information about American political judgments, antiterrorist plans, and military actions to his conspirators in the Philippines (Diamond, 2005). The FBI arrested him in September 2005, after Aragoncillo attracted the attention of immigration authorities by trying to bail out Michael Ray Aquino, his friend and coconspirator, after Aquino's arrest for immigration violations. Convicted, Aragoncillo was sentenced in July 2007 to 10 years in prison for conspiracy to transmit classified information and other espionage-related offenses (Honan, 2007; “Former spy,” 2007). His is a disquieting case of divided loyalties. A decorated Marine, favored with a prominent White House position, he chose the path of betrayal by a trusted insider. His latent identification with the country of his birth proved to be easily roused and then manipulated, turning him into an enthusiastic spy for the Filipino political opposition. Among the motives for his actions also was his apparent pleasure in working with powerful politicians, which stoked his ego and ambition to play a role in the future of the Philippines.

Ryan Anderson. Anderson, 26, would have shipped out to Iraq to fight as a tank crew member with the Washington State National Guard if not for the complication that the month before he was to leave, he was arrested for attempting to contact, aid, and pass information to an enemy of the United States—Al Qaeda. In February 2004, the FBI arrested him at Fort Lewis, WA, after a brief sting operation that collected video evidence of his actions. At his court-martial in September, he faced five counts of trying to pass intelligence on technical characteristics and military tactics to FBI officers he thought were Al Qaeda. Included in his offer was information on the vulnerabilities of the M1A1 Abrams tank, the Stryker vehicle, and the Humvee, and specific “advice on how to kill American soldiers” (Janofsky, 2004; Sanders, 2004). Two aspects of Anderson’s case are of particular interest as counterintelligence lessons: first, his eccentric behavior and attitudes, which, in retrospect, presented an observable pattern, yet did not arouse enough concern during his training and background investigation to prevent him gaining Secret-level access and a trusted military job; and second, the way his activities were discovered.

Anderson liked guns. He collected them, enthused about them in Internet chat rooms, once walked toward an elementary school carrying one (which earned him a brief arrest and a warning), and shot the local coyotes in backyards and the birds out his college dorm room window (Tizon, 2004). Anderson expressed strong, black-and-white opinions in frequent letters to the local newspaper, but his opinions shifted around dramatically. In high school he said he was a “die-hard Christian” looking for action in a paramilitary group, to which he could bring his own gun (“Ryan G. Anderson,” 2004). He proclaimed himself a patriot, and berated anyone who would not unequivocally support the United States (North, 2004). He became vice president of the high school chapter of Junior Statesmen of America, where he passionately debated political issues and gun control, which he opposed (Shokovsy & Heckman, 2004). In college, Anderson abruptly dropped Christianity and converted to Islam, and took a degree in military history, concentrating on the Middle East. He disturbed people: he alienated the leaders of a Muslim website in Seattle by offering to teach his Muslim friends how to shoot guns. A fellow Guardsman recalled how he decided to steer clear of Anderson after the latter confided that he had joined the Army to “take those skills to the motherland and help liberate the Muslim brothers” (Janofsky, 2004; Rivera, 2004). Anderson told wild, implausible stories while in Guard training: his mother was Jordanian; he had been born in Afghanistan; he had been a mercenary in South Africa; his girlfriend had died in an explosion there—none was true. Eventually fellow Guardsmen reported their concerns about Anderson to their drill sergeant, but they never saw anything come of their report (Rivera, 2004).

At his trial, psychologists diagnosed Anderson with several forms of mental illness, including bipolar disorder and Asperger's Syndrome, a high-performing form of autism characterized by social awkwardness and impaired thought patterns. They pointed to his exaggerations about himself and his penchant for playing roles without recognizing the consequences that might come from those roles—such as the role of "Al Qaeda agent" (Mitchell, 2004). His court-martial held that Anderson did realize the implications of his actions, and sentenced him to life in prison with possible parole, dishonorable discharge, and reduction in rank to private (Sanders, 2004). In his unbalanced, exaggerated reactions and swings of enthusiasm, Anderson resembled Ariel Weinmann, who was his same age and background. In his exaggerations about himself, his bragging, and his role-playing, he resembled the 1980s volunteer spy for Israel, Jonathan Pollard.

Anderson used up-to-the-minute information technology to make his contacts, and he was caught by those using the same technology. He reached out on the Internet to Muslims in the Seattle, WA, area to join their chat rooms, then tried to make contact with Al Qaeda cells across the country. He used cell phone text messaging as well as emails sent over the Internet to "offer his services" to one of the enemies he was training to fight ("Soldier guilty," 2004; Janofsky, 2004). An amateur terrorist watcher, Shannon Rossmiller, a city judge in a small town in Montana, first noticed Anderson's emails to an Islamist website she was monitoring, and she pursued him by posing online as a fellow extremist until she had identified him, and then she contacted the FBI (Fermino, 2004). FBI agents posed as Al Qaeda operatives on line to Anderson, then met him in person several times, videotaping their meetings, before they arrested him (Fermino, 2004; Rivera, 2004). Provoked by the attacks on 9/11 to get involved against terrorism, Rossmiller had become an amateur Islamist website "cyber-sleuth" who used her monitoring skills to reel in a potential military insider betrayal.[13]

[13] Shannon Rossmiller was not the only person who was inspired to monitor Islamist websites after 9/11. She began tracking information and contacts on such sites while convalescing at home from a broken pelvis, having first researched Al Qaeda and Arab culture in general, and learning the rudiments of Arabic. By late 2002, she had made contact with six other individuals around the world who were engaged as amateurs in monitoring Islamist sites on the Internet. Together they founded an online detective agency, the "Seven Seas," incorporating people in Singapore, Canada, Australia, and several places in the United States. They began to work cooperatively, each monitoring thousands of websites, and met online daily to discuss leads and developments. They use translation software with the Arabic and other languages they do not speak, and pass along tips they identify to the authorities (Fermino, 2004; Civilian cyber war, 2004).

Hassan Abujihaad. Paul R. Hall grew up in San Bernardino, CA, and joined the U.S. Navy in 1995 when he was 19. He then converted to Islam, changed his name to Hassan Abujihaad (Abujihaad is "father of jihad" in Arabic) and around the time of the Al Qaeda bombing of the *U.S.S. Cole* in October 2000, began an email correspondence with an English language Islamist website, run by Azzam Publications and based in London. Six years later, in March 2007, he was arrested and charged with materially aiding terrorism with intent to kill U.S. citizens, and with transmitting classified information to those not authorized to receive it (Medina, 2007). In February 2008, Abujihaad stood trial and was convicted March 6 of providing material support to terrorists and of disclosing classified national defense information ("Former sailor," 2008).

Abujihaad allegedly contacted the Azzam Publications website in late 2000 to order videos that encouraged violent jihad. From his military duty station as a signalman on the destroyer *U.S.S. Benfield*, he ordered several videos and corresponded by email about payment and shipment options. He also reached out for personal contact with the anonymous jihadists at the website, expressing his enthusiasm for his adopted faith and for terrorist tactics:

> [Referring to Islamist fighters in one of his videos] with their only mission in life to make Allah's name and mission supreme all over the world, I want to let it be known that I have been in the middle east for almost a total of 3 months [that is, while onboard the *U.S.S. Benfield*]. For those 3 months you can truly see the effect of this psychological warfare taking a toll on junior and high ranking officers…[they were] running around like headless chickens very afraid (United States District Court of Connecticut, Warrant, 2007).

Authorities stumbled on Abujihaad through his links to two other terrorism arrests. One link led to London, UK. In 2004, the founder of the Azzam Publications website, Babar Ahmad, a British national of Pakistani descent, and his colleague, Syed Talha Ahsan, were indicted in the United States and arrested in London for allegedly providing material support to Chechen terrorist groups and the Taliban by running a network of fundraising websites that served as a "recruitment and propaganda tool for al Qaeda and the mujahedeen" (Thomas, Ryan & Date, 2007). The indictments against Ahmad and Ahsan had been filed in U.S. District Court in Connecticut, where one of the website's Internet service providers was located. The two website owners have been fighting extradition to the United States in the British courts since late 2004 (Whitlock, 2005).[14] Shortly before their arrest, a raid

---

[14] The case of Babar Ahmad, which is outside the scope of this study since Ahmad is a British citizen, is nevertheless a fascinating one and merits attention by American counterintelligence officers. Ahmad founded Azzam.com in 1996 as the first English language jihadist website, setting the standard for all subsequent global sites that sought to communicate in English, and for the first time linking to established sites in Arabic, making them accessible to a larger audience. He featured sophisticated graphics on his site, and he advanced a radical agenda in a tone of moderation, luring in the curious and gullible. "It taught an entire generation about jihad," one terrorism researcher noted, "Even in its nascency, it was professional." Since his

on Ahmad's house turned up a password-protected floppy disk with the plan for a U.S. Navy battle group (including the *U.S.S. Benfield*) to transit from California to the Persian Gulf in the spring of 2001. The material on the disk also pointed out vulnerabilities in the ships' defenses and the best locations from which to attack the fleet. Prosecutors allege this classified information was sent by Abujihaad, who held a Secret clearance, passing it along to his friends at Azzam Publications (United States District Court, Warrant, 2007; United States Attorney's Office District of Connecticut, 2007).

The second link led to the greater Chicago area. Abujihaad left the Navy in 2002 with an honorable discharge. In the fall of 2004, he was in Phoenix, AZ, rooming with a fellow would-be jihadist, Derrick Shareef, when news broke that Babar Ahmad had been arrested in London and the Azzam website had been shut down. Shareef in turn was arrested early in December 2006 in Genoa, IL, where he was accused of planning a terror attack on holiday shoppers at the CherryVale shopping mall. He had bartered his stereo speakers for hand grenades (actually duds) from FBI agents in a sting operation ("Ex-sailor accused," 2007). Shareef reported to investigators while under arrest that 2 years earlier, his roommate Abujihaad had been upset when he learned about Ahmad's arrest: he had blurted out, "I think this is about me!" started to cry, and soon set about destroying his videos and deleting his emails from Azzam Publications (White, 2007). This information, added to the evidence of the classified fleet transit plan and the emails that had been exchanged with Azzam personnel, led to Abujihaad's arrest in Phoenix in March 2007. At the time, Abujihaad was working for United Parcel Service (UPS) as a deliveryman and supporting two small children ("Ex-sailor accused," 2007).

This complicated case, unresolved because Abujihaad has not yet been tried or convicted of a crime, suggests that since 9/11, espionage may be intertwined with the visions of global terrorism; espionage may be passing information to a stateless cause that is not rooted in any one country. The case demonstrates the fact that some few American citizens may respond to the Islamist message and use their access to national defense information to try to advance terrorist agendas such as Islamic jihad. It illustrates the power of the Internet to communicate an extremist message and to recruit acolytes to a cause. It depicts the outward ordinariness of life and work that could be maintained by an alleged Al Qaeda recruit while he was on active duty on a U.S. navy vessel, and then while he worked at UPS in Phoenix to support a family.

---

arrest in 2004, Ahmad has worked from prison to publicize his plight and to advance the Islamist cause to an even wider audience. Working with relatives and friends outside who put his material onto his new website, Ahmad argues there that if he were extradited to Connecticut, he would end up a casualty of the unpopular U.S. war on terror, imprisoned in Guantanamo Bay. British public figures, antiwar activists, Muslim support groups, and entertainment notables have come out in support of Ahmad in his claim of innocence; 10,000 people signed an online petition calling on the British government to block the extradition, and in 2005 Ahmad ran for Parliament from his cell, garnering 2% of the vote in his district (Whitlock, 2005). As of the summer of 2007, the appeal of Ahmad's case to refuse extradition was with the European Human Rights Court, Parliament having declined it.

Ahmed Fathy Mehalba. Mehalba immigrated to the United States from his native Egypt in the early 1990s, became a U.S. citizen, and settled in the Boston, MA, area. He held 10 jobs in 10 years, and served briefly in the U.S. Army in 2000 until he was medically discharged for being overweight. During the decade he scrabbled for a living, he had married and divorced, declared bankruptcy in 1997, and been sued by one of his employers, the owner of a taxi company, who claimed that when Mehalba drove a taxi he had not reported his traffic accidents (Murphy & Stockman, 2003; Becker, 2003). In 2002 Mehalba answered a newspaper ad for Arabic speakers to serve as translators, and after background checks by the contractor who supplied linguists to the federal government, Titan Corporation, and by the U.S. Army, he was sent to the interrogation center at Guantanamo Bay, Cuba, to do translation and interpretation.

Seven months later, Mehalba was arrested at Logan International Airport, Boston, MA, on September 29, 2003, while returning from several months of emergency leave to visit his family in Egypt, during which he had also married. Among over 100 computer disks in his luggage was one disk with 725 documents copied onto it, amounting to some 2,000 pages; 368 of the documents were classified SECRET or SECRET/NOFORN that originated with the FBI, CIA, Department of Defense (DoD), or Department of Justice (DOJ) (Murphy & Stockman, 2003; Murphy, 2005a). At the airport, Mehalba denied knowing about the documents or how they got onto the disk in his possession. He was charged with making false statements and with mishandling national security information by removing classified documents from Guantanamo Bay. The fact that he had an uncle in Egyptian military intelligence was of considerable concern, as was his sale on eBay of a personal computer, which the FBI retrieved and found five classified documents still on its hard disk ("Translator to remain," 2003; Grier & Bowers, 2003).

In January 2005, Mehalba changed his plea to guilty and admitted copying and removing the 368 classified documents, claiming he wanted to work on them at home to do a better job. In exchange for his guilty plea, the government agreed to a reduced sentence based on the defense's claim that Mehalba had suffered from diminished mental capacity because, despite his diagnosis several years earlier of bipolar disorder, depression, and attention deficit disorder, he had received no medication for bipolar disorder or his other problems while at Guantanamo Bay (Finer, 2005). He received a 20-month sentence in February 2005; with time already served in jail and time off for good behavior, Mehalba had 22 days left to serve of his sentence (Murphy, 2005b).

In retrospect, Mehalba seems like a poster child for high security risk, since he had issues with many of the 13 Adjudicative Guidelines that determine eligibility for access to classified information, including employment instability, mental health issues, past criminal record, bankruptcy and financial problems, divorce, computer security violations, and having close relatives living in a Middle Eastern country. Yet the government's demand for speakers of Arabic has been so great since 9/11 that Mehalba was hired on by Titan Corporation and sent to Guantanamo Bay.[15] Once there, physical security against insiders was also trusting. When he left for his flight to Egypt, the facility did not regularly perform bag searches or computer searches of contactor employees like Mehalba; it began these security procedures after his arrest (Taylor, 2003). Prosecutors did not prove he passed classified information to others, and although officials from the Joint Terrorism Task Force tried to trace his movements and contacts in Egypt, it is unclear whether he intended or attempted to pass his documents (Taylor, 2003). His case illustrates a new type in recent espionage, one closely intertwined to the American response to terrorism and Islamic extremism.

Almaliki Nour, a.k.a. Noureddine Malki. Since this individual used at least five different aliases during his two or three decades in the United States (when he arrived in the country is in dispute), it is challenging to decide what name to use in discussing his case. He was prosecuted under the name “FNU LNU” for “first name unknown, last name unknown,” since authorities continue to be unsure of his actual name. On his application for naturalization in 1998 and on his applications for employment and a security clearance in 2003, he gave his name as “Almaliki Nour,” so this is the name used here (Waterman, 2005).

Like Ahmed Mehalba, Nour also applied to be an Arabic translator for the U.S. Army in Iraq by seeking work with Titan Corporation. He was hired by Titan in August 2003. Since classified information is involved in the work, Nour filled out an SF-86 application for a security clearance. He received eligibility for access to Secret and then for Top Secret information, and went to work in Iraq in the Sunni triangle, a particularly dangerous assignment, from late 2003 through the fall of 2005 (Rashbaum, 2005a). In September 2005 security concerns appear to have led the FBI to interview Nour about whether he could keep his clearance; in October, personnel from the Joint Terrorist Task Force in New York searched Nour’s Brooklyn apartment and the FBI interviewed him again. In November 2005, he was indicted for making false statements to government officials in three instances: on his naturalization application, on his SF-86 application for access to classified information, and during his interview with the FBI in September (United States District Court of the Eastern District of New York, Complaint, 2005). He pled guilty to the falsification charges the following month (Rashbaum. 2005b). He had lied about his name, his birth date, his birthplace, his parents’ religious background and location, the dates and his reasons for emigrating, and his marriage (Waterman, 2005).

In March 2006, Nour was indicted on additional charges: four counts of unauthorized possession of national defense documents that had been found in searches of his apartment and computer. While in Iraq, he had downloaded a thick

[15] The need was not only for speakers of Arabic. *USA Today* reported in 2003 that detainees at Guantanamo Bay at that time represented 42 countries and spoke 17 languages (Johnson, Squitieri & Moniz, 2003).

classified file from the 82nd Airborne Division of the U.S. Army onto an unclassified thumb drive and then onto a CD, taken other hard copy classified documents, and stored them in his Brooklyn apartment. The classified information described insurgent activities in Iraq in detail: routes pilgrims would take on their religious journeys to Mecca, Saudi Arabia, that would require protection; artillery positions for upcoming actions; and a photograph of a battle map Nour made on U.S. troop routes during the battle of Najaf, Iraq (United States Attorney's Office Eastern District of New York, Press Release, 2007). Further details emerged in the case that called into question Nour's loyalties and his intentions for the classified information in his possession: telephone numbers found in his address book led investigators to document that he had had email contacts and placed over 100 phone calls to various Sunni sheiks, including Al Qaeda leaders, from whom he admitted taking bribes. Images found stored on his computer, which had been downloaded from the Internet, glorified Al Qaeda and the 9/11 attacks (Goldstein, 2007). Prosecutors did not claim to have evidence that Nour actually passed classified information to others. On February 14, 2007, Nour pled guilty to illegally possessing classified defense documents in addition to his earlier guilty plea on the falsification charges (White, 2007). As of March 2008, he has not been sentenced.

On top of his warehousing stolen classified information and his unauthorized interactions with Iraqis, the scale of the lies Almaliki Nour told about himself to U.S. government officials makes his case startling. It highlights the near-impossibility of checking background details for persons who were born and lived abroad. Since the demand to employ native speakers of Middle Eastern languages as interpreters has been urgent during the Iraq war, this security vulnerability has grown. Nour is another instance of the recent intertwining of espionage-related activities with potential terrorism by the Al Qaeda network.

Shaaban Hafiz Ahmad Ali Shaaban. Like Almaliki Nour, Shaaban brought a complicated international past with him when he immigrated to the United States sometime around 1993, settled in Greenfield, IN, and started a second family, which he supported by driving a truck. He is described as a Palestinian born in Jordan who lived in Moscow, Soviet Union, in the early 1970s, where he married a Russian woman, his first wife, and where he may have received intelligence training from the KGB. Later in the 1990s he applied for and received naturalization as a U.S. citizen and in 1997, he legally changed his name to Joe H. Brown. During his stay in the United States, however, he continued to maintain two distinct identities; he used more than a dozen aliases; he held five passports and several social security numbers; and he listed at least 10 addresses during the decade before he was arrested on March 3, 2005 ("Moscow-trained," 2005).

In late 2002 Shaaban, then 52, contacted Iraqis at the United Nations and offered to sell information. He also communicated with contacts in Iraq by phone and fax. The Iraqis arranged for him to fly to Baghdad, Iraq, via Paris, France, and Damascus, Syria. (It was then illegal for Americans to travel to Iraq under provisions of the International Emergency Economic Powers Act [IEEPA], which applied United Nations economic sanctions against Saddam Hussein's regime.) At a secretly taped meeting with Iraqi intelligence, Shaaban offered to sell them the names of 60 CIA operatives then undercover in Iraq for $5 million—names he claimed he could procure on the Russian black market (United States Attorney's Office Southern District of Indiana, Press release, 2005; Gateway Pundit, 2006, January 9; Corcoran, 2006a). He later lowered his price to $3 million, and the Iraqis expressed interest if he could show them a convincing sample. At the same meeting, he told them he planned to use the money to start a pro-Iraqi television station in the United States that would broadcast in Arabic. He offered, for a fee, to organize volunteers to go to Iraq as "human shields" to protect Iraqi infrastructure in the coming war. While in Baghdad, he also broadcast messages of support for Iraq and encouragement of resistance to the United States ("Indiana man," 2005; United States Attorney's Office Southern District of Indiana, Press release, 2006a).

After a year-long investigation, Shaaban was indicted on seven federal charges, and convicted on six of them in January 2006, including conspiracy to commit an offense against the United States, acting as an agent of a foreign government without registering, violation of the IEEPA sanctions, unlawful procurement of an identification document (his driver's license), unlawful procurement of naturalization (for not disclosing his alternate identities), and tampering with a witness (he had threatened his older brother with beheading if he testified at his trial) (Corcoran, 2006b).

Shaaban proved unable to provide the names of the CIA agents he had promised, and it is unclear if he ever could have. His deal with Iraqi intelligence fell apart. At his trial, which started in January 2006 in U.S. District Court for Southern Indiana in Indianapolis, he insisted on handling his own defense. He told the court he had been working for the CIA as a psychological provocateur against Saddam Hussein in 2003, and that the government had him confused with a dead twin brother (Another brother, defying the death threats, testified that Shaaban did not have a twin brother). Shaaban took the stand himself as the only defense witness, where he questioned himself in English, answered himself in Arabic, and waited for the court translation before posing the next question in English (Gateway Pundit, 2006, January 11; Gateway Pundit, 2006, January 23). Convicted in January, he was sentenced in late May 2006 to 13 years and 4 months in prison and stripped of his American citizenship (United States Attorney's Office Southern District of Indiana, Press release, 2006b).

There are aspects of this case that cannot be fully explained from open sources, such as how Shaaban's actions and information from Iraq came to the attention of authorities. Some comedic elements support the evaluation by Shaaban's court-appointed lawyers (frustrated that he mounted his own amateur defense), when they claimed he was only an international con man and never a threat to national security ("13 Years," 2006). On the other hand, despite the local judge's recommendation that Shaaban be incarcerated in Terra Haute, IN, near his family, the Assistant U.S. Attorney in Indiana requested and received from the U.S.

Attorney General, Alberto Gonzalez, a secret administrative order that instead has incarcerated Shaaban in the super-maximum-security facility in Florence, CO. There his life consists of spending 23 hours a day in his cell, with no interaction with other inmates or visitors, no news or reading material, and constant monitoring by security cameras, a regimen he shares with notorious spies and terrorists including Robert Hanssen, Sheik Omar Abdel-Rahman, Richard Reid, and the Unabomber, Theodore Kaczynski (Corcoran, 2006c).

Matthew Diaz. Diaz, 41, dropped out of high school in Kansas in the 11th grade and joined the U.S. Army. Diaz went on to earn his GED and most of a BA in the Army. When he left the Army in 1991, he enrolled in law school. He earned his law degree in 1995, and then joined the U.S. Navy's Judge Advocate General (JAG) Corps. In mid-2004 the Navy sent him to Guantanamo Bay for a 6-month tour as the Deputy Staff Judge Advocate. A week before he arrived in Cuba to begin a job overseeing the coordination of all detainees' potential legal contacts, the Supreme Court ruled in *Rasul v. Bush* that detainees held at Guantanamo did have a Constitutional right to challenge their detentions in U.S. federal court (Wiltrout, 2006; Wiltrout, 2007c; United States Department of the Navy General Court-Martial, Defense response, 2007).

According to his defense lawyers, "LCDR Diaz's billet placed him directly in the middle of the legal and logistical fallout from the Supreme Court's decision in *Rasul*" (United States Department of the Navy General Court-Martial, Defense response, 2007). Later in 2004, lawyers seeking to defend detainees based on the Supreme Court decision tried to learn their names and countries of origin, but they found the Navy, the Pentagon, and the Bush administration unwilling to respond with the information. A DoD lawyer testified at Diaz's court martial that the Pentagon had no intention of making this information public (by turning it over to lawyers who requested it) based on the policy that "We do not publish lists of people captured in armed conflict" (Rosenberg, 2007a).

Early in January 2005, as Diaz approached the end of his tour in Cuba, he saw himself in a "moral dilemma" (Scutro, 2007). He felt what he characterized as the government's "stonewalling" of potential defense lawyers for detainees was wrong and illegal, since in the United States everyone has a right to legal representation, and the Supreme Court had just affirmed that right specifically for detainees. Given his father's incarceration, Diaz felt this issue strongly.[16] He would soon lose his access to the information about the detainees that was being denied. Diaz acted on his dilemma by printing out the database of 550 detainees from a file on the Secret Internet Protocol Router Network (SIPRnet), a classified DoD network. It listed the names, countries, and various codes reflecting what if any intelligence had been gleaned and the interrogation team assigned to the individual (Scutro, 2007). He

[16] Diaz's father was convicted of 12 murders of patients that had been in his nursing care and he was sentenced to death. Despite his father's claim of innocence, he remains on California's death row at the end of 2007.

reduced the pages to index card size, cut the printout into 39 pages, wrapped them in a valentine, and on his last day in Cuba, sent them anonymously to Barbara Olshansky, a lawyer for the Center for Constitutional Rights. The center is a nonprofit legal rights organization in New York City. Olshansky had been one of the lawyers who brought suit in the *Rasul* case, and she was then suing for the detainees' names in federal court. Although the pages were not marked classified, when Olshansky looked at them she inferred she might not have a legal right to see them, and turned them over to the federal court. The judge in turn notified the FBI, which used computer forensics, fingerprinting, and a national security letter requesting Diaz's AOL email to determine who had sent the pages (Wiltrout, 2007a; Rosenberg, 2007b; "Navy lawyer," 2007).

Charges against Diaz were made public late in August 2006. During the investigation he continued to work as a Navy lawyer in Jacksonville, FL. He was charged under the Uniform Code of Military Justice with violating the Navy's information security program by mailing a classified document through the first class mail; with conduct unbecoming an officer by transmitting a classified document to someone who was not authorized to receive it, and three counts of violating the Espionage Act: making a printout of a classified document relating to the national defense with intent or reason to believe it would be used to injure the United States or for the advantage of a foreign nation; knowingly and willingly communicating that information to someone not authorized to receive it, and removing the information without authority with intent to store it in an unauthorized location (United States Department of the Navy General Court-Martial, Defense response, 2007).

The court martial began in May 2007 in Norfolk, VA. Diaz's defense argued that the printout was not really classified—it was not marked as such, and all the information on it subsequently had been made public back in April 2006 in response to a Freedom of Information suit (Wiltrout, 2006). The prosecution argued that the printout had been classified when Diaz mailed it—it had come from the SIPRnet, a classified information system, and the Judge Advocate's office was a "classified environment," of which Diaz was well aware (Scutro, 2007; Rosenberg, 2007a). Others testified that the information in the codes on the printout involved "sources and methods" of intelligence, and the names of countries that did not want to be publicly identified (Rosenberg, 2007b). The court martial found Diaz guilty of four of the charges, which could have meant 24 years in prison. He was sentenced on May 18, 2007, to 6 months in prison and discharge from the Navy, with the likelihood of his military pension being forfeited due to the espionage-related conviction (Wiltrout, 2007b).

"We think this will send a clear message that you can't just release classified information, no matter how good an intention you think you have," the prosecution commented on the trial (Wiltrout, 2007c). Diaz spoke at his sentencing and defended his belief that the detainees were being treated unfairly and illegally, but he admitted that as a naval officer, his choice of action on his belief was wrong. He admitted that other avenues to register his disapproval of his government's policies had been available to him, and he expressed shame that by sending the printout anonymously, he had not acted with the courage of his convictions (Wiltrout, 2007c). Diaz is the first American citizen in the PERSEREC Espionage Database convicted under the espionage statutes of passing classified information to an American rather than a foreign organization. His case illustrates the expansion and reframing of the application of espionage by U.S. authorities since the terrorist attacks of 9/11 that resulted in the declaration of a "global war on terror" and the establishment of a detention center at Guantanamo Bay.

Patterns in the Most Recent Espionage by Americans

This study has focused on the impact of historical context—the issues and pressures that impinged on perpetrators in a given period, the technical means that were available to accomplish their crimes, and how these affected a person's espionage—as well as on how the context of the person's own life shaped his or her decision. Much has changed in the recent past. Options for retrieving information and the media available for storing it, means of electronic communication, shifts in potential and likely customers for American intelligence, even the most likely motives for spying, are different now than they were only a decade ago. In order to capture the context as well as the texture of the most recent cases, they have been described in some detail. These cases may suggest some of the characteristics of what espionage by Americans will look like in the years to come, although, given the uncertainties of the future, it would be imprudent to make predictions based on this small number of cases. In order to help refine counterintelligence efforts, as well as to better understand how espionage is changing, this report has taken two related approaches: it has compared the similarities and differences among spies who began their activities in three time periods over the last 60 years and, in order to sketch in the particular challenges that may lie ahead, it has explored the most recent cases in more depth.

A comparison across these recent cases suggests that they have some common characteristics. Since 2000, four of the 11 espionage offenders have been naturalized citizens, six had foreign attachments or business connections, and seven had foreign cultural ties. The racial and ethnic group identity of these 11 individuals was heterogeneous, with four whites, two blacks, three persons of Arab decent, and two Hispanics. The trend apparent in data on espionage since 1990, toward a more cosmopolitan American population that reflects new sources of immigration and ongoing economic globalization, is borne out in these cases from the recent past.

The 11 most recent espionage offenders include an almost equal number of civilians and uniformed military. Almost all volunteered to commit an espionage-related offense: only two of 11 individuals were recruited. Six of the 11 were intercepted before they could pass information—some before authorities could even unambiguously document an attempt. Nine of the individuals held security clearances; only two persons did not have a current clearance. This subset who began espionage since 2000 therefore presents higher proportions of uniformed military and of persons with security clearances than does the cohort of 37 that began since 1990, which included the subset.

Considering the characteristics of the espionage and the consequences suffered by individuals in the 11 most recent cases, the six interceptions before they could pass information contrast with the most long-lasting espionage career category, in which only two individuals spied for 5 years or more. This relative lack of longevity at spying could be expected in a group that is defined as those who have already been apprehended and who began their activities since 2000. The shift in customers for American intelligence to Al Qaeda, or other loosely affiliated terrorist groups (in some cases it is unclear who were the intended terrorist recipients), can be seen in four of the 11 cases. The shift of focus to the Middle East during the Iraq War is apparent in two additional cases, those that involve Iraq and Egypt. Russia, once so dominant, is a recipient in only one of the most recent cases, and two allies of the United States, Israel and the Philippines, appear as customers in two others. As the first instance in the PERSEREC Espionage Database, espionage was successfully charged against an American citizen for passing classified information to an American organization that the government determined should not have it.

Payment for espionage-related offenses has dwindled to no payment at all in the 11 most recent cases; although five individuals sought money as part of their motivation, it does not appear from open sources that any of these individuals received payment, though for some of them it is somewhat unclear. On the other hand, the prison sentences meted out to the nine individuals who have been sentenced are more severe than in earlier periods: three persons received less than 5 years, four received 5 to 20 years, one received more than 20 years, and one (Ryan Anderson) was sentenced to life in prison.

Two changes are illustrated by the 11 recent cases compared to those who began espionage before 2000: (1) in the methods used to contact potential customers and to maintain contact with them, and (2) in the methods used to steal and store information that could be exchanged. Ten of the 11 individuals relied on the computer and its related technologies to copy, download, store, and transfer from one device to another the information they collected. Seven of the 11 used the Internet to search for customers, to attempt to make contact with terrorist groups, or to send classified information by email attachment. The transformation in information creation, storage, retrieval, and transfer that now characterizes every office and workplace also characterizes the information transfer involved in espionage. The convenience of the Internet, now used by millions, is also preferred by spies and would-be spies.

The motives of those in the 11 most recent cases include most of the motives familiar from earlier periods, and some that are distinctive. Three persons among the 11 had a single motive, and eight persons had multiple motives. For those with more than one motive, a judgment was made as to which of their motives was primary.

Unlike the espionage offenders who began their activities in earlier periods, most of the individuals who began their activities since 2000 were not solely or primarily motivated to spy for money. For five persons money was one of their multiple motives, but only one person, Shaaban Shaaban, sought money as the primary motive among several.[17] Instead, divided loyalties to another country or cause were more common as motives among this recent subset: for two persons, Mehalba and Nour, divided loyalties seem to have been their sole motive, and for three others, Aragoncillo, Anderson, and Abujihaad, they were primary among multiple motives.

Disgruntlement was the second most common motive. For Diaz this was his sole motive (although he was disgruntled with the policies of his government, not the more common disgruntlement against coworkers or workplace), and for three others (Smith, Ford, and Weinmann) disgruntlement was primary among their multiple motives. Ingratiation figured in four cases. Ingratiating himself with those who could help him was the primary motive for Franklin among his multiple motives. Three other individuals (Aragoncillo, Anderson, and Abujihaad) who were motivated primarily by divided loyalties but who had additional motives as well, all sought to ingratiate themselves with people who could provide them with favors, power, or emotional support. Franklin's egotistical desire for recognition—some would characterize this as ambition for advancement in his job—made recognition his strong second motive for his actions.

Two elements in the motivations of the individuals in these 11 cases were notable: the ambition for advancement that was evident in several instances and the number of instances of stockpiling of classified information for potential future use. Ford took boxes of documents that apparently were to be used to further his career in his next job; Franklin passed classified information to lobbyists for Israel, as well as to Israeli officials, to influence the course of American foreign policy and get himself a job at the NSC; Aragoncillo threw in his fortunes with a Philippine opposition politician who, if he had been returned to the presidency of that country, could reward friends like Aragoncillo. In three of the most recent cases, people stockpiled classified materials for future use: Ford's casual storage of boxes of documents in various rooms in his house, Mehalba's downloading of hundreds of classified documents onto a CD and taking them to Egypt on a visit, and Nour's downloading documents onto a thumb drive and then storing them on CDs in his apartment. Stockpiling has occurred in previous instances of espionage in which the individuals had wide access to information (such as John Walker, James

[17] Assigning the relative weight among an individual's discernible motives is an exercise of judgment; other analysts could argue for a different ordering in a particular case.

Harper, and Brian Regan), but to find three instances in a short period of time is somewhat unusual.[18]

Four individuals had serious mental or emotional problems that contributed to their attempts to steal or pass classified information. Smith was diagnosed with severe alcohol addiction and mental instability while awaiting his trial, and was sentenced to treatment for these conditions and time served. Weinmann was diagnosed by a consulting psychiatrist as brittle, immature, and impulsive to a degree that led him into desertion and espionage. Anderson was diagnosed with Asperger's syndrome, a form of autism that may prevent rational thought and dull the awareness of the consequences of one's actions. Mehalba had been diagnosed with bipolar disorder and various attention deficit problems. Three of the four (excluding Smith) passed background investigations that are intended in part to prevent access to classified information by persons with mental illness; instead, the three were granted security clearances and access to classified information.

A Context for Espionage that Includes Global Terrorism

Wars provide opportunities and incentives for espionage rarely matched in peacetime. The Vietnam War provoked the espionage of Ronald Humphrey and Robert Lipka, the Gulf War was the context for the espionage of Michael Schwartz and Albert Sombolay. The persistent Cold War between the United States and the Soviet Union provoked 105 Americans to spy for the Soviets, or Soviet client states in the Eastern Bloc, between 1947 and 1991 when the Soviet Union collapsed. It is not surprising, therefore, that the recent international context, in which the Al Qaeda network and its offshoots have declared holy war—jihad—on the United States, and President George Bush in turn has declared a "global war on terror" on terrorists around the world, has influenced the course of American espionage. It is probable that all instances of espionage by Americans in the recent past have not been uncovered, so conclusions based on these 11 cases must be tentative.

Two Emerging Issues: Identity Vetting and Use of the Internet. Since the United States has announced that Islamist terrorism is an international enemy, terrorists—Islamist or others—have also become the potential consumers of illicit American intelligence that would help them in their contest with the West. Terrorism and espionage are more often found together in the recent cases that began since 2000, and to understand espionage also begins to demand understanding of developments and changes in terrorism. Six of the 11 most recent espionage cases involved terrorists, either as potential or actual recipients of information, or by translators at the Guantanamo Bay detention camp for accused terrorists, or as a protest of conscience against the treatment of those detainees.

[18] The degree to which stockpiling of classified materials before beginning espionage activity is a common pattern needs more study. With the ease of electronic storage capabilities, this behavior could be facilitated in the future.

One issue that straddles the response to global terrorism and efforts of prevent espionage is the vetting of a person's identity. The need for more robust mechanisms for proving one's identity became clear after the attacks on 9/11, which demonstrated how easily the foreign hijackers could exploit lax identity vetting procedures. That realization has led to the more rigorous requirements for identity vetting issued by the federal government in Homeland Security Presidential Directive 12 in 2004, but these procedures are still under development. The recent espionage cases illustrate many of the current difficulties with identity vetting: the two translators, Mehalba and Nour, and the opportunist Shaaban, hid parts of their past lives, made up false identities, used multiple identities and false documents, and generally demonstrated how frustrating it has been to ascertain the identity and background of persons born and raised in countries where records are difficult for American investigators to check, and the danger of alerting foreign intelligence agencies may make vetting counterproductive. They also illustrate the need for better cross-checking and comparison of data on identity between agencies. Yet in order to engage global terrorism, the language skills and cultural insights of first or second generation immigrants to the United States have never been more necessary. These cases illustrate issues against which security and counterintelligence authorities have been struggling for some time, including the use of false identities and fictional backgrounds when immigrants apply for naturalization or for access to classified information, the maintenance of more than one Social Security account to support a false identity, the presentation of false identification documents, and falsifying security clearance applications to gain sensitive employment.

A second issue that mixes global terrorism with recent espionage is how terrorist cells are evolving to rely on the Internet. In the 6 years since 9/11, Islamist terrorism has adjusted some of its tactics in the face of relentless Western surveillance and opposition. Relevant here is its shift away from a single network to a loose, shifting series of regional networks and "home-grown cells" (Mazetti, 2007), and the ever more sophisticated use of the Internet to maintain a "virtual community of believers," now that a physical community is more often hounded and broken up (Coll & Glasser, 2005). Individuals or ad hoc cells of friends now can find their terrorist training manuals and statements of jihadist ideals online, sampling from "a massive and dynamic online library of training materials," that includes manuals, reports, and videos covering topics such as how to develop lethal poisons, how to make bombs, how to raid a house, how to shoot a rocket-propelled grenade, how to blow up a car, and many, many more tips and techniques. From its beginnings, Al Qaeda relied on technology; it was staffed by "educated and privileged gadget hounds," while recently a younger generation of Al Qaeda followers has taken its Internet skills to even higher levels, relying on jihadist bulletin boards for communication, websites with free file upload services, using fake email spam in which to disguise actual messages, and hacking into vulnerable servers worldwide to take them over to "hop from Web address to Web address," evading the cyber-investigators tracking them (Coll & Glasser, 2005).

This reliance on the Internet by terrorists increases the potential customer base for American spies peddling information by multiplying the number of discrete cells with which spies might make contact. Terrorists' use of the Internet is apparent in the most recent espionage cases discussed here. Terrorists and spies agree on the usefulness of the Internet for their purposes. Spies and would-be spies have eagerly employed any technology available to them, and use of automated information systems for espionage dates back into the 1980s (in the activities of both Aldrich Ames and Robert Hanssen, for example), when the first computers appeared in intelligence offices. What has changed is the ubiquity of spies' reliance on electronic files for copying, storing, transmitting, and hiding. The laptop computer, the thumb drive storage device, and the Internet have only made espionage quicker and easier while it has smoothed the contact with customers.

Global Terrorism Puts New Strains on American Espionage Statutes. The espionage statutes of the United States date from 1911, and their current provisions still embody a formulation that was adopted in the face of World War I in 1917. They have been expanded with new provisions, while the old ones remained in effect, creating what many observers have called a "patchwork" (Elsea, 2006b). This has caused difficulties interpreting and applying the various statutes to particular potential instances of espionage in the modern context, and more so since 2001 with the recognition of a transnational terrorist threat. District Court Judge T.S. Ellis notes in a Memorandum Opinion issued in December 2006 that it is possible that

> a more carefully drawn statute could better serve both the national security and the value of public debate. Indeed, the basic terms and structure of this [espionage] statute [referring to Title 18 USC 793] have remained largely unchanged since the administration of William Howard Taft. The intervening years have witnessed dramatic changes in the position of the United States in world affairs and the nature of the threats to our national security. The increasing importance of the United States in world affairs has caused a significant increase in the size and complexity of the United States' military and foreign policy establishments, and in the importance of our nation's foreign policy decision making. Finally, in the nearly one hundred years since the passage of the Defense Secrets Act mankind has made great technological advances affecting not only the nature and potential devastation of modern warfare, but also the very nature of information and communication (United States District Court for the Eastern District of Virginia, United States of America v. Steven J. Rosen and Keith Weissman, 2006).

Inconsistencies in important terms used among the various provisions of the main espionage statutes are one cause of difficulties.[19] The early statutes (now in Title 18 USC 793 and 794) that define espionage refer to "national defense information" or "information relating to the public defense," while later statutes refer specifically to "classified information" (for example, in 18 USC 798). Some provisions require proof of the intent of the action as "injury to the United States or to the advantage of a foreign nation," others do not mention intent. Some add that the action must be done "willfully," others do not. Some specify that the unlawful recipient of the information includes not only foreign governments, but also "a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States," or even "a representative, officer, agent, employee, subject, or citizen of such a government, faction, party, or force," yet other provisions do not include factions or parties and only refer to foreign governments (Elsea, 2006b). These inconsistencies may result in unpredictable applications of the statutes; according to one researcher, the inconsistencies leave gaps in the protection of "information the government legitimately needs to protect."

> Certain information is protected regardless of whether it belongs to the government or is subject to normal classification. Technical and scientific information, for example, can be restricted regardless of source. Information related to "the national defense" is protected even though no harm to the national security is intended or is likely to be caused through its disclosure. However, nonmilitary information with the potential to cause serious damage to the national security is only protected from willful disclosure with the specific intent to harm the national interest, or with the knowledge that such harm could occur (Elsea, 2006b).

In the recent instances of espionage-related offenses discussed here in which Al Qaeda or other terrorist groups have been the intended or actual recipients of information, it is unclear whether current statutes actually prohibit passing information to a transnational terrorist network, since the specified "faction, party, or force" meant to cover a nonstate group is followed by the phrase "within a foreign country," not a group linked simultaneously across the boundaries of various foreign countries (Elsea, 2006b). One legal scholar suggests that the espionage statutes should be revised to add the word "enemy" to the phrase that is currently in place "to the advantage of any foreign nation," so that the prohibition would be against passing information "to the advantage of an *enemy* of the United States," and then defining "enemy" to include both lawful and unlawful combatants under the Military Commissions Act of 2006, which specifically refers to nonstate actors such as the Taliban and Al Qaeda (Epstein, 2007).

[19] Title 18 USC Sections 792 through 782, 951, and 1924; Title 50 USC Section 783; and the Uniform Code of Military Justice (UCMJ) Article 106a, found at Title 10 USC Section 906a are the provisions being considered here as the main espionage statutes.

Uncertainty about whether our espionage statutes cover transnational terrorist networks illustrates the strain put on the legal framework for espionage by recent cases of espionage that have involved terrorist groups as intended or actual recipients of information. The "traditional" act of espionage assumes the action causes an injury to the United States or gives an advantage to another country or countries. When Hassan Abujihaad allegedly sent U.S. Navy plans to a supporter of terrorism in London, or when Ryan Anderson went online looking for Al Qaeda so he could offer them information about the vulnerabilities of American military vehicles and how to kill Americans soldiers, their actions may have caused injury to the United States, but they did not give an advantage to another nation state, only to individuals loosely connected across countries, often in the virtual linkage made possible by the Internet. When Matthew Diaz sent 500 names of detainees being held by the United States as possible terrorists at Guantanamo Bay to an American legal aid group in New York City, the recipients of his classified information were fellow American citizens (though undoubtedly they were also "individuals not authorized to receive it"). Diaz was found guilty at court martial of two of the three espionage provisions with which he had been charged, but not guilty of intent to injure the United States.[20] Since he was acquitted of causing injury, left unclear is whether the guilty verdicts for the other two charges imply that Diaz's actions did provide an "advantage to a foreign nation," and if so, which nation it was. The conjunction of espionage and terrorism raises a tangle of legal, political, and definitional difficulties illustrated in some of the recent espionage cases, and it shines a spotlight on the need for revision and reformulation of the statutes that govern the crimes of espionage.

A SUMMARY OF MAJOR FINDINGS SINCE 1990

This summary briefly describes traits and trends among the 37 individuals who began espionage since 1990. It is a selective summary, and does not include every finding.

It is not straightforward to summarize this study's findings without repeating each finding in the same detail as it was stated initially, with numbers and percentages

---

[20] The charges against Diaz included: UCMJ Article 92, disobeying the Department of the Navy Information Security Program by mailing classified information and failing to secure it while doing so; UCMJ Article 133, conduct unbecoming an officer by "*wrongfully and dishonorably* transmitting classified information to an unauthorized individual;" UCMJ Article 134, general misconduct, for three specifications of espionage: 1) violation of Title 18 USC 793(b), knowingly and willfully making a printout of classified SECRET information respecting the national defense with *the intent or reason to believe that the information was to be used to the injury of the United States or to the advantage of a foreign nation* (all italics in original); 2) violation of Title 18 USC Section 793, knowingly and willfully communicating information relating to the national defense of the United States of America, which LCDR Diaz had *reason to believe* could *be used to the injury of the United States or to the advantage of a foreign nation*; and 3) violation of Title 18 USC Section 1924, knowingly removing materials containing classified information without authority and *with the intent to retain such materials at an unauthorized location.* (United States Department of the Navy General Court-Martial, 2007). Diaz was convicted on four of the five counts, acquitted of the charge under Section 793(b), intent to injure the United States (Wiltrout, 2007c).

and comparisons across the three groups that have been defined by when individuals began espionage. For example, to summarize by saying that in the group that began spying since 1990 a trait is “more likely” or “more common,” begs questions about how much more likely it is, and how a finding for this group compares to groups that began spying earlier. In order to summarize the major findings on trends in espionage by Americans in the recent past, and still satisfy the inevitable curiosity a summary provokes about the details that support the summary, for each statement here, page references are provided that refer back to the tables, examples, and discussions in the report itself.

Personal Attributes. The individuals who began espionage since 1990 were older than earlier spies (p. 7). They had more years of education, and twice as many of them held advanced degrees (p. 9).

Foreign Influence. Since 1990 spies were more likely to be naturalized citizens and to have foreign relatives, foreign business and professional connections, and foreign cultural ties (pp. 10-11). Reflecting the increased salience of foreign ties among individuals in the recent cohort that began since 1990, spying prompted by divided loyalties has become the most common motive for American espionage, replacing spying for money as the primary motive (pp. 12-14).

Employment and Clearance. Among those who began espionage since 1990, twice as many of individuals have been civilians (both government employees and contractor employees) as have been members of the uniformed military (pp. 14-15). More people have been engaged in unusual occupations not normally associated with espionage when they began spying (p. 15). There has been a continuing trend toward holding Secret clearances, with a smaller proportion of individuals holding Top Secret clearances (p. 15-16). A larger proportion—more that one third—of the recent cohort that began since 1990 held no security clearance when they began espionage (p. 16). Methods for obtaining information to be passed to another country or group without holding a security clearance included: using the access of an accomplice, relying on memory from past access, passing unclassified but sensitive information, stealing classified information, and claiming access to information which the person did not in fact hold (pp. 16-22). Ambiguities in espionage statutes may account for the increase in espionage by persons with no security clearance (pp. 23-24).

Characteristics of Espionage. Two thirds of the individuals who began espionage since 1990 volunteered rather than being recruited, a proportion that has remained about the same since 1980 (p. 25). Spies in the recent cohort that began since 1990 were less likely to be intercepted before passing information, but more likely to be caught within 5 years (p. 25). Typical customers of information from American spies have shifted from the Soviet Union during the Cold War to an array of recipients, prominently including various Middle Eastern countries, Cuba, and the stateless terrorist network, Al Qaeda and its offshoots (p. 28).

Consequences of Espionage. Among individuals who began espionage since 1990, only 19% have received any payment for espionage, either because they were intercepted or because they spied from other motives (p. 30). Amounts of payment have been declining over time (p. 30). Individuals in this recent cohort were more likely to serve time in prison, but to receive somewhat lighter sentences (p. 31).

Motivations for Espionage. Money was not the sole or primary motive for espionage as frequently since 1990. From 47% and 74% of the two earlier groups who spied solely for money, in the recent cohort a single individual spied solely for the money (p. 33). Divided loyalties to another country or cause besides the United States have replaced money as the most common motive for espionage by Americans in the recent period (pp. 34-35). Disgruntlement, ingratiation, and recognition or ego each motivated smaller numbers of the individuals in the recent cohort (pp. 35-37). Coercion, never a common motive among American spies, has not been a sole or primary motive for espionage since 1980 (p. 37).

Vulnerabilities that May Increase Risk of Insider Threat. Among the issues of security concern defined in the 13 *Adjudicative Guidelines* that are used to determine eligibility for a security clearance, for those who began espionage since 1990 fewer individuals (compared to the two earlier cohorts) demonstrated alcohol or drug problems, no one had a recognized problem with gambling, but more individuals had issues of security concern with allegiance and foreign preference or foreign influence (pp. 40-41). Among the typical financial motives of debt or greed, debt continued to motivate espionage more often than greed. (p. 42).

Life Events as Triggers for Espionage. One third of all 173 individuals, considered across all three time periods, experienced life crises (positive or negative) 6 to 8 months before they began espionage, including events such as divorce, death in the family, moving one's household, or entering a new significant relationship (pp. 42-43). Available data do not support identifying a decrease or increase over time in the incidence of cases that included a potential trigger event (pp. 43-44).

The Most Recent Espionage by Americans. The 11 individuals who began espionage since 2000 are a subset of the cohort considered in this study that began since 1990. The subset of 11 persons is too small to support stable conclusions, but it offers suggestive characteristics to watch for in the future (p. 61). Most of these individuals made use of computer technology to retrieve, store, and transfer information. Many of them (7 of the 11) made use of the Internet to make or maintain contact with customers (p. 62). The 11 individuals reflected the shift in motivation seen in the larger cohort that began espionage since 1990, that is, away from money and toward divided loyalties as a sole or primary motive (pp. 62-63). Other common motives, including disgruntlement, ingratiation, and ego persist in the most recent cases (p. 61). Ambition for career advancement appears as a distinctive motive in several recent cases. The incidence of deliberate stockpiling of classified materials for future sale may be increasing (p. 63). Four of the 11 individuals suffered from mental health issues (p. 63).

A Context for Espionage that Includes Global Terrorism. Terrorism is more involved in the espionage cases that began since 2000 (p. 64). Six of the 11 recent cases involved terrorists (p. 64). The most recent espionage cases illustrate the difficulties and importance of accurately vetting a person's identity (p. 64). The evolution of terrorism into shifting regional networks and "home-grown cells" has also increased the customer base for espionage (pp. 64-65). Terrorists' increasingly sophisticated use of the Internet mirrors its use by spies. Recent cases that intertwine espionage and terrorism put new strains on American espionage statutes, which have received little systematic updating in many decades. In the recent instances in which Al Qaeda or other terrorist groups have been the intended or actual recipients of information, it is unclear whether current espionage statutes actually prohibit passing information to a transnational terrorist network, suggesting that reorganization and redrafting of the statutes is needed (pp. 65-67).

REFERENCES

Amos, C. (2006a, December 6). Psychiatrist calls sailor in espionage case immature. *Navy Times*, p. 2 [Weinmann].

Amos, C. (2006b, December 7). Submarine sailor gets 12 years for espionage. *Navy Times,* p. 1 [Weinmann].

Bamford, J. (2001, August 28). Guard the secrets, then catch the spies. *The New York Times,* p. A28 [Regan].

Barandes, L. (2007). A helping hand: Addressing new implications of the Espionage Act on freedom of the press. *Cardozo Law Review*, 29: 371-403.

Becker, M. (2003, October 2). Red flags on Gitmo suspect. *The New York Daily News*, p. 3 [Mehalba].

Black, E. (2004, December 31). Spat erupts between neocons, intelligence community. *Forward.* Retrieved from http://www.forward.com/main [Franklin].

Black, D., Gates, G., Sanders, S., & Taylor, L. (2000). Demographics of the gay and lesbian population in the United States: Evidence from available systematic data sources. *Demography, 37*(2), 139-154.

Borger, J. (2001, March 6). Carry on spying. *The Guardian* (London, UK), pp. 5-6. [Red Avispa; Guerrero].

Bragg, R. (2000, May 31). I.N.S. official is convicted on charges of espionage. *The New York Times,* p. B2 [Faget].

Brenner, M. (1997, September 21). A traitor's life: Why Earl Pitts betrayed his country. *The Washington Post Magazine,* p. 6.

Brinkley, J., Bradsher, K., & Oppel, R. (2004, September 17). U.S. diplomat quit post, then met with Taiwan agents. *The New York Times,* p. 8. [Keyser].

Brock, B. (1987, July). Spying's dirty little secret. *Money, 16*(7), 130-148.

Brodie, J. (1991, December 4). US Gulf war spy is jailed for 34 years. *The Daily Telegraph* (London, UK), p. 2. [Sombolay].

Castaneda, R. (2005, November 30). Md. Man on trial over NSA documents. *Washington Post*, p. A1 [Ford, Jr.].

Cho, D., & Cha, A.E. (2007, November 16). Chinese spying is a threat, panel says. *The Washington Post,* p. 9.

Ciccarello, N., & Thompson, T. (2003, March). Money, the fear of failure, and espionage. Report of an interview with Robert Philip Hanssen, 5 December

2002. Washington, DC: The Personnel Security Managers' Research Program.

Civilian cyber war. Group of cybersleuths works to track down possible terrorists on the internet. (2004, July 17). *ABC News*. Retrieved from http://www.ABCNEWS.com.

Coll, S., & Glasser, S. (2005, August 7). Terrorists turn to the web as a base of operations. *The Washington Post,* p. A1.

Corcoran, K. (2006a, January 15). Accused Iraq agent's trial ends its 1st week. *The Indianapolis Star,* p. 2B [Shaaban].

Corcoran, K. (2006b, January 26). Shaaban Shaaban convicted of 6 federal crimes, *Current Events Discussion Forum.* Retrieved from http://www.curevents.com

Corcoran, K. (2006c, November 6). Convicted in spy case, locked away in secrecy. *The Indianapolis Star,* p. 4B [Shaaban].

Crawford, D. (1998) Volunteers: The betrayal of national defense secrets by Air Force traitors. Washington, DC: Government Printing Office [Buchanan].

Cummings, J. (1994, September 13). Federal worker sentenced: Stealing U.S. files brings prison term; Ga. Woman gets 3-year sentence. *The Atlanta Journal and Constitution* (Atlanta, GA), p. 6. [Jones].

Davison, P. (1998, September 16). Cubans infiltrated US military base, says FBI. *The Independent (*London, UK*).* p. 10 [Hernandez; Red Avispa].

Defense Personnel Security Research Center. (2004). *Espionage cases 1975-2004, Summaries and sources.* Monterey, CA: Author.

Department of Defense. (2005, January). Defense language transformation roadmap. Washington, DC: Author.

Department of Justice, Office of the Inspector General. (2006). A review of the FBI's handling and oversight of FBI asset Katrina Leung. Washington, DC: Author.

Diamond, J. (2005, October 7). Analyst allegedly used same system as spy. *USA Today*, p. 3 [Aragoncillo].

Duffy, S. (1997, September 25). Spy sentenced to 18 years. *The Legal Intelligencer*, p. 3 [Lipka].

Edgar, H., & Schmidt, Jr., B.C. (1973). The espionage statutes and publication of defense information. *The Columbia Law Review, 73*(5): 929-1087.

Elsea, J. (2006a, December 21). The protection of classified information: The legal framework. Congressional Research Service: CRS Report for Congress. Washington, DC: Government Printing Office.

Elsea, J. (2006b, December 26). Protection of national security information. Congressional Research Service: CRS Report for Congress. Washington, DC: Government Printing Office.

Engelberg, S. (1986, June 6). Spy telling of Israeli operations: Pelton convicted of selling secrets; former official found guilty on 4 counts in espionage trial. *The New York Times,* p. A2.

Epstein, R.D. (2007). Balancing national security and free-speech rights: Why Congress should revise the Espionage Act. *Commlaw Conspectus*, 15: 483-512.

Executive Order 10450, *Security requirements for government employees,* April 27, 1953.

Executive Order 12958, *Classified national security information*, April 17, 1995, as amended by Executive Order 13292, *Further amendment to Executive Order 12958,* March 25, 2003.

Executive Order 12968, *Access to classified information*, August 2, 1995, as amended by Executive Order 13388, *Further strengthening the sharing of terrorism information to protect Americans,* October 25, 2005.

Ex-sailor accused of supporting terrorism. (2007, March 8). *CBS News/Associated Press.* Retrieved from http://www.cnsnews.com/stories [Abujihaad].

Ex-sailor charged in terror case discussed attacking military personnel, prosecutor says. (2007, July 24). *Arizona Daily Star,* p. B3. [Abujihaad].

Federal Bureau of Investigation. (2002). Affidavit in support of a complaint against and arrest warrant for John Joungwoong Yai and Susan Youngja Yai. Los Angeles: Author.

Fermino, J. (2004, July 12). Lady who nets spies. *The New York Post*, p. 10 [Anderson].

Finer, J. (2005, January 11). Interpreter pleads guilty to taking data. *The Washington Post*, p. 6 [Mehalba].

Five Cubans convicted of espionage in U.S. (2001, June 9). Associated Press, reprinted in *The Monterey County Herald* (Monterey, CA), p. A6. [Red Avispa; Guerrero].

Flaccus, G. (2007a, March 22). Chinese-born engineer awaits trial. *The Washington Post,* p. 4 [Mak].

Flaccus, G. (2007b, June 6). Plea deal ends China tech export case. *The Washington Post*, p. 6 [Chiu].

REFERENCES

Foreign Associations Ad Hoc Working Group. (2006, December). *Minutes.* Washington, DC: Author.

Former sailor is convicted in terror case. (2008, March 6). *The New York Times,* p. A1 [Abujihaad].

Former spy and Cheney aide gets 10 years. (2007, July 18). *CBS News*. Retrieved from http://www.cbsnews.com/stories/2007/07/18/national/ [Aragoncillo].

Gateway Pundit. (2006, January 9). Trial begins for Indiana truck driving Saddam Hussein spy. Retrieved from http://gatewaypundit.blogspot.com/2006/01/[Shaaban].

Gateway Pundit. (2006, January 11). Trial of Shaaban Hafiz Ahmad Ali Shaaban or "Joe Brown" heats up. Retrieved from http://gatewaypundit.blogspot.com/2006/01/

Gateway Pundit. (2006, January 23). Russian trained, Indiana truck driver spy grills self in trial. Retrieved from http://gatewaypundit.blogspot.com/2006/01/[Shaaban].

Gaudin, S. (2007). If an FBI analyst can steal national secrets, what are your workers lifting? *Information Security Weblog*. Retrieved from http://www.informationweek.com/blog/main/archives/2007/05/ [Aragoncillo].

Geis, S. (2006, May 25). FBI officials are faulted in Chinese spying case. *The Washington Post,* p. 13 [Leung].

Gerstein, J. (2006, July 14). A novel-like tale of cloak, dagger unfolds in court. *The New York Sun.* Retrieved from http://www.nysun.com/article/36073 [Keyser].

Gertz, B. (1993, February 6). Ex-DIA official pleads guilty in document leak. *The Washington Times*, p. B1 [Hamilton].

Gertz, B. (2006, September 9). Pentagon analyst gets light jail term. *The Washington Times,* p. 7 [Montaperto].

Gertz, B. (2007, June 8). Inside the ring: spy damage. *The Washington Times,* p. 8 [Mak].

Golden, T. (2002, October 17). Ex-U.S. aide sentenced to 25 years for spying for Cuba. *The New York Times,* p. A6 [Montes].

Goldstein, J. (2007, February 9). Classified documents from Iraq are at the heart of translator case. *The New York Sun.* Retrieved from http://www.nysun.com/article/48353 [Nour].

Glazov, J. (2007, August 27). True believer. *Front Page Magazine*, p. B6 [Montes].

Grieco, E., & Cassidy, R. (2001, March). Overview of race and Hispanic origin. *Census 2000 Brief*. Washington DC: U.S. Census Bureau.

Grier, P. (1997, January 27). Ex-wife's view of life with an accused CIA spy. *The Christian Science Monitor,* p. 1 [Nicholson].

Grier, P.,& Bowers, F. (2003, October 23). Guantanamo probe stirs wider security concerns. *The Christian Science Monitor*, p. 2 [Mehalba].

Grier, P. (2005, November 30). Spy case patterns the Chinese style of espionage. *The Christian Science Monitor,* p. 1 [Mak].

Hall, C. (1997, March 1). Plea deal arranged in 2 spy cases. *The Washington Post,* p. A1 [Pitts, Nicholson].

Hawkins, W.R. (2007, March 4). GAO Report: Uncoordinated federal technology policies put nation at risk. United States Business & Industry Council. Retrieved from http://www.americaneconomicalert.org/

Herbig, K.L. (1994). A history of recent American espionage. In T.R. Sarbin, R.M. Carney & C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal* (pp. 39-67). Westport, CT: Praeger.

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

Heuer, R.J. (2007). Rethinking the adjudication of foreign influence and foreign preference issues. Unpublished discussion paper. Monterey, CA: Defense Personnel Security Research Center.

Holthaus, D. (1991, December 5). Husband's no spy, woman says. *The Gazette* (Montreal, CD), p. 1 [Sombolay].

Honan, E. (2007, July 18). Ex-Cheney aide gets 10 years in prison in spy case. *Reuters*, p. 3 [Aragoncillo].

Horn, R. (2000, December 2). Sailor faces likely probation after stealing Navy disks. *The Sun* (Bremerton, WA), p. 2 [Smith].

Indiana man charged with trying to sell secrets to Iraq. Indictment: Man offered to get U.S. intelligence agents' names. WPXI, Indianapolis. Retrieved from http://www.wpxi.com [Shaaban].

Janofsky, M. (2004, February 13). Guardsman taken into custody and examined for Qaeda tie. *The New York Times*, p. A2 [Anderson].

Johnson, K., Squitieri, T., & Moniz, D. (2003, October 2). Three suspects' screening questioned. *USA Today*, p. 3.

Johnston, D. (1994, March 2). U.S. shows list of secrets Moscow wanted to obtain. *The New York Times,* p. A2 [Ames].

Johnston, D. (1996, September 26). Navy analyst accused as spy for South Korea. *The New York Times,* p. B1 [Kim].

Johnston, D. (2006, January 21). Former military analyst gets prison term for passing information. *The New York Times*, p. 6 [Franklin].

Krause, M. (2002, April). Divided national loyalties: A primer for personnel security staff. Washington, DC: Personnel Security Managers' Research Program.

Krikorian, G. (2003, February 6). FBI watched spy suspect for 7 years. *The Los Angeles Times,* p. 3 [Yai].

Krofcheck, J.L., & Gelles, M.G. (2005, January). *Behavioral consultation in personnel security: Training and reference manual for personnel security professionals.* New York: Yarrow Associates.

Lacayo, R. (1996, December 2). Teacher or traitor; What if CIA spy Aldrich Ames wasn't the last of the moles? After months of surveillance, agents arrest another one of their own. *Time Magazine,* p. 30 [Nicholson].

LeFebvre, S. (2005). Sex again: The Smith-Leung spy case. *International Journal of Intelligence and Counterintelligence*, *18*(2), 296-304.

LeFebvre, S. (2007). The case of Denald Keyser and Taiwan's National Security Bureau. *International Journal of Intelligence and Counterintelligence, 20*(3), 512-526.

Lentz, P. (1985, June 13). Why spy? Try greed, high tech, lax controls. *The Chicago Tribune*, p. A1.

MacIntyre, B. (1999, September 13). Files led FBI to agent at work in US. *The Times (*London, UK*),* p. 3 [Lipka].

Markon, J. (2003a, January 28). Spy suspects portrayals: Disloyal or fantasizing. *The Washington Post,* p. B1 [Regan].

Markon, J. (2003b, February 25, 2003). Convicted spy won't get death penalty. *The Washington Post*, p. B1 [Regan].

Markon, J. (2003c, March 21). Convicted spy accepts life sentence. *The Washington Post,* p. B1 [Regan].

Markon, J. (2003d, July 31). Spy hid secret papers in parks. *The Washington Post,* p. B1 [Regan].

Markon, J. (2004, September 16). Powell aide gave papers to Taiwan, FBI says. *The Washington Post*, p. A1. [Keyser]

Markon, J. (2005a, July 3.) FBI tapped talks about possible secrets. *The Washington Post.* p. A2 [Franklin].

Markon, J. (2005b, October 6). Defense analyst guilty in Israeli espionage case. *The Washington Post.* p. A4 [Franklin].

Markon, J. (2006, August 6). UPDATE: Alleging lack of cooperation, prosecutors seek to void plea in classified-documents case. *The Washington Post,* p. C2 [Keyser].

Martin, J. (2007, July 18). Courier in spy case gets 6-year sentence. *The Star-Ledger* [NJ], p. 2 [Aragoncillo].

Masters, B. (1997a, March 4). CIA spy admits guilt, says he'll reveal damage. *The Washington Post,* p. A1 [Nicholson].

Masters, B. (1997b, June 24). Ex-FBI agent gets 27 years for passing secrets to Moscow. *The Washington Post,* p. A2 [Pitts].

Mazzetti, M. (2007, April 2). New generation of Qaeda chiefs is seen on rise. *The New York Times,* p. A1.

Mazzetti, M., & Lewis, N.A. (2007, April 3). U.S. cites Indian government agencies in weapons controversy. *The New York Times,* p. B1.

McGlone, T. (2006, December 10). Why a patriotic teen joined the Navy and then turned to espionage. *The Virginian-Pilot* (Hampton Roads, VA), p. 1 [Weinmann].

Medina, J. (2007, March 9). Sailor started e-mail on terror, U.S. says. *The New York Times,* p. 9 [Abujihaad].

Meyer, J. (2007, October 11). U.S. targets illegal sales to enemies. *The Los Angeles Times,* p. A7.

Mitchell, M. (2004, September 2). Accused GI called bipolar, 'social misfit.' *The Seattle Post-Intelligencer,* p. 17 [Anderson].

Molotsky, I. (1985, June 6). Money said to have replaced ideology as main spy motive. *The New York Times,* p. B13.

Moscow-trained Jordanian tried to sell U.S. agents to Iraq. (2005, March 7). *Weekly Intelligence Notes.* Washington, DC: Association for Intelligence Officers [Shaaban].

Murphy, S. (2005a, January 8). Plea deal signals trouble with case against translator. Th*e Boston Globe,* p. 3 [Mehalba].

Murphy, S. (2005b, February 19). Translator sentenced in Guantanamo documents case. *The Boston Globe*, p. 2 [Mehalba].

REFERENCES

Murphy, S., & Stockman, F. (2003, October 1). Guantanamo translator seized at Logan. *The Boston Globe,* p. 1 [Mehalba].

National news briefs: Former C.I.A. operative gets 5 years in prison. (1998, September 27). *The New York Times,* p. A12 [Groat].

Navy lawyer on trial for leaking info. (2007, May 14). *Morning Edition.* National Public Radio, transcript [Diaz].

North, S. (2004, February 13). Letters to *The Herald* voiced strong opinions. *The Daily Herald* [Everett, WA], p. 18 [Anderson].

Pentagon man jailed over spying. (2006, January 20). *British Broadcasting Corporation News.* Retrieved from http://news.bbc.co.uk/go/pr/fr [Franklin].

Pressley, S. (1998, September 15). 10 arrested on charges of spying for Cuba. *The Washington Post,* p. 2 [Red Avispa].

Rashbaum, W.K. (2005a, September 8). Translator in Iraq lied in citizenship bid, U.S. says. *The New York Times,* p. 9 [Nour].

Rashbaum, W.K. (2005b, December 21). Metro briefing/New York: Brooklyn: Arabic translator admits he lied. *The New York Times,* p. D4 [Nour].

Reza, H.G. (2007a, May 11). Engineer in China case convicted. *The Los Angeles Times,* p. 1 [Mak].

Reza, H.G. (2007b, June 7). 5th defendant in spy case pleads guilty. *The Los Angeles Times,* p. 4 [Chiu].

Risen, J. (1997, June 6). Convicted CIA turncoat gets 23 ½ years in prison. *Los Angeles Times,* p. A16 [Nicholson].

Rivera, R. (2004, August 31). Guardsman Anderson accused of "betrayal" as court martial begins. *The Seattle Times,* pp. 3-4.

Rosenberg, C. (1998, October 22). Couple admit role in Cuban spy ring. *The Miami Herald,* p. 6 [Hernandez].

Rosenberg, C. (1999, August 16). Shadowing of Cubans a classic spy tale. *The Miami Herald,* pp. 9-10 [Red Avispa].

Rosenberg, C. (2007a, May 17). Lawyer: U.S. policy shielded list of captives. *The Miami Herald,* p. 2 [Diaz].

Rosenberg, C. (2007b, May 18). Navy lawyer guilty of spilling secrets. *The Miami Herald,* p, 4 [Diaz].

Rosenzweig, D. (2005, February 5). Judge urged to reverse decision ending FBI espionage case. *The Los Angeles Times,* p. 1 [Leung].

Ross, C.E. & Mirowsky, J. (1979, June). A comparison of life-event weighting schemes: Change, undesirability, and effect-proportional indices. *Journal of Health and Social Behavior, 20*(2), 166-177.

Ryan G. Anderson. (2004, June 10). *CI Centre*. Retrieved from http://www.cicentre.com/Documents/DOC_Ryan_Anderson.htm

Sanders, E. (2004, September 4). Guardsman given life in prison for trying to help Al Qaeda. *The New York Times*, p. A16 [Anderson].

Schmitt, R. (2003, January 27). Veteran's spy trial to begin. *The Los Angeles Times,* p. 5 [Regan].

Scofield, D. (2004). Commentary: South Korea's 'heroic' spy. *Asia Times*. Retrieved from http://www.atimes.com

Scutro, A. (2007, May 16). Navy lawyer says shared info wasn't secret. *Navy Times,* Retrieved from http://www.navytimes.com/news/2007/05/navy_guantanamo-trial [Diaz].

Shukovsky, P., & Heckman, C. (2004, February 13). Soldier accused of trying to aid al-Qaida. *The Seattle Post-Intelligencer,* p. 16 [Anderson].

Skolnik, S. (2000, April 14). Seaman admits stealing defense secrets. *Seattle Post-Intelligencer*, p. A1 [Smith].

Smith, J., & Hall, C. (1996, November 19). CIA officer charged with spying. *The Washington Post,* p. A1 [Nicholson].

Smith, J., & Thomas, P. (1996, February 24). FBI arrests ex-soldier as mysterious KGB spy in super secret NSA. *Washington Post,* p. A21 [Lipka].

Soldier guilty of trying to aid Al Qaida. (2004, September 3). *The New York Times*, p. A3 [Anderson].

Spy suspects were paid $2.5 million, U.S. says. (1994, March 1). *The New York Times,* p. A3 [Ames].

Stein, J. (1994, July 5). The mole's manual. *The New York Times,* p. 4 [Description of "Project Slammer"].

Suro, R., & Thomas, P. (1996, December 20). Pitts gave FBI opening to trace security breaches of '80s. *The Washington Post,* p. A18.

Taylor, G. (2003, October 3). Antispy controls at Guantanamo aided in arrests. *The Washington Times*, p. 6 [Mehalba].

13 years for attempt to sell CIA info. (2006, May 27). *United Press International* [Shaaban].

REFERENCES

Thomas, P., Ryan, J., & Date, J. (2007, March 7). Former Navy sailor charged with passing secrets to Al Qaeda. *ABCNews Internet Ventures.* Retrieved from http://www.abcnews.go.com [Abujihaad].

Tizon, T. (2004, February 23). Spy suspect was devoted to God, guns. *The Los Angeles Times,* p. 26 [Anderson].

Translator to remain in jail as judge considers evidence. (2003, October 15). *Cable News Network (CNN).* Retrieved from http://edition.cnn.com/2003/LAW/10/15/translator/hearing/index.html [Mehalba].

Treverton, G.F. (2005, February). Emerging threats to national security: Statement to the Permanent Select Committee on Intelligence, United States House of Representatives. Santa Monica, CA: Rand Corporation.

United States Attorney's Office of Maryland. (2006, March 30). Former Maryland NSA employee sentenced for wrongfully possessing classified information. Retrieved from http://USAOMD.BLOGSPOT.COM/2006_03_26_USAMD_ARCHIVE.HTML [Ford, Jr.].

United States Attorney's Office District of Connecticut. (2007, March 7). Former member of US Navy arrested in Arizona on terrorism and espionage charges. U.S. Department of Justice. [Abujihaad].

United States Attorney's Office Eastern District of New York. (2007, February 14). Press release: U.S. Army translator pleads guilty to unauthorized possession of classified documents concerning Iraqi insurgency [Nour].

United States Attorney's Office Southern District of Indiana. (2005, March 3). Press release: Local man charged with working with former Iraqi intelligence officers in the United States [Shaaban].

United States Attorney's Office Southern District of Indiana. (2006a, January 25). Press release: Local man convicted of working with former intelligence officers [Shaaban].

United States Attorney's Office Southern District of Indiana. (2006b, May 26). Press release: Central Indiana man sentenced for working with former Iraqi intelligence officers [Shaaban].

United States Department of the Navy General Court-Martial. (2007, April 23). Defense response to government motions in limine to exclude certain evidence, United States v. Matthew M. Diaz, LCDR, JAGC, USN.

United States District Court for the Central District of California. (2005, February). Grand Jury Indictment, United States of America v. Chi Mak, Rebecca Laiwah Chiu, Tai Wang Mak.

United States District Court for the District of Connecticut. (2007). Warrant for arrest, United States v. Hassan Abujihaad a/k/a "Paul R. Hall."

United States District Court Eastern District of New York. (2005). Complaint, United States of America v FNU LNU [Nour].

United States District Court for the Eastern District of Virginia. (1996). Criminal complaint, United States of America v. Earl Edwin Pitts.

United States District Court for the Eastern District of Virginia. (2002). Superseding indictment, United States of American v. Brian Patrick Regan.

United States District Court for the Eastern District of Virginia. (2005). Criminal complaint, United States of America v. Lawrence Anthony Franklin.

United States District Court for the Eastern District of Virginia. (2005). Superseding indictment, United States of America v. Lawrence Anthony Franklin.

United States District Court for the Eastern District of Virginia. (2006). Memorandum in support of motion to find defendant in material breach of plea agreement and to release the government from its plea obligations, United States of America v. Donald Willis Keyser.

United States District Court for the Eastern District of Virginia. (2006). Memorandum opinion, United States of America v. Steven J. Rosen and Keith Weissman.

United States Magistrate Judge. (1996). Affidavit in support of criminal complaint, arrest warrant, and search warrant [Nicholson].

United States Magistrate Judge. (2001). Affidavit in support of criminal complaint, arrest warrant, and search warrants [Montes].

U.S. soldier convicted as a spy in Gulf War. (1991, December 3). *The New York Times,* p. A7 [Sombolay].

Waldman, P., Seib, G., Markov, J., & Cooper, C. (2001, November 26). Sergeant served U.S. Army and bin Laden, showing failing in FBI's terror policing. *The Wall Street Journal*, pp. A1-3 [Mohamed].

Waterman, S. (2005, October 23). Linguist in Iraq accused of fraud. *The Washington Times*, p. 11 [Nour].

Weaver, J. (2005, August 11). Spy trial likely to start anew elsewhere. *The Miami Herald,* p. 3 [Red Avispa].

Weaver, J. (2007, February 28). FIU [Florida International University] couple heading to jail. *The Miami Herald*, p. 4 [Alvarezes].

Weiner, T. (1998a, April 4) C.I.A. charges dismissed spy yielded secrets. *The New York Times*, p. A9 [Groat].

Weiner, T. (1998b, April 12). A straight-arrow policeman turns loose cannon at C.I.A. *The New York Times,* p. A2 [Groat].

Weiner, T. (1998c, April 17). Bail is denied for former C.I.A. officer accused of being a spy. *The New York Times,* p. A4 [Groat].

Whelan, J. (2007, May 6). The plot to steal U.S. secrets for a foreign coup. *The Star-Ledger* [NJ], p. 1 [Aragoncillo].

White, J. (2007, February 15). Translator who faked identity pleads guilty to having secret data. *The Washington Post,* p. A3 [Nour].

White, J. (2007, March 8). Former sailor accused of providing data to terrorist web site. *The Washington Post,* p. A8 [Abujihaad].

Whitlock, C. (2005, August 8). Briton used internet as his bully pulpit. *The Washington Post,* p. A1 [Abujihaad].

Williams, C. (2005, September 5). Cuban spy case poses dilemma for U.S. *The Los Angeles Times*, p. 1 [Red Avispa].

Wilson, S. (1997, May 24). Ex-clerk at NSA is guilty of spying; Former soldier sold secret documents to Soviets in mid-1960s. *The Baltimore Sun,* p. 1B [Lipka].

Wiltrout, K. (2006, August 29). Navy lawyer once posted at Cuba base is charged. *The Norfolk Virginian-Pilot*, found at http://home.hamptonroads.com/stories [Diaz].

Wiltrout, K. (2007a, May 15). Navy lawyer admits revealing names of Gitmo detainees. *The Norfolk Virginian-Pilot,* p. 2 [Diaz].

Wiltrout, K. (2007b, May 18). Naval officer sentenced to six months in prison, discharge. *The Norfolk Virginian-Pilot,* p. 1 [Diaz].

Wiltrout, K. (2007c, May 19). Naval officer sentenced to six months in prison, discharge. *The Norfolk Virginian-Pilot,* p. 3 [Diaz].

Wood, S., & Fischer, L.F.(2002). *Cleared DoD employees at risk – Report 2: A study of barriers to seeking help.* Monterey, CA: Defense Personnel Security Research Center.

Wood, S., & Wiskoff, M.F. (1992). *Americans who spied against their country since World War II.* Monterey, CA: Defense Personnel Security Research Center.

Yanez, L. (2005, August 11). Group seeks release of 5 accused spies. *The Miami Herald,* p. B1 [Red Avispa].

APPENDIX A:

INDIVIDUALS IN THE PERSEREC ESPIONAGE DATABASE

Table A-1
Individuals in the PERSEREC Espionage Database

Surname	Given Name	Affiliation	Date Began[21]	Date of Arrest	Volunteer or Recruit	Recipient Country or Group
Abujihaad	Hassan	Navy	01/07/19	07/03/07	V	AL QAEDA
Ahadi	(pseudonym)	Civilian	67/00/00	69/0000	V	EGYPT
Allen	Michael Hahn	Civilian	86/00/00	86/12/04	V	PHILIPPINES
Alonso	Alejandro M.	Civilian	94/00/00	98/09/10	V	CUBA
Alvarez	Carlos	Civilian	77/00/00	06/01/09	R	CUBA
Alvarez	Elsa	Civilian	82/00/00	06/01/09	R	CUBA
Ames	Aldrich Hazen	Civilian	85/04/00	94/02/21	V	SOVIET UNION
Ames	Maria del Rosario	Civilian	92/00/00	94/02/21	R	SOVIET UNION
Anderson	Ryan Gilbert	Army	04/01/00	04/02/12	V	AL QAEDA
Anzalone	Charles Lee F.	Marine	90/11/00	91/02/13	V	SOVIET UNION
Aragoncillo	Leandro	Marine	00/08/00	05/09/10	R	PHILIPPINES
Baba	Stephen Anthony	Navy	81/09/01	81/10/09	V	SOUTH AFRICA
Barnett	David Henry	Civilian	76/10/00	80/03/18	V	SOVIET UNION
Baynes	Virginia Jean	Civilian	90/00/00	92/00/00	R	PHILIPPINES
Bell	William Holden	Civilian	78/10/00	81/06/24	R	POLAND
Boeckenhaupt	Herbert William	Air Force	65/06/00	66/10/24	V	SOVIET UNION
Boone	David Sheldon	Army	88/00/00	98/10/10	V	SOVIET UNION
Borger	Harold Noah	Civilian	59/10/00	61/03/03	R	EAST GERMANY
Boyce	Christopher John	Civilian	75/05/10	77/01/16	V	SOVIET UNION
Bronson	(pseudonym)	Air Force	77/10/00	78/00/00	V	SOVIET UNION
Brown	Joseph Garfield	Civilian	90/00/00	92/12/27	R	PHILIPPINES
Brown	Russell Paul	Navy	89/04/00	89/07/25	V	SOVIET UNION
Buchanan	Edward Owen	Air Force	85/05/06	85/05/17	V	EAST GERMANY
Butenko	John William	Civilian	63/04/21	63/10/29	R	SOVIET UNION
Carney	Jeffrey Martin	Air Force	83/04/00	91/04/22	V	EAST GERMANY
Cascio	Guiseppe	Air Force	52/00/00	52/09/21	V	NORTH KOREA
Cavanagh	Thomas Patrick	Civilian	84/12/00	84/12/18	V	SOVIET UNION
Charlton	John Douglas	Civilian	93/07/00	95/05/00	V	FRANCE
Chin	Larry Wu-Tai	Civilian	52/00/00	85/11/22	R	CHINA

[21] The "date began" field is coded by year, month, and then day. For 64 individuals of the 173 persons in the database (37%) the exact month and day the person began espionage-related activity is unknown, and for those persons only the year is recorded, with zeros for month and day. Activity is defined as some action, not simply thinking about or talking about doing something.

Surname	Given Name	Affiliation	Date Began[21]	Date of Arrest	Volunteer or Recruit	Recipient Country or Group
Chiu	Rebecca Laiwah	Civilian	83/00/00	05/10/28	R	CHINA
Clark	James	Civilian	76/00/00	97/10/04	R	EAST GERMANY
Conrad	Clyde Lee	Army	74/00/00	88/08/23	R	HUNGARY,CZECHOSLOVAKIA
Cooke	Christopher M.	Air Force	80/12/23	81/05/05	V	SOVIET UNION
Cordrey	Robert Ernest	Marine	84/04/12	84/05/16	V	SOVIET UNION
Davies, A.	Allen John	Civilian	86/09/22	86/10/27	V	SOVIET UNION
DeChamplain	Raymond George	Air Force	71/06/05	71/07/02	R	SOVIET UNION
Dedeyan	Sahag Katcher	Civilian	73/03/00	75/06/27	R	SOVIET UNION
Diaz	Matthew	Navy	05/01/15	07/01/08	V	USA
Dolce	Thomas Joseph	Civilian	79/00/00	88/04/16	V	SOUTH AFRICA
Drummond	Nelson C.	Navy	58/00/00	62/09/28	R	SOVIET UNION
Dubberstein	Waldo Herman	Civilian	77/00/00	79/0000	R	LIBYA
Dunlap	Jack Edward	Army	58/00/00	63/0000	V	SOVIET UNION
Ellis	Robert Wade	Navy	83/02/09	83/02/09	V	SOVIET UNION
Faget	Mariano	Civilian	99/00/00	00/02/17	R	CUBA
Ford, Jr.	Kenneth W.	Civilian	04/01/00	04/01/12	V	UNKNOWN
Franklin	Lawrence A.	Civilian	02/08/15	05/05/04	V	ISRAEL
French	George Holmes	Air Force	57/04/05	57/04/06	V	SOVIET UNION
Garcia	Wilfredo	Navy	85/00/00	87/00/00	R	PHILIPPINES
Gessner	George John	Army	60/12/07	61/01/00	V	SOVIET UNION
Gilbert	Otto Attila	Civilian	82/04/17	82/04/17	R	HUNGARY
Gowadia	Noshir	Civilian	99/12/12	05/10/25	V	CHINA, ISRAEL, GERMANY, SWITZERLAND, AUSTRIA and 3 others
Graf	Ronald Dean	Navy	89/00/00	89/03/03	V	UNKNOWN
Gregory	Jeffrey Eugene	Army	84/03/00	93/04/29	R	HUNGARY,CZECHOSLOVAKIA
Groat	Douglas	Civilian	97/03/24	98/04/01	V	UNKNOWN
Grunden	Oliver Everett	Air Force	73/09/28	73/11/02	V	SOVIET UNION
Guerrero	Antonio	Civilian	91/00/00	98/09/12	R	CUBA
Haeger	John Joseph	Navy	89/10/00	89/12/01	R	SOVIET UNION
Haguewood	Robert Dean	Navy	86/02/00	86/03/04	V	UNKNOWN
Hall	James William, III	Army	82/12/00	88/12/21	V	EAST GERMANY, SOVIET UNION
Hamilton	Frederick Christophe	Civilian	91/02/00	92/00/00	V	ECUADOR
Hamilton	Victor Norris	Civilian	62/00/00	63/0000	V	SOVIET UNION
Hanssen	Robert Philip	Civilian	79/00/00	01/02/18	V	SOVIET UNION
Harper	James Durward, Jr.	Civilian	75/00/00	83/10/15	R	POLAND

Surname	Given Name	Affiliation	Date Began[21]	Date of Arrest	Volunteer or Recruit	Recipient Country or Group
Harris	Ulysses Leonard	Army	67/02/08	67/08/25	V	SOVIET UNION
Hawkins	Stephen Dwayne	Navy	85/00/00	85/08/07	V	UNKNOWN
Helmich	Joseph George, Jr.	Army	63/00/00	81/07/15	V	SOVIET UNION
Hernandez	Linda	Civilian	94/00/00	98/09/10	R	CUBA
Hernandez	Nilo	Civilian	92/00/00	98/09/12	R	CUBA
Hoffman	Ronald Joshua	Civilian	86/09/09	90/06/15	V	JAPAN
Horton	Brian Patrick	Navy	82/06/00	82/09/30	V	SOVIET UNION
Howard	Edward Lee	Civilian	84/09/00	85/0000	V	SOVIET UNION
Humphrey	Ronald Louis	Civilian	76/00/00	78/01/31	V	VIETNAM
Irene	Dale Vern	Civilian	84/08/12	84/08/23	R	SOVIET UNION
Jeffries	Randy Miles	Civilian	85/12/14	85/12/20	V	SOVIET UNION
Jenott	Eric O.	Army	96/00/00	96/06/26	V	CHINA
Johnson	Robert Lee	Army	53/02/00	65/04/05	V	SOVIET UNION
Jones	Geneva	Civilian	91/00/00	93/08/03	V	LIBERIA
Kampiles	William Peter	Civilian	78/02/00	78/08/17	V	SOVIET UNION
Kauffman	Joseph Patrick	Air Force	60/09/00	61/12/00	R	EAST GERMANY
Keyser	Donald Willis	Civilian	95/00/00	04/09/15	R	TAIWAN
Kim	Robert Chaegon	Civilian	96/04/00	96/09/24	V	SOUTH KOREA
King	Donald Wayne	Navy	89/00/00	80/30/3	V	UNKNOWN
Koecher	Karel Frantisek	Civilian	73/02/00	84/11/27	R	CZECHOSLOVAKIA
Kota	Subrahmanyam	Civilian	85/00/00	95/10/18	R	SOVIET UNION
Kunkle	Craig Dee	Civilian	88/12/00	89/01/10	V	SOVIET UNION
Lalas	Steven J.	Army	77/00/00	93/05/03	9	GREECE
Ledbetter	Gary Lee	Navy	67/04/00	67/05/00	R	SOVIET UNION
Lee	Andrew Daulton	Civilian	75/05/18	77/01/17	V	SOVIET UNION
Lee	Peter H.	Civilian	85/00/00	97/00/00	V	CHINA
Lessenthien	Kurt G.	Navy	96/00/00	96/04/22	V	RUSSIA
Leung	Katrina M.	Civilian	90/04/00	03/04/09	R	CHINA
Lipka	Robert Stephan	Army	65/09/00	96/02/23	V	SOVIET UNION
Lonetree	Clayton John	Marine	84/00/00	86/12/00	R	SOVIET UNION
Madsen	Lee Eugene	Navy	79/07/26	79/08/14	V	UNKNOWN
Mak	Chi	Civilian	83/00/00	05/10/28	R	CHINA
Martin	William Hamilton	Civilian	60/08/00	61/0000	V	SOVIET UNION
Mehalba	Ahmed	Civilian	03/00/00	03/09/29	R	EGYPT
Miller	Richard William	Civilian	84/05/00	84/10/03	R	SOVIET UNION

Surname	Given Name	Affiliation	Date Began[21]	Date of Arrest	Volunteer or Recruit	Recipient Country or Group
Mintkenbaugh	James Allen	Army	53/06/00	65/04/05	R	SOVIET UNION
Mira	Francisco de Asis	Air Force	82/05/00	83/03/25	V	SOVIET UNION
Mitchell	Bernon Ferguson	Civilian	60/08/00	61/00/00	V	SOVIET UNION
Mohamed	Ali Abdelseoud	Army	86/00/00	98/09/10	V	AL QAEDA
Montaperto	Ronald N.	Civilian	83/00/00	04/02/04	R	CHINA
Montes	Ana Belen	Civilian	80/00/00	01/09/21	R	CUBA
Moore	Edwin Gibbons, II	Civilian	76/12/22	76/12/22	V	SOVIET UNION
Morison	Samuel Loring	Civilian	84/07/00	84/10/01	V	UNITED KINGDOM
Mortati	Thomas	Civilian	81/00/00	89/12/01	R	HUNGARY
Mueller	Gustav Adolph	Air Force	49/10/00	49/10/00	V	SOVIET UNION
Murphy	Michael Richard	Navy	81/06/00	81/00/00	V	SOVIET UNION
Nesbitt	Frank Arnold	Civilian	89/09/00	89/10/14	R	SOVIET UNION
Nicholson	Harold James	Civilian	94/06/27	96/11/16	V	SOVIET UNION
Nour	Almaliki	Civilian	03/00/00	06/10/00	V	IRAQ
Ott	Bruce Damian	Air Force	86/01/09	86/02/22	V	SOVIET UNION
Payne	Leslie Joseph	Army	74/00/00	74/10/00	V	EAST GERMANY
Pelton	Ronald William	Civilian	80/01/15	85/11/25	V	SOVIET UNION
Peri	Michael Anthony	Army	89/02/20	89/03/04	V	EAST GERMANY
Perkins	Walter Thomas	Air Force	68/12/00	71/10/21	R	SOVIET UNION
Petersen	Joseph Sidney, Jr.	Civilian	48/03/01	54/10/09	V	NETHERLANDS
Pickering	Jeffrey Loring	Navy	82/00/00	83/00/00	V	SOVIET UNION
Pitts	Earl Edwin	Civilian	87/07/00	96/12/18	V	SOVIET UNION
Pizzo	Francis Xavier II	Civilian	85/08/11	85/08/13	V	SOVIET UNION
Pollard	Anne Henderson	Civilian	85/11/00	85/11/22	R	ISRAEL, CHINA
Pollard	Jonathan Jay	Civilian	84/06/00	85/11/21	R	ISRAEL, CHINA
Ponger	Kurt Leopold	Civilian	49/06/15	53/01/14	R	SOVIET UNION
Ramsay	Roderick James	Army	83/09/00	90/06/07	R	HUNGARY,CZECHOSLOVAKIA
Rees	Norman john	Civilian	42/00/00	71/0000	V	SOVIET UNION
Regan	Brian Patrick	Air Force	99/00/00	01/08/21	V	LIBYA, IRAQ, CHINA
Rhodes	Roy Adair	Army	51/12/00	57/06/00	R	SOVIET UNION
Richardson	Daniel Walter	Army	88/01/00	88/01/14	V	SOVIET UNION
Rohrer	Glenn Roy	Army	58/00/00	65/0000	R	CZECHOSLOVAKIA
Rondeau	Jeffrey Stephen	Army	85/00/00	92/10/22	R	HUNGARY,CZECHOSLOVAKIA

Surname	Given Name	Affiliation	Date Began[21]	Date of Arrest	Volunteer or Recruit	Recipient Country or Group
Safford	Leonard Jenkins	Army	67/02/08	67/08/25	V	SOVIET UNION
Santos	Joseph	Civilian	94/00/00	98/09/10	R	CUBA
Sattler	James Frederick	Civilian	67/00/00	74/0000	R	EAST GERMANY
Scarbeck	Irvin Chambers	Civilian	60/12/22	61/06/13	R	POLAND
Schoof	Charles Edward	Navy	89/10/00	89/12/01	V	SOVIET UNION
Schuler	Ruby Louise	Civilian	79/05/01	83/0000	R	POLAND
Schwartz	Michael Stephen	Navy	92/11/00	96/00/00	9	SAUDI ARABIA
Scranage	Sharon Marie	Civilian	83/12/00	85/07/11	R	GHANA
Seldon	Phillip Tyler	Civilian	92/11/00	96/00/00	R	EL SALVADOR
Shaaban	Shaaban Hafed	Civilian	02/00/00	05/03/03	V	IRAQ
Slatten	Charles Dale	Army	84/02/00	84/04/14	V	SOVIET UNION
Slavens	Brian Everett	Marine	82/08/31	82/09/04	V	SOVIET UNION
Smith	Richard Craig	Civilian	81/00/00	84/05/04	V	SOVIET UNION
Smith	Timothy Steven	Civilian	00/04/07	00/04/07	V	UNKNOWN
Sombolay	Albert T.	Army	90/12/00	91/03/29	V	JORDAN, IRAQ
Souther	Glenn Michael	Civilian	80/00/00	86/0000	V	SOVIET UNION
Squillacote	Theresa M.	Civilian	80/00/00	97/10/07	R	EAST GERMANY
Stand	Kurt Allen	Civilian	72/00/00	97/10/04	R	EAST GERMANY
Szabo	Zoltan	Army	67/00/00	89/05/21	R	HUNGARY
Thompson	Robert Glenn	Air Force	57/06/00	65/00/00	V	SOVIET UNION
Tobias	Bruce Edward	Civilian	85/08/12	85/08/23	V	SOVIET UNION
Tobias	Michael Timothy	Navy	85/08/11	85/08/13	V	SOVIET UNION
Trofimoff	George	Civilian	69/00/00	00/06/14	R	SOVIET UNION
Tsou	Douglas S.	Civilian	86/03/00	88/02/09	V	TAIWAN
Tumanova	Svetlana	Civilian	78/00/00	87/09/28	R	SOVIET UNION
Verber	Otto	Civilian	49/06/15	53/01/14	R	SOVIET UNION
Walker	Arthur James	Civilian	81/00/00	85/05/29	R	SOVIET UNION
Walker	John Anthony, Jr.	Navy	68/01/00	85/05/20	V	SOVIET UNION
Walker	Michael Lance	Navy	83/09/00	85/05/22	R	SOVIET UNION
Walton	(pseudonym)	Air Force	64/00/00	72/0000	V	SOVIET UNION
Warren	Kelly Therese	Army	86/00/00	97/07/10	R	EAST GERMANY
Weinmann.	Ariel Jonathan	Navy	05/07/00	06/03/26	V	RUSSIA
Wesson	(pseudonym)	Air Force	60/00/00	63/0000	R	SOVIET UNION
Whalen	William Henry	Army	59/12/00	66/07/12	R	SOVIET UNION
Whitworth	Jerry Alfred	Navy	75/02/00	85/06/03	R	SOVIET UNION

APPENDIX A

Surname	Given Name	Affiliation	Date Began[21]	Date of Arrest	Volunteer or Recruit	Recipient Country or Group
Wilmoth	James Rodney	Navy	89/02/00	89/07/25	V	SOVIET UNION
Wine	Edward Hilledon	Navy	68/08/21	68/09/29	V	SOVIET UNION
Wold	Hans Palmer	Navy	83/05/00	83/07/21	V	SOVIET UNION
Wolf	Ronald Craig	Civilian	89/03/00	89/05/05	V	SOVIET UNION
Wolff	Jay Clyde	Civilian	84/12/15	84/12/15	V	UNKNOWN
Wood	James David	Air Force	73/03/07	73/07/21	V	SOVIET UNION
Yai	John Joungwoong	Civilian	97/12/00	03/02/04	9	NORTH KOREA

APPENDIX B:

A SELECTED LIST OF ESPIONAGE STATUES IN THE UNITED STATES CODE (USC) OR THE UNIFORM CODE OF MILITARY JUSTICE (UCMJ)

Title 18	USC	Chapter 90	Protection of trade secrets (Economic Espionage Act of 1996) Section 1831 Economic espionage Section 1832 Theft of trade secrets
Title 18	USC	641	Theft or conversion of government property
Title 18	USC	792	Harboring or concealing persons
Title 18	USC	793	Gathering, transmitting, or losing defense information
Title 18	USC	794	Gathering or delivering defense information to aid foreign government
Title 18	USC	795	Photographing and sketching defense installations
Title 18	USC	796	Use of aircraft for photographing defense installations
Title 18	USC	797	Publication and sale of photographs of defense installations
Title 18	USC	798	Disclosure of classified information
Title 18	USC	951	Agents of foreign governments
Title 18	USC	952	Diplomatic codes and correspondence
Title 18	USC	1030	Information retrieved by knowingly accessing a computer without or in excess of authorization; willful retention, communication, or transmission of same
Title 18	USC	1924	Unauthorized removal and retention of classified documents or materials
Title 28	USC	533	Espionage in U.S. diplomatic mission abroad
Title 35	USC	181	Disclosure of patents placed under security
Title 42	USC	2274	Communication of Restricted Data
Title 50	USC	402a	Coordination of counterintelligence activities
Title 50	USC	421	Protection of identities of certain U.S. undercover intelligence officers, agents, informants, and sources
Title 50	USC	783	Communication of classified information by government employees
UCMJ	Article 104		Aiding the enemy
UCMJ	Article 106a		Espionage