



# PERSEREC

---

Technical Report 17-10  
August 2017

## The Expanding Spectrum of Espionage by Americans, 1947 – 2015

Katherine L. Herbig, Ph.D.  
*Northrop Grumman Technology Services*



---

Approved for Public Distribution  
Defense Personnel and Security Research Center  
Office of People Analytics

NOTE: For correspondence about this report, please contact [PERSEREC@mail.mil](mailto:PERSEREC@mail.mil)



**Technical Report 17-10**

**August 2017**

**The Expanding Spectrum of Espionage by Americans, 1947 – 2015**

Katherine L. Herbig, Ph.D.—*Northrop Grumman Technology Services*

Released by – Eric L. Lang, Ph.D.

Defense Personnel and Security Research Center  
Office of People Analytics  
400 Gigling Rd.  
Seaside, CA 93955

NOTE: For correspondence about this report, please contact [PERSEREC@mail.mil](mailto:PERSEREC@mail.mil)



## REPORT DOCUMENTATION PAGE

<b>REPORT DOCUMENTATION PAGE</b>			<b>Form Approved OMB No. 0704-0188</b>		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>					
1. REPORT DATE:		2. REPORT TYPE Technical Report		3. DATES COVERED: Sept. 2014 – Mar. 2017	
4. The Expanding Spectrum of Espionage by Americans, 1947 – 2015		5a. CONTRACT NUMBER:			
		5b. GRANT NUMBER:			
		5c. PROGRAM ELEMENT NUMBER:			
6. AUTHOR(S): Katherine L. Herbig, Ph.D.		5d. PROJECT NUMBER:			
		5e. TASK NUMBER:			
		5f. WORK UNIT NUMBER:			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel and Security Research Center Defense Office of People Analytics 400 Gigling Road Seaside, CA 93955		8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC-TR-17-10			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITOR'S ACRONYM(S)			
		11. SPONSORING/MONITOR'S REPORT NUMBER(S):			
12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited					
13. SUPPLEMENTARY NOTES:					
<p>ABSTRACT: The report describes characteristics of 209 Americans who committed espionage-related offenses against the United States since 1947. Three cohorts are compared based on when the individual began espionage: 1947-1979, 1980-1989, and 1990-2015. Using data coded from open published sources, analyses are reported on personal attributes of persons across the three cohorts, the employment and levels of clearance, how they committed espionage, the consequences they suffered, and their motivations. The second part of the report explores each of the five types of espionage committed by the 209 persons under study. These include: classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. The statutes governing each type are discussed and compared. Classification of national security information is discussed as one element in espionage. In Part 3, revisions to the Espionage statutes are recommended in light of findings presented in the report.</p>					
14. SUBJECT TERMS:					
15. SECURITY CLASSIFICATION OF: UNCLASSIFIED			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 260	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-583-2846
Standard Form 298 (Rev. 8/98) Prescribed by ANSI td. Z39.18					



## PREFACE

The Defense Personnel and Security Research Center (PERSEREC) dates from 1986. It was founded because of the espionage of John Walker and his ring of spies. Part of a record year for spies in 1985, when eleven Americans were arrested for espionage, Walker's capture and the revelation that for 20 years he had betrayed the trust the U.S. Navy placed in him as a cryptographic radioman, provoked outrage. A commission to investigate security practices then formed under General Richard G. Stilwell. Among its recommendations for improvement was the creation of an organization to perform behavioral science research on personnel security policies and practices, so the Department of Defense (DoD) established PERSEREC a year later to ground those practices in objective research.

For 30 years, PERSEREC has been working to improve the effectiveness, efficiency, and fairness of the DoD personnel and industrial security systems. One consistent research focus has been the phenomenon of trust betrayal in crimes such as espionage. This report is the fourth in a series of unclassified reports on espionage based on information collected in a database maintained by PERSEREC.<sup>1</sup> Materials on espionage and espionage-related offenses, including attempted espionage, conspiracy to commit espionage, and theft or illegal collection of closely held national defense information with the intent to commit espionage, have been coded into the database. These reports are based on open sources in order to facilitate public access to them. A founding goal of PERSEREC's is to improve security education and awareness; broad public distribution of unclassified analytical products about espionage furthers that goal.

Eric L. Lang, Ph.D.  
Director

---

<sup>1</sup> The PERSEREC Espionage Database contains information that is designated For Official Use Only (FOUO) as well as personally identifiable information, and therefore the database itself is FOUO. The information used in this report is unclassified, and this report is unclassified.



## EXECUTIVE SUMMARY

This report is the fourth in the series on espionage by Americans that the Defense Personnel and Security Research Center (PERSEREC) began publishing in 1992. The current report updates the scope of earlier work by including recent cases, and it extends the scope by exploring related types of espionage in addition to the classic type. There are three parts to this report. Part 1 presents findings on characteristics of Americans who committed espionage-related offenses since 1947. The findings are based on analyses of data collected from open sources. Part 2 explores the five types of espionage committed by the 209 individuals in this study: classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. Each type is described by its legal bases; examples of cases and comparisons with the other types of espionage are provided. Part 3 of the report considers the impact of the context in which espionage takes place, and discusses two important developments: (1) information and communications technologies (ICT), and (2) globalization. Recommendations are offered for revisions of the Espionage Statutes in response to the acceleration in the changes of context for espionage.

Part 1 compares data across three cohorts of persons by when the individual began espionage: 1947-1979 (the early Cold War), 1980-1989 (the later Cold War), and 1990-2015 (the post-Soviet period). As the Cold War recedes in time, the recent cohort offers the most applicable data for the present. This executive summary focuses on findings for the recent cohort. Among the characteristics of the 67 Americans who committed espionage-related offenses since 1990, we find that

- They have usually been male and middle-aged. Half were married, half not.
- Reflecting changes in the population as a whole, they were more diverse in racial and ethnic composition and more highly educated than earlier cohorts.
- Three-quarters have been civil servants, one-quarter military, and compared to the previous two cohorts increasing proportions have been contractors, or have held jobs not related to espionage, and or have not held security clearances.
- Three-quarters succeeded in passing information, while one-quarter were intercepted before they could pass anything; 60% were volunteers, and 40% were recruited. Among recruits, 60% were recruited by a foreign intelligence service, 40% by family or friends; contacting a foreign embassy was the most common way to begin as a volunteer.
- Compared to earlier cohorts, in which the Soviet Union and Russia predominated as the recipient of American espionage, recent espionage-offenders have transmitted information to a greater variety of recipients.
- Sixty-eight percent received no payment. Shorter prison sentences than earlier cohorts have been the norm in the recent past.
- Money is the most common motive for committing espionage-related offenses, but it is less dominant than in the past, since in the recent cohort money was a

## EXECUTIVE SUMMARY

motive for 28%, down from 41% in the first and 45% in the second of the two earlier cohorts. Divided loyalties is the second most common motive at 22%. Disgruntlement and ingratiation are nearly tied for third place, and more people seek recognition as a motive for espionage.

The majority of these 209 individuals committed traditional, classic espionage, in which controlled national security information, usually classified, was transmitted to a foreign government. Classic espionage predominates in each cohort under study, but in the first cohort 94% committed classic espionage, in the second cohort it was 95%, while in the most recent cohort classic espionage declined to 78%. This reflects authorities' recent increasing treatment as espionage of the four additional types that are discussed in Part 2. They include (1) leaks; (2) acting as an agent of a foreign government; (3) violations of export control laws; and (4) economic espionage. Understanding all five types requires describing their backgrounds. Each of the four additional types is prosecuted under its own subset of statutes, which differs from those used in cases of classic espionage. The various types are usually handled by different agencies of the federal government. They also differ in how involved the information of private companies and corporations is alongside government agencies.

The five types of espionage are not mutually exclusive, and a person may be charged with and convicted of more than one type. The assumption that espionage consists simply of classic espionage should be reexamined in light of how these four additional crimes are similar to or even charged as identical to classic espionage. They also impose losses of national defense information, intellectual property, and advanced technologies that cause grave damage to the security and economy of the nation.

In the detailed discussions in Part 2 of each of the five types of espionage, four elements frame the analysis. First, the legal statutes that define the crimes are identified and described. Prosecutorial choices as to which statutes to use are considered, alternate statutes that have been used in similar circumstances are identified, and reasons for the choices suggested. Second, examples of individual cases of each type of espionage are presented: instructive cases where rich details have been published are developed into more substantial case studies. Third, issues resulting from classification of information are identified and discussed for each type if they apply. And fourth, the numbers of individuals among the 209 under study here are presented in tables for each of the five types, along with descriptive statistics to indicate trends over time.

Part 3 discusses these trends by recognizing two central dimensions of the current context: information and communications technology (ICT) and globalization. The ubiquitous use of ICT is shaping the context in which espionage takes place. Spies have moved with the times, and they employ all the technological sophistication and Internet advantages they can access. Implications from this changing context are discussed, including how American espionage-offenders gather, store, and

transmit intelligence to a foreign government in the ICT context, and how a foreign government may now steal controlled information directly across interconnected networks, threatening to make spies obsolete.

Globalization affects many dimensions of life, but is especially apparent in areas relevant to espionage, such as in political and military affairs, development of defense technologies, and international finance. It can influence the recruitment of spies and the likelihood that people will volunteer to commit espionage as part of a trend toward a global culture, with its easy international transmission of ideas, civic ideals, and loosening allegiances of citizenship.

This report concludes by recommending revisions of the Espionage statutes (Title 18 U.S.C. sections 792 through 798). Revision is needed in order to address the inconsistencies and ambiguities in them. Based on provisions enacted in 1917 and updated in 1950—before computers or networks were conceived—they are outdated. Three approaches to revision are outlined: (1) try to eliminate inconsistencies among the Espionage statutes themselves; (2) consider how to update the Espionage statutes to reflect the current context of cyber capabilities, the Internet, and globalization; and (3) consider how to reconcile the statutes that apply to all five types of espionage discussed in this report to reconcile inequities, eliminate gaps or overlaps between them, and create more consistency in the legal response to activities that are similar, even though they take place in different spheres.

In an appendix, this report examines how espionage fits into the broader study of insider threat, and it considers three insights from insider threat studies that may illuminate espionage: personal crises and triggers, indicators of insider threat, and analyzing organizational culture.



TABLE OF CONTENTS

**INTRODUCTION** \_\_\_\_\_ **1**

BACKGROUND \_\_\_\_\_ 1

ORGANIZATION OF THE REPORT \_\_\_\_\_ 4

**METHODOLOGY** \_\_\_\_\_ **7**

**PART 1 CHARACTERISTICS OF ESPIONAGE BY AMERICANS** \_\_\_\_\_ **8**

PERSONAL ATTRIBUTES \_\_\_\_\_ 9

EMPLOYMENT AND CLEARANCE \_\_\_\_\_ 14

    Espionage Offenders without Security Clearances \_\_\_\_\_ 16

ELEMENTS OF THE ACT OF ESPIONAGE \_\_\_\_\_ 29

    How Information Has Been Transmitted \_\_\_\_\_ 38

CONSEQUENCES OF ESPIONAGE \_\_\_\_\_ 41

MOTIVATIONS \_\_\_\_\_ 44

    Strong Motivations for Espionage \_\_\_\_\_ 44

    Motivations through Time \_\_\_\_\_ 47

    Examples of Spying for Money \_\_\_\_\_ 49

    Examples of Spying from Divided Loyalties \_\_\_\_\_ 54

    Ingratiation, Coercion, Thrills, and Recognition \_\_\_\_\_ 58

    Helping and Ingratiation \_\_\_\_\_ 59

**PART 2 TYPES OF ESPIONAGE BY AMERICANS** \_\_\_\_\_ **63**

FIVE TYPES OF ESPIONAGE \_\_\_\_\_ 64

ELEMENTS OF CLASSIC ESPIONAGE \_\_\_\_\_ 69

    Classification and Legal Dimensions of Classic Espionage \_\_\_\_\_ 76

LEAKS AS A TYPE OF ESPIONAGE \_\_\_\_\_ 83

    Shamai Leibowitz \_\_\_\_\_ 88

    Stephen Jin-Woo Kim \_\_\_\_\_ 89

    John Kiriakou \_\_\_\_\_ 91

    Donald Sachtleben \_\_\_\_\_ 94

    Bradley Manning \_\_\_\_\_ 96

    Matthew Diaz \_\_\_\_\_ 100

    Lawrence Franklin \_\_\_\_\_ 102

    Edward Snowden \_\_\_\_\_ 106

ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF  
ESPIONAGE \_\_\_\_\_ 110

    Individuals Charged as Agents of a Foreign Government \_\_\_\_\_ 112

    Classic Spies Who Were Also Convicted as Foreign Agents \_\_\_\_\_ 115

    Employees of Foreign Intelligence Services \_\_\_\_\_ 117

    Persons Not Convicted of Classic Espionage, but Convicted of Acting as  
    Agents of Foreign Governments, Solely or with Other Charges \_\_\_\_\_ 118

VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE \_\_\_\_\_ 128

    Three Export Control Statutes \_\_\_\_\_ 129

    Enforcement of Export Control \_\_\_\_\_ 132

ECONOMIC ESPIONAGE \_\_\_\_\_ 146

    Trade Secrets \_\_\_\_\_ 146

    The Economic Espionage Act of 1996 \_\_\_\_\_ 149

## TABLE OF CONTENTS

<b>PART 3 CONTEXT AND RECOMMENDATIONS</b>	<b>161</b>
CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE	162
Information and Communications Technology (ICT)	162
Globalization	170
IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES	175
Revise Title 18 U.S.C. sections 792 through 798	175
Revise Espionage-related Statutes to Reflect Cyber Capabilities, Globalization, and the Internet	178
Reconcile Statutes that Apply to the Five Types of Espionage	180
<b>REFERENCES</b>	<b>183</b>
<b>APPENDIX A : ESPIONAGE AS AN INSIDER THREAT</b>	<b>A-1</b>
<b>APPENDIX B : LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS</b>	<b>B-1</b>

### LIST OF TABLES

Table 1 Personal Attributes	9
Table 2 Employment and Clearance	14
Table 3 Miscellaneous Occupations of Espionage Offenders	16
Table 4 Espionage Offenders with No Security Clearance When Espionage Began	17
Table 5 Frequency of Methods of Access for Espionage Offenders with No Current Security Clearance	20
Table 6 Elements of the Act of Espionage	30
Table 7 What, How, and Where Information Was Transmitted	39
Table 8 Consequences of Espionage	41
Table 9 Strong Motivations for Espionage	45
Table 10 Motivations for Espionage through Time	48
Table 11 Divided Loyalties Motivation, Citizenship, and Foreign Preference	57
Table 12 Types of Espionage by Americans	67
Table 13 Percentages of Classic Espionage Cases	67
Table 14 Security Clearance Status at Start of Classic Espionage	77
Table 15 Leaks	87
Table 16 Individuals Convicted as Agents of a Foreign Government	113
Table 17 Individuals Convicted Both of Classic Espionage and as Agents of a Foreign Government	115
Table 18 Individuals Working for a Foreign Intelligence Service (FIS) and Convicted as Agents of a Foreign Government	117
Table 19 Individuals Not Convicted of Classic Espionage but Convicted as Agents of a Foreign Government	119
Table 20 Individuals Convicted of Export Control Violations	135
Table 21 Use of Information and Communications Technology by Decade Espionage Began	164

**LIST OF FIGURES**

Figure 1 Number of Attempts and Transmissions of Information to Recipients, by Region \_\_\_\_\_ 37

Figure 2 Sole, or Strong, Motivations \_\_\_\_\_ 47

Figure 3 All Motivations \_\_\_\_\_ 49

Figure 4 A Model of Espionage Elements Based on Classic Espionage \_\_\_\_\_ 66

Figure 5 Leaks in a Model of Espionage Elements \_\_\_\_\_ 83

Figure 6 Acting as an Agent of a Foreign Government in a Model of Espionage Elements \_\_\_\_\_ 127

Figure 7 Export Control Violations in a Model of Elements of Espionage \_\_\_\_ 133

Figure 8 Economic Espionage in a Model of Elements of Espionage \_\_\_\_\_ 160

**LIST OF TABLES IN APPENDICES**

Table A-1 Precipitating Personal Crises and Triggers as Contextual Factors in 209 Espionage-related Offenders \_\_\_\_\_ A-8

Table B-1 List of the 209 Individuals in this Study and Selected Characteristics \_\_\_\_\_ B-3

**LIST OF FIGURES IN APPENDICES**

Figure A-1 The Government Accountability Office’s Summary of Key Elements in Insider Threat Programs \_\_\_\_\_ A-6



## INTRODUCTION

This is the fourth technical report in the series on espionage published by the Defense Personnel Security and Research Center (PERSEREC). The reports have been based on a For Official Use Only (FOUO) database collected by PERSEREC for 30 years. In its approach, this report shares with the three earlier reports many of the database variables discussed, yet it also differs from them in that it reflects the concerns of this time, and thus it takes up the issues and challenges of the early 21<sup>st</sup> century.

### BACKGROUND

The first PERSEREC espionage report, published in 1992, looked at 117 American citizens who had committed espionage during the Cold War. In its findings were compared by trait. So, for example, the authors looked at civilian versus military spies, volunteers versus recruited spies, successful versus unsuccessful spies. They then applied these results to issues such as improving the personnel security system, the changing motivations for espionage, and explaining the sudden increase of espionage by Americans in the 1980s (Wood & Wiskoff, 1992).

The second report in the series was published a decade later, in 2002. By then the number of Americans convicted of espionage or espionage-related<sup>2</sup> offenses had grown to 150. The report followed the analytical scheme of the first by comparing across traits, but it discussed in some depth new issues that were shaping the context of espionage, including the history of Soviet espionage in the United States and the impact of the Soviet Union's collapse after 1991; shifting policies on the prosecution of espionage, technological advances that were reshaping information storage and communications, and globalization's effects on national allegiances (Herbig & Wiskoff, 2002).

The third PERSEREC report on espionage was published in 2008, when there were 173 Americans to consider. This report shifted the analytical focus from the traits of the earlier reports to emphasize changes over time. Instead of looking at the whole group of individuals by military versus civilian or volunteer versus recruited spy, the whole group was divided into three subgroups based on when the person began espionage, and all analyses were structured across the three subgroups. For example, the number of volunteers versus the number of recruits was compared across the three subgroups: those who began between 1947 and 1979 (the early Cold War), those who began between 1980 and 1989 (the later Cold War), and those who began between 1990 and 2015 (the post-Soviet period). Because so many Americans began attempting espionage during the 1980s—and demographically they were a distinctive cohort—the 1980s were called out separately.

---

<sup>2</sup> Espionage-related offenses are those that were not charged under the Espionage statutes but under related statutes that nonetheless punish crimes identical in important respects to espionage as defined in the Espionage statutes.

## INTRODUCTION

Comparing across subgroups produced findings about how traits among spies had changed over time, and so it helped to identify trends. Since the violent terrorist attacks of 9/11 shaped so many aspects of life in the United States, including espionage, this report highlighted the 11 persons who had then spied since 9/11 in short case studies. New issues discussed in the third report reflected 9/11's impact: the context of global terrorism, homegrown terrorists, the impact of terrorism on espionage; the application of the expanding capabilities of the Internet for espionage; and the strain placed on American espionage statutes by prosecuting non-state groups or their supporters using laws from 1917 (Herbig, 2008).

As of 2015, 209 American citizens were convicted of espionage or espionage-related crimes. While 36 individuals have been entered into the database since the third report was published in 2008, not all of those 36 began espionage or even were arrested between 2008 and 2015. Some earlier spies only came to light since 2008, such as Marta Velazquez; a few earlier spies have been added as materials became available. This fourth report follows the analytical conventions of the third in that it divides the whole group into three subgroups based on when they began espionage: between 1947 and 1979, between 1980 and 1989, and between 1990 and 2015. The goals of this report are to understand espionage by Americans, to discern changes over time, to explore the five types of espionage these individuals represent, and to suggest trends that may guide successful countermeasures.

Some issues raised in earlier reports have expanded or deepened since 2008; others are new. Domestic terrorist attacks or sabotage have come to be framed as "insider threats," reflecting the attacks on fellow U.S. citizens at Ft Hood, Texas, and the Washington Navy Yard; espionage is often folded in with other crimes by insiders into this more encompassing description. With the information the Internet provides us have also come attacks of enemies in cyberspace and an evolving sophistication of cyber espionage. Economic espionage, merely mentioned as a threat in 2008, has grown wildly and now among analysts challenges "classic" espionage (that is, seeking national defense information) as a serious threat to national security. The People's Republic of China continues to perfect its unique approach to espionage and continues to profit from it. And the phenomenon of leaks, that is, providing secrets to the press or the public who then provides them to everyone, has exploded onto the scene with the actions of Bradley (Chelsea) Manning and Edward Snowden and the unprecedented prosecution of leaks since 2009. These issues help form the current context for espionage that will be considered here.

The PERSEREC Espionage program has three elements. The PERSEREC Espionage Database (FOUO) currently holds electronic data on 209 individuals whose activities span the 67 years from 1947 to 2015. Secondly, PERSEREC has built a collection of files on each individual in the database from press accounts, scholarly articles, and books documenting these cases. Thirdly, PERSEREC publishes unclassified reports based on the database and files, which allows wider distribution of findings on American espionage to any government agency and to

the public interested in following specific cases or learning more about espionage in general.

The 209 individuals in the espionage database were convicted or initially 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, in a few cases, 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 improper 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). A noticeable trend in the prosecution of recent cases has been the increasing number 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 since 2001, twice as many individuals have been charged with acting as an agent of a foreign power as in any earlier decade.

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),

## INTRODUCTION

- (4) Individuals for whom clear evidence of actual or attempted espionage existed, 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.

## ORGANIZATION OF THE REPORT

This report is structured in three parts. Part 1, Characteristics of Espionage by Americans, reports findings based on analyses of 209 individuals who committed espionage-related crimes. Part 2, Types of Espionage, explores in detail the five types of espionage these 209 individuals committed, providing examples and analyses from data collected on them. The five types are classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. Part 3, Context and Recommendations, considers changes in the context of espionage, how those changes shape espionage, and how they require revisions in the statutes that govern it.

Part 1 first compares across time periods (1947-1979, 1980-1989, and 1990-2015) based on when people began espionage-related activities, and then explores selected traits and how they apply to contemporary issues. An assumption underlies the decision to focus 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 ways in which it was possible to commit espionage in 1955 differed quite dramatically from the ways espionage could be committed in 1985, and it was different again in 2015. On the other hand, basic elements of the crime of espionage persist across any period. The basic and necessary elements for committing espionage include opportunity, conception, motive, lack of internal constraints, and ineffective external constraints (Herbig, 1994). It is because such basic elements can be found in any act of espionage that one instance can be compared 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 the very real changes over time.

Two events mark 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 in slow-motion, from the fall of the Berlin Wall in November 1989 to the dissolution of the Soviet Union as a government in December 1991; here 1990 serves as the turning point within that time. The second event that marks an abrupt shift in context is the attacks on the World Trade Center and the Pentagon

by Al Qaeda on 9/11. Since then, implications from those attacks have been and still are unfolding.

Before the Soviet Union fell apart, it competed with the United States for more than four decades as our main Cold War adversary, and it was the foremost customer for espionage by Americans. 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 time periods studied here. After the 9/11 attacks focused the nation's attention on the growing threat from global terrorism, it became apparent that Islamic terrorists that were organized internationally in networked cells posed a new, transnational intelligence threat. It is a threat whose challenges can be quite different from the Cold War parameters of two competing superpowers. Changes since 9/11 in the context of espionage—in the collection of intelligence, the creation of new agencies to respond, and the new challenges from cyberspace—have reshaped the espionage game.

The individuals studied in this report are 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 issues and pressures in a given period may have had on the person's decision to spy, along with the personal context of what went into his or her decision at that time.

This report attempts to identify and highlight the counterintelligence implications of the cases of espionage discussed. If it was available, information was collected on personal traits that could serve as triggers for espionage, on personnel security concerns as defined by the Uniform Adjudicative Guidelines for access to classified information, on indicators that espionage was in progress such as unexplained affluence, and on details about motivations, methods of transmission, and how people were caught (Berger, 1997). Open sources are often deliberately vague about counterintelligence details and on the fine points of more obscure spies' lives, but all available open-source information was sought and collected to offer a starting point for counterintelligence analysis.

In the analyses in Part 1, results are usually first reported in tables. The text accompanying the tables draws attention to highlights of the results and does not try 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 collected in PEREREC's files of articles on individuals who committed espionage-related offenses. Most of the examples come from the third cohort, individuals who began their activities since 1990, and especially those who began since the last technical report was published in 2008. Persons in this most recent group are new to this series and have not been discussed before. Some of the examples have been developed into brief thumbnail sketches to illustrate a trait or to provide materials for increased public awareness of espionage.

## INTRODUCTION

Part 2 examines the five types of espionage that comprise the expanding spectrum of espionage by Americans: classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. Each type is discussed in terms of the statutes that apply to it, explored in terms of how it is similar to and different from the classic type, and illustrated with example cases. Each type is summarized using a common figure drawn from classic espionage to highlight commonalities among the types of espionage.

Part 3 describes the current context of espionage by Americans by focusing on two developments: information and communications technology (ICT) and globalization. These shape the environment in which spying takes place now. This section concludes by considering how, in light of the earlier sections on recent espionage, the Espionage statutes need to be revised. Three approaches to revision are suggested.

A discussion of how the study of espionage may be enriched by studying selected works on insider threat appears in Appendix A.

For a list of the names and selected characteristics of the 209 individuals included in this study, see Appendix B.

## 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 were consulted, such as Google Scholar and CIBCentre.com, an Internet application 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 could confirm what was known, but except for a proportion of information that had been designated FOUO, 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 people first got involved with espionage, how their careers as spies evolved, how they operated 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 coded Yes, No, or Unknown.<sup>3</sup>

Data were coded into variables in the database by several coders over time. A detailed codebook was used to guide decisions and judgments during the coding.

The 209 individuals discussed here constitute a very small number of instances of any phenomena on which to apply statistical analysis. Descriptive statistics, with a comparison of frequencies, are the simple analytical tools used here on such small numbers that do not support more sophisticated techniques. 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 209 represent the known instances described in open sources that meet the criteria for inclusion defined here.

---

<sup>3</sup> More details on the coding procedures and considerations in the PERSEREC Espionage Database can be found by consulting the second report (Herbig & Wiskoff, 2002).

---

---

**PART 1**

**CHARACTERISTICS OF ESPIONAGE BY AMERICANS**

---

---

## PERSONAL ATTRIBUTES

The first dimension to consider in how espionage by Americans may have changed over time since 1947 is the personal attributes of the individuals, their gender, race, age when they began espionage, level of education, marital status, and sexual orientation. Table 1 reports findings on these characteristics.

**Table 1**  
**Personal Attributes**

Characteristics	1947-1979		1980-1989		1990-2015	
	<i>n</i> =68	%	<i>n</i> =74	%	<i>n</i> =67	%
Gender						
Male	65	95	65	88	61	91
Female	3	5	9	12	6	9
Race/Ethnicity <sup>4</sup>						
White	58	85	60	81	37	55
Black	5	7	2	3	4	6
Arab	2	3	2	3	6	9
Asian	2	3	4	5	10	15
Hispanic	1	2	5	7	10	15
Native American	0	0	1	1	0	0
Age when espionage began						
Less than 20	3	4	7	10	0	0
20 to 29	23	34	34	46	11	16
30 to 39	26	38	15	20	22	33
40 or more	16	24	18	24	34	51
Education, in years <sup>5</sup>	<i>(n</i> =66)		<i>(n</i> =68)		<i>(n</i> =40)	
10 years	4	6	5	7	0	0
12 years	23	35	25	37	12	30
14 years	13	20	13	19	4	10
16 years	17	26	10	15	10	25
18 or more years	9	13	15	22	14	35
Marital status when espionage began <sup>6</sup>			<i>(n</i> =69)		<i>(n</i> =58)	

<sup>4</sup> These are categories based on descriptions from open sources. They do not reflect a person's self-identification and they do not use the latest categories from the U.S. Census. White, African-American or Black, Asian, and Native American are commonly used racial categories. Arab and Hispanic may be ethnic, cultural, or linguistic categories for people of various races. For a discussion of these issues, see Cohn & Caumont, 2016.

<sup>5</sup> There is more missing data for education than for many variables, especially in the third cohort, which makes conclusions about that cohort more tentative. Of the 27 persons in the third cohort whose level of education is unknown, 13 are naturalized citizens, who may have been educated abroad, and the difficulty in tracking that information may account for some of the missing education data.

## PERSONAL ATTRIBUTES

Characteristics	1947-1979		1980-1989		1990-2015	
Married	48	70	35	51	33	57
Single	16	24	26	38	16	28
Separated or divorced	4	6	8	11	9	15
Sexual orientation	<i>(n=61)</i>		<i>(n=55)</i>		<i>(n=57)</i>	
Heterosexual	57	93	53	96	56	98
Homosexual	4	7	2	4	1	2

American spies continue to be overwhelmingly male. In the recent cohort, 91% were men and 98% were heterosexual, but other personal attributes have changed with time. As the population of the United States has become more diverse, so have spies. Whites are no longer so predominate at 55% of the total; since 1990, American citizens of Arab background first appear as 9% of spies, and more Asians and Hispanics have attempted espionage. Asian Americans were 13% of the recent cohort and Hispanic Americans were 15%.

The 60% of recent spies for whom the level of education is known mirrors a trend in the general population toward more education. Recent spies appear to be better educated than the previous two cohorts, with 35% having education beyond high school and another 35% holding postgraduate degrees. By comparison in 2010, the most recent census data, in the general population of the United States, 89% of native-born citizens 25 years or older held a high school degree or higher including 28% with bachelor's degrees. Among the foreign-born naturalized citizens in 2010, 68% were high school graduates or higher, including 27% with bachelor's degrees (Grieco et al, 2012). The trend in Table 1 over the decades since the late 1940s show a rising level of education among spies, which was interrupted during the 1980s by an influx of young military wannabe spies who often were unsuccessful at espionage. Most of the wannabes were only high school graduates. The most recent cohort appears to be the best-educated yet.

Marital status echoes this pattern. The general trend in American society over the past 60 years has been toward more divorce. Divorce rates doubled among people over 35 between 1990 and 2008, although they leveled off during the same period among younger people (Kennedy & Ruggles, 2014). Spies reflect that trend, with a rising rate of divorce that was interrupted during the 1980s when there were more young and single military spies. In the earlier two cohorts 6% and 11% were divorced, while 15% of the recent group of spies was divorced.

Only 18 of 209 American spies across all three time periods were women. There were more women spies during the 1980s than in the earlier or more recent

---

<sup>6</sup> There is more missing data for marital status than for some variables, especially for the third cohort; for 9 of the 67 persons in the third cohort marital status is unknown. This makes conclusions about that cohort's marital status more tentative.

cohorts; from a peak of 12% female spies in the 1980s, the recent group has dropped to 9%. Espionage remains a man's crime. Like many crimes, espionage entails taking risks, and if we extrapolate from crime in general and other risky behaviors, we can expect that espionage would likewise have a skewed gender ratio. More men than women commit crimes of all kinds. More men than women engage in risk-taking, such as interpersonal violence, dangerous sexual behaviors, risky sports, gambling, or risky maneuvers on the highways that result in accidents (Harris, Jenkins, & Glaser, 2006; Heuer, Jr., 1992). Men are also typically placed in jobs that have access to information to commit espionage than are women. Four times as many men than women are in government and in military jobs that grant access to national defense information and to highly classified secrets; men have more opportunity to betray secrets (ClearanceJobs, 2012). More men than women are expert in computer hacking or cyber security, which gives them access to classified or sensitive electronic information (Landivar, 2013). More men than women are highly placed in corporations, where their access to corporate information means that economic espionage could be tempting and lucrative (Warner, 2014).

Marta Rita Velazquez, a successful female spy for decades for Cuba, was an exception to the preponderance of male spies. Her espionage only became publicly known in 2013, but by then she had been an agent and source for Cuba for 30 years. Her case is not well known because of the long hiatus in making its outlines public.

Starting in 1989, she worked as an attorney advisor for a series of government agencies, including the Department of Transportation (DOT), the U.S. Agency of International Development (USAID), and the Department of State (DoS). The Cuban Intelligence Service (CIS) had recruited Velazquez to be an agent in 1983, early in her graduate studies at the Johns Hopkins University School of Advanced International Studies. In 1984 she met Ana Belen Montes, who was studying there part time for an international career. They became friends, and Velazquez spotted, assessed, and recruited Montes for the CIS (United States District Court for the District of Columbia, 2004).

In March 1985, Velazquez and Montes traveled to Cuba for intelligence training. First they flew to Madrid, where they met Cuban agents and picked up false passports to use for a flight to Prague. More agents met them in Prague and provided two more false passports and clothing in which they flew to Cuba. It was illegal then for Americans to travel to Cuba under the embargo, requiring this subterfuge. The CIS training in Cuba covered communications using high-frequency radio broadcast encrypted messages, operational security measures, and practice polygraphs to inoculate the two agents against revealing themselves. They retraced their steps via Prague and Madrid using their false passports, and once back in the United States, took up careers as successful civil servants and Cuban spies. During the 1990s, Velazquez sent Top Secret information and the identities of at least two American intelligence agents to the CIS using her radio, and

## PERSONAL ATTRIBUTES

continued to spot potential agents (United States District Court for the District of Columbia, 2004).

Her real success as a spy, however, was in recruiting Montes, since Montes went on to become the top intelligence official on Cuba in the Defense Intelligence Agency (DIA). Her reports to Cuba over 17 years seriously damaged American intelligence. Montes was arrested on September 21, 2001 in a reaction rushed by the 9/11 attacks and concern that Montes would pass on plans for the American response. In March 2002, she pled guilty to espionage and, in a plea bargain, began to cooperate with authorities. Three months later Velazquez resigned her government position in the U.S. Embassy in Guatemala and abruptly moved to Sweden, where she continues to live secure from extradition. The Federal Bureau of Investigation (FBI) learned of Velazquez from Montes in its debriefings of her in 2002 and Velazquez was indicted in 2004, but the FBI only notified her that she is under suspicion of espionage in 2010, and publicly unsealed her indictment in April 2013 (United States District Court for the District of Columbia, 2004; Venteicher, 2013; Popkin, 2013).

Recently, American spies have also been older when they began their espionage activities. In the first cohort that began spying between 1947 and 1979, 38% were under 29 years old, while in the second cohort with the influx of young military spies that began during the 1980s, 56% were under 29. The recent cohort that started between 1990 and 2013 shows decided aging: no one was under 20, only 16% were between 20 and 29, and over half were 40 or older.

Benjamin Pierce Bishop is an example of the greying American spy. He was 59 in June 2011 when he met a Chinese graduate student at an international defense conference in Hawaii. She was 27. They became friends, then lovers. She asked him for advice and sources for her research, and he began to bring classified documents home so he could review them before answering her questions. Eventually he emailed answers to her that included classified national defense information and orally discussed other issues with her, including details of a meeting classified Secret between the United States and South Korea, nuclear war plans and strategies, early warning radar systems, missile defense systems, and strategic resources and resource locations (United States Attorney's Office District of Hawaii, 2014).

Bishop had recently retired as a Lieutenant Colonel in the U.S. Army and was working as a contractor at the U.S. Pacific Command at Camp H.M. Smith on the island of Hawaii. He held a Top Secret SCI (TS-SCI) security clearance and served as a planner and specialist in cyber defense. His wife and daughter had remained in Utah while he worked on assignment in Hawaii, but in 2012 he asked for a divorce, explaining that he had met someone else. The requirements of his clearance specified that he disclose all of his contacts with foreign nationals and any travel he undertook that included such contacts; Bishop changed the name of

his lover on his disclosure forms to a masculine variation to hide their affair and her identity (Zimmerman, 2014).

He was arrested on March 15, 2013 and charged with two counts of espionage, willfully disclosing classified national defense information to someone not authorized to receive it and illegally retaining classified national defense information at home. He pled guilty and was sentenced on September 17, 2014, to 87 months (7 years and 3 months) in prison plus 3 years of supervised release (Former U.S. Officer, 2014). The press pronounced that Bishop had fallen into a “honey trap,” a snare set by a young woman seeking to lure an older man into a romance from which she could profit and use his access to classified information. The Chinese national was not charged and her name was not revealed by the prosecution. At his sentencing, Bishop’s lawyer blamed his reckless actions on love, saying “There was no intent to harm the United States. He made an error, a serious error in judgment for the love of a woman.” (Semko, 2013; Zimmerman, 2014).

In general, recent persons convicted of espionage-related offenses have been male, middle-aged, well-educated, and of a variety of racial and ethnic backgrounds that mirrors the increasing level of education and diversity of American society.

## EMPLOYMENT AND CLEARANCE

### EMPLOYMENT AND CLEARANCE

The jobs individuals perform and the level of security clearance they hold in those jobs largely determine whether they will have the opportunity to commit espionage. Table 2 reports trends across the three cohorts in the proportions of civil servants, contractors, and uniformed military, ranks of military, types and fields of employment, and levels of security clearance.

**Table 2**  
**Employment and Clearance**

Characteristics	1947-1979		1980-1989		1990-2015	
	<i>n</i> =68	%	<i>n</i> =74	%	<i>n</i> =67	%
Civilian or uniformed military						
Civilian (civil servants and contractors)	34	50	39	53	51	76
Uniformed military	34	50	35	47	16	24
Rank of uniformed military						
E1 – E3	3	9	10	28	3	19
E4 – E6	16	47	18	51	4	25
E7 - WO	10	29	3	9	3	19
Officer	4	12	2	6	4	25
Unknown	1	3	2	6	2	12
Type of employment during espionage						
Uniformed military	34	50	35	47	16	24
Civil servant	15	22	16	22	15	22
Government contractor	8	12	8	11	14	21
Job unrelated to espionage	11	16	15	20	20	30
Unknown	0		0		2	3
Occupational field when espionage began						
Communications/intelligence	25	37	23	31	12	18
General/technical	10	15	22	30	11	16
Scientific/professional	18	26	12	16	18	27
Functional support/administrative	12	18	10	14	9	14
Miscellaneous	3	4	7	9	17	25
Security clearance when espionage began						
Top secret SCI	10	15	11	15	14	21
Top secret	28	41	20	27	12	18
Secret	12	18	16	22	11	17
Confidential	1	1	3	4	0	0
None held during espionage	12	18	21	28	29	43
Unknown	5	7	3	4	1	1

Table 2 shows us that occupations we would expect to present opportunities to commit espionage, such as communications and intelligence, actually declined by half after 1990, from 37% and 31% in the two earlier cohorts to 18% in the most recent one. The number of spies in functional support or administrative occupations stayed about the same across time, while the influx of young military spies in the 1980s caused the proportion of general or technical occupations to spike up for the second cohort. The proportion of scientific or professional occupations decreased in the 1980s, and then returned to 27% of the total, to a level similar to the first cohort.

In the recent past, espionage has become a crime of civilians. The proportion of civilians increased from half uniformed military and half civilian in the first cohort, and from almost half and half during the 1980s, to 76% civilian in the most recent cohort. Among the uniformed military, there was also a shift in the recent past toward equal opportunity across ranks. From a predominance of the lower enlisted ranks in the first two cohorts, the recent cohort has a higher proportion of senior enlisted and more officers at 25%.

The greater proportion of civilians coincides with two other trends in the type of occupations held during espionage. One is an increase in the number of spies who were government contractors: from 12% and 11% contractors in the first two cohorts, the proportion of recent spies since 1990 has doubled to 21% contractors. This increase likely reflects the expanded hiring of contractors after 9/11 by the federal government responding to the terrorist threat, and the consequent increase in the proportion of clearances held by contractors in intelligence and defense roles (Sanger & Peters, 2013; Security from Within, 2013).

The second related trend is an increase in the number of spies in jobs apparently unrelated to espionage; there has been a doubling in frequencies between the first cohort and the third. This is reflected in a notable increase in spies with miscellaneous occupations that would seem to have little to do with espionage and, on the surface, would not provide an opportunity to commit such a crime. From 4% and 9% in the two earlier cohorts, miscellaneous types of employment increased among recent spies to one-fourth of the total, 25%. Table 3 lists the miscellaneous occupations in the three cohorts.

## EMPLOYMENT AND CLEARANCE

**Table 3**  
**Miscellaneous Occupations of Espionage Offenders**

1947-1979	1980-1989	1990-2015
1. unemployed	1. unemployed	1. boat pilot
2. drug dealer	2. public relations	2. housewife and student
3. retired	3. shoe salesman	3. Taekwondo instructor
		4. retired
		5. housewife and mother
		6. go-between, entrepreneur and organizer
		7. truck driver
		8. shop owner
		9. Chinese furniture importer
		10. pizza parlor clerk
		11. laborer and escort
		12. trader and importer of Middle Eastern foodstuffs
		13. airline gate agent
		14. unemployed broker of military equipment
		15. car dealer
		16. supervisor at aluminum door and window frame company
		17. menial jobs allowing observation of military installations

Changes in the level of security clearance held by espionage-related offenders show a trend toward unclassified but sensitive information. (These data are reported in Table 2.) Persons with a clearance level of TS-SCI comprised 15% in the first two cohorts, and this increased slightly to 21% in the recent cohort. The proportion of those holding TS level clearances declined with each cohort: from 41% to 27% to 18% in the most recent cohort. Secret level clearances remained similar across time at 18%, 22%, and 17%. There were few Confidential clearances among espionage offenders, and this disused clearance level disappears from the recent cohort. However, the proportion of persons who held no security clearance while committing an espionage-related offense increased over time from 18% to 28% to 43% in the recent cohort, approaching half of the total.

### **Espionage Offenders without Security Clearances**

The expectation about spies is that they have betrayed classified information. This is not consistently the case. Table 4 lists by name the 62 espionage-related offenders who did not hold security clearances or have access to classified information when they began committing an espionage-related offense. It also reports the methods they used to access information or the type of information they offered, and the outcome or sentence the person received.

**Table 4**  
**Espionage Offenders with No Security Clearance When Espionage Began**

<b>Decade Began Espionage</b>	<b>Name</b>	<b>Method of Access or Type of Information in the Case</b>	<b>Outcome or Sentence</b>
1940s	Rees, Norman	Passed unclassified information <sup>7</sup>	Suicide
1950s	Borger, Harold	Had accomplice with classified access	2.5 years in prison
	Cascio, Guiseppe	Had accomplice with classified access	20 years in prison
1960s	Harris, Ulysses	Had accomplice with classified access	7 years in prison
	Sattler, James	Passed unclassified information	Defection
1970s	Lee, Andrew	Had accomplice with classified access	Life in prison
	Harper, James	Had accomplice with classified access	Life in prison
	Clark, James	Had accomplice with classified access	12 years 8 months in prison
	Stand, Kurt	Had accomplice with classified 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 of probation
	Barnett, David	Relied on his 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 of probation
	Wilmoth, James	Had accomplice with classified access	35 years in prison, reduced to 15 years
	Wolff, Jay	Stole classified information	5 years in prison
	Davies, Allen	Relied on his memory of classified information	5 years in prison
	Slavens, Brian	Relied on his memory of classified information	2 years in prison

<sup>7</sup> It is not necessary to transmit classified information to be convicted of espionage under Espionage statutes. The main Espionage statutes (Title 18 U.S.C sections 792-798) were passed in 1917 and do not mention classification, which was not applied until 1940, and there are numerous other statutes often applied to espionage-related crimes that also do not require information to be classified. These issues are discussed in detail later.

## EMPLOYMENT AND CLEARANCE

<b>Decade Began Espionage</b>	<b>Name</b>	<b>Method of Access or Type of Information in the Case</b>	<b>Outcome or Sentence</b>
	Howard, Edward	Relied on his memory of classified information	Defection
	Smith, Richard	Relied on his memory of classified information	Released
	Pelton, Ronald	Relied on his memory of classified information	Life in prison
	Buchanan, Edward	Claimed access to classified information	2 years and 6 months in prison
	Irene, Dale	Had accomplice with classified access	2 years in prison
	King, Donald	Had accomplice with classified access	30 years in prison
	Tobias, Bruce	Had accomplice with classified access	5 months in prison
	Chiu, Rebecca	Had accomplice with classified access	3 years in prison, renounce U.S. citizenship and deportation
	Pizzo, Francis	Had accomplice with classified access	10 years in prison
	Pollard, Anne	Had accomplice with classified access	5 years in prison
	Mortati, Thomas	Had accomplice with classified access	1 year and 8 months in prison
	Alvarez, Elsa	Passed unclassified information	3 years in prison and 1 year of probation
	Ali, Amen	Had accomplice with classified access	5 years in prison and 3 year probation
	Myers, Gwendolyn	Had accomplice with classified access	7 years in prison and forfeiture of spouse's government salary and their sailboat
1990s	Ames, Rosario	Had accomplice with classified access	5 years in prison
	Brown, Joseph	Had accomplice with classified access	6 years in prison
	Leung, Katrina	Had accomplice with classified 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

**EMPLOYMENT AND CLEARANCE**

<b>Decade Began Espionage</b>	<b>Name</b>	<b>Method of Access or Type of Information in the Case</b>	<b>Outcome or Sentence</b>
	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 his memory of classified information	5 years in prison and 3 years of probation
	Sombolay, Albert	Passed restricted, but not classified information	34 years in prison
	Charlton, Jeffrey	Retained classified information to sell after he lost his access	2 years in prison, 5 years of probation, and \$50,000 fine
	Latchin, Sami	Passed unclassified information	4 years in prison
	Gari, George	Passed unclassified information	7 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
	Kuo, Tai-Shen	Has accomplice with classified access	15 years and 6 months in prison
	Nicholson, Nathaniel	Relied on accomplice's memory of classified information	5 years of probation and 100 hours of community service
	Roth, John	Passed restricted, but not classified information	4 years in prison and two years of probation
	Sherman, Daniel	Passed restricted, but not classified information	1 year and 2 months in prison
	Shemami, Najeb	Passed unclassified information	3 years and 10 months in prison
	Shu, Quan-Sheng	Passed restricted, but not classified information	4 years and 3 months in prison and \$387,000 fine
	Shriver, Glenn	Passed unclassified information	4 years in prison
	Knapp, Marc	Passed restricted, but not classified information	3 years and 10 months in prison
	Nozette, Stephen	Relied on his memory of classified information	13 years in prison

## EMPLOYMENT AND CLEARANCE

<b>Decade Began Espionage</b>	<b>Name</b>	<b>Method of Access or Type of Information in the Case</b>	<b>Outcome or Sentence</b>
	Soueid, M	Passed unclassified information	1 year and 6 months in prison
	Hoffman, II, Richard	Relied on his memory of classified information	30 years in prison
	Kiriakou, James	Relied on his memory of classified information	2 years and 6 months in prison
	Orr, Brian	Retained classified information to sell after he lost his access	3 years and 1 month in prison, 3 years of probation, and \$10,000 fine

There are eight methods of access listed in Table 4, two more than were reported in the 2008 version of this report. Table 5 summarizes the frequencies of these eight methods.

**Table 5**  
**Frequency of Methods of Access for Espionage Offenders with No Current Security Clearance**

<b>Method of Access or Type of Information in the Case</b>	<b>n=62</b>	<b>%</b>
Had accomplice with classified access	21	34
Passed unclassified information	16	26
Relied on memory of classified information	10	16
Stole classified information	5	8
Passed restricted, but unclassified information	5	8
Claimed access to classified information	2	3
Retained classified information to sell after losing access	2	3
Relied on accomplice's memory of classified information	1	2

The most frequent method of obtaining information for attempting espionage by persons who did not have access themselves was to rely on an accomplice who did have current access to classified information. More than one-third of offenders, 34%, were accomplices of someone with active access to classified information. One additional person served as an accomplice to someone who relied on his memories of past access in order to pass classified information.

For example, Gwendolyn Myers was an accomplice and active participant in the espionage career of her husband, Walter Kendall Myers. Starting in 1978, these two spied for Cuba for 30 years. They met in mid-life after matching failed marriages, a car accident in which Kendall Myers had killed a teenage girl, a disillusion with American politics, and a taste for radicalism that led them to grow marijuana in their basement and take illegal trips to Cuba. A Cuban intelligence official recruited them to serve as clandestine agents, and directed Kendall to seek employment in the Washington, DC, area that would provide classified access, such as at the CIA or the Department of State. Spying was to be a glorious adventure and a new joint

chapter in life for them to share. In 1985, he moved from contract teaching at the State Department and at Johns Hopkins School of Advanced International Studies—the same school Marta Velazquez and Ana Montes were then attending—to become a State Department professor and European analyst with Secret and later Top Secret clearances and SCI access. Gwendolyn worked in various jobs, at a bookstore and as an administrative assistant in a Washington, DC, bank, and never had classified access (Chaddock, 2009; Harnden, 2009).

The Myers spy team was discreet, careful, and effective as agents for Cuba for 3 decades. He would memorize information at work or take notes to bring home overnight. Occasionally he brought home classified documents, but would return them the next morning. Gwen would transcribe the notes or documents. They received encrypted radio broadcasts over a shortwave radio—the same model the Cubans also provided to Montes—with directions, codes, and requests from their handlers. The Myerses preferred to hand papers directly to Cuban agents. Gwen would leave papers in her shopping cart and exchange the cart with an agent in the local Giant supermarket, but over the years they also met Cubans in various foreign locations including Mexico, Trinidad and Tobago, Argentina, Brazil, Ecuador, and Jamaica. Later their handlers trained them in the sending and receiving of encrypted email from Internet cafes (United States District Court for the District of Columbia, 2009; Clark, 2010; Gentile, 2009).

The FBI began searching for a spy at State in 2006, and after Kendall made some intemperate public remarks that earned him criticism in the State Department, he retired under a cloud in 2007. Focusing on the Myerses first by monitoring their emails and phone calls, the FBI set up a sting in which an undercover agent posed as a Cuban sent to reengage the Myerses in more active espionage. “I was actually thinking it would be fun to get back in to it,” Kendall told the undercover agent in one of their meetings. Kendall and Gwendolyn Myers were arrested in June 4, 2009, and pled guilty in November of that year to acting as Cuban agents, conspiring to and actually collecting and transmitting national defense information to a foreign power, and wire fraud. Kendall was sentenced to life in prison without parole on July 16, 2010, and negotiated a lighter sentence for his wife in exchange for cooperating with extensive debriefings by the FBI. Gwendolyn received only 6 and ½ years in prison, minus the time served since their arrest, which reduced her sentence to 5 and ½ years. He was 73 and she was 72 when they entered prison (United States Department of Justice, 2010; Hsu, 2010).

The judge noted at their sentencing that the Myerses were unrepentant and seemed serenely resigned. Kendall came from wealth and status in American society: he was the great-grandson of Alexander Graham Bell, and had attended exclusive private schools all his life. The couple lived in a luxury co-op on Cathedral Avenue in Northwest Washington, DC. They could afford to buy a small yacht and learned to sail in hopes that someday they could sail it to Cuba. Early in their marriage, they fell in love with the Cuban revolution and with Fidel Castro. Castro granted them a personal audience with him in 1995 while they were visiting in Cuba, and

## EMPLOYMENT AND CLEARANCE

for one unforgettable evening they chatted with their hero and received a medal from him for their espionage. They took no payment for their activities, motivated by their ideological commitment to Communism and Castro, but also by the mutual adventure of being spies. “We share the ideals and dreams of the Cuban revolution,” they declared as they were sentenced to prison (Thompson, 2009; Harnden, 2009).

Nathaniel (Nathan) Nicholson is the one person who became an accomplice to espionage by relying on the memories of classified information recalled long after access had ended. This source was his father, Harold James (Jim) Nicholson. Jim Nicholson was already serving a prison sentence for his own espionage for the Soviets. He had been a career Central Intelligence Agency (CIA) officer starting in the 1980s; he became a station chief and a valued trainer of young CIA agents. Blaming a bitter and costly divorce, he began selling classified information to the Russians in June 1994, and continued until his unmasking and arrest in November 1996. He gave the Russians the names and assignments of all the CIA trainees he had ever worked with, compromising and endangering them. He did not pass a routine polygraph test in October 1995, which prompted surveillance and an investigation into his travel and finances (Joint CIA-FBI press release, 1996). Convicted of conspiracy to commit espionage in 1997, for which he received over \$300,000, Jim Nicholson began serving a 23 and ½ year prison sentence at the Federal Correctional Institution in Sheridan, Oregon, not far from where his three children were to live with his parents during his incarceration. His youngest son, Nathan, was 12. (United States Department of Justice, 2009).

Jim Nicholson did not give up. Though the authorities monitored his communications in prison, the FBI noted in 2002 that Nicholson was trying to manipulate fellow inmates into contacting the Russians for him. When Nathan returned to Portland from serving as a paratrooper in the Army Rangers in 2006 with an injury that put him out of the Army, Jim began grooming Nathan to be his go-between with the Russians. Jim claimed the Russians owed him a “pension” that they had promised him, and he wanted them to pay him before any information he still had in his head went stale (Lichtblau, 2009).

Nathan, then 22, visited his father regularly in prison during 2006, receiving training and advice on how to contact the Russians and establish a connection, how to travel to meeting places without attracting attention, how to carry cash payments into the country, and how to bank the money surreptitiously. Jim wrote out notes and questions for the Russians that Nathan smuggled out of the prison on crumpled paper. Nathan began a 2-year odyssey meeting Russian handlers in various world cities, including San Francisco, Mexico City, Lima, Peru, and Nicosia, Cyprus. The Russians proved interested in renewing this contact, and pressed Jim Nicholson for details from the mid-1990s about how he thought he might have been caught. They hoped to do their own damage assessment to find a possible mole in Russian intelligence that could have betrayed Nicholson. Jim passed on through Nathan details of his last months as a Russian agent, including his suspicion that a

## EMPLOYMENT AND CLEARANCE

contact in Malaysia had been tainted, the name of the CIA polygrapher who failed him, descriptions of federal agents who interrogated him after his arrest, concerns that he had been tailed while working as deputy station chief in Malaysia, and suspicion that his computer at the CIA training facility had been tapped (Denson, 2010).

Nathan collected \$47,000 in installments from the Russians, which at Jim's direction, he disbursed among his family members. Nathan was exhilarated by this secret adventure, but in fact it was no secret. The FBI got court approval to tap Nathan's cellphone, intercept his email, search and surveil his apartment, and track his vehicle. FBI agents followed him on all his travels and, when he returned from Cyprus, detained him while they searched his luggage and photocopied his spy notebook with the codes, addresses, questions, and notes he used, plus a \$7,000 payment hidden in a video game case (Pincus, 2010). Nathan was arrested in January 2009, pled guilty to acting as a foreign agent and to money laundering and, after his father also pled guilty so that his son would not have to testify against him, they appeared at a joint sentencing hearing in January 2011. Nathan was sentenced to 100 hours of community service with his fellow military veterans and 5 years of probation; Jim Nicholson received 8 years in prison added onto his existing sentence. He will be in his early 70's upon his release in 2024 from a federal prison in Terre Haute, IN, far from his family in Oregon (Pincus, 2010; Denson, 2011).

Gwendolyn Myers and Nathaniel Nicholson are examples of persons who became accomplices of other people who had active access to classified information or, in Nicholson's case, relied on the memories of another's past access. Combined, these two categories based on the role of accomplices account for 36% of methods used by persons with no clearance themselves, and makes being an accomplice the most frequent among non-clearance holders.

The second most frequent method of committing an espionage-related offense without having a security clearance is to pass unclassified information. This may seem counterintuitive: how does the transmittal of unclassified information result in an espionage-related conviction? Yet United States Espionage statutes do not consistently require the information involved in espionage to be classified. The laws have built on one another over time, becoming complex and contradictory. Early major statutes specify "national defense" information because they were written before classification was even developed early in the Second World War. Later statutes starting in 1950 do specify classified information (Edgar & Schmidt, Jr., 1973; Elsea, 2013). This and several other inconsistencies have led to ambiguity and variability in prosecutions and, some would argue, occasionally to unjust results.

John Joungwoong Yai is an example of someone who had no access to classified information himself, but who passed unclassified information to a foreign nation and was convicted of an espionage-related offense. A naturalized citizen since 1981,

## EMPLOYMENT AND CLEARANCE

Yai was a successful businessman who owned and operated various small businesses in Los Angeles. He was arrested early in 2003 after a 7-year FBI investigation that used wiretaps, electronic surveillance, and secret searches. For at least 3 years, Yai sent to his contact in North Korea publicly available information about trends in government intentions toward North Korea. He also plotted to get access to classified information for himself by getting a government job, and worked to plant other young Koreans in jobs that would have access to classified information so they could 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 at least \$18,000 for his efforts. He pled guilty to acting as an agent of a foreign power and to several counts of customs violations for his failure to declare his earnings over \$10,000 upon reentry into the United States after meetings with his handlers. Yai's wife, Susan Younja Yai, accompanied him on trips to meet with North Korean handlers; she received a year of probation and \$500 fine for her role. In February 2003, Yai was sentenced to 2 years in prison (Krikorian, 2003; Federal Bureau of Investigation, Affidavit, 2003; United States District Court for the Central District of California, Indictment, 2002).

The third-most frequent method of committing an espionage-related offense without having personal access to classified information was to rely on one's memory of classified information after losing access to it. Ten individuals called up information from their memories and sold or gave it to persons unauthorized to receive it. Robert Hoffman II is a recent example.

After 20 years in the U.S. Navy, Hoffman retired in November 2011 as a Petty Officer First Class (E-6) rated as a Cryptologic Technician-Technical. His work with electronic sensors used in submarine surveillance and tactical guidance to the sub's commander meant that he had held access to highly classified information while serving in the Navy. A few months before his retirement, he had treated himself to a fling by traveling to the Republic of Belarus, ostensibly in search of several Byelorussian women he had enjoyed meeting earlier during a port call in Bahrain. He posted descriptions of his 3-week trip on social media, including the unlikely boast that he had dropped in on the President of Belarus. The FBI began to follow this submariner with the highly classified access who traveled to a former Russian state and was not following security guidelines. A female undercover FBI agent answered Hoffman's Craigslist ad seeking companionship. She conducted a 5-month courtship over the Internet, and met him for several dates (United States Attorney's Office Eastern District of Virginia, 2014; Daugherty, 2013a; Daugherty, 2014).

Then the FBI raised the stakes and sent Hoffman a letter, apparently from "Vladimir" in Russia, inviting him to help with technical expertise for which he would be well compensated. Within hours Hoffman agreed to this proposal and volunteered his help. In his diary and later statements he said he needed money but that he also liked the thrills that espionage promised. Over several months, he

delivered three collections of classified information on thumb drives to a hollow at the base of a tree in nearby First Landings State Park in Virginia Beach, the dead drop site suggested by the FBI. The information Hoffman left in the tree covered naval capabilities and equipment, specific missions, and data about adversaries and intelligence. It would have allowed the Russians to track American submarines while avoiding detection. According to the Assistant U.S. Attorney speaking at Hoffman's trial, "He did not pass official government documents but instead created his own documents of secret information from memory (McGlone, 2012)." His FBI contacts arrested Hoffman early in December 2012. He was convicted of attempted espionage at trial in August 2013, and sentenced on February 10, 2014, to 30 years in prison (Federal Bureau of Investigation, 2014; Daugherty, 2013b).

Five of the persons convicted of espionage-related offenses who did not hold security clearances or access to classified information passed information or technology that was restricted because, as a military defense or dual military and commercial use, it was subject to export control laws. The DoS administers the United States Munitions List that details in 20 categories the technologies, equipment, and information that are restricted from export to foreign persons—that is, non-U.S. citizens. Export in this context includes the sharing of information (U.S. Code Title 22, chapter 39, §2778). Marc Knapp is a recent example of someone in this group who tried to export restricted military technology to a hostile foreign power now under a trade embargo, Iran.<sup>8</sup>

Starting in December 2009, for 7 months Knapp negotiated with a person he thought was a buyer for Iranians seeking restricted American military equipment and manuals that were export controlled. Knapp was a collector of military hardware, so he had connections into the world of buying and selling such articles, and since 2007 he had been unemployed after he lost his human resources job at a biotechnology company (Associated Press, 2011; O'Sullivan, 2011). He needed money. An acquaintance of Knapp's, who was already being investigated for illegal technology export, pointed investigators to Knapp as one of the sources of the equipment he had sold, and cut a deal for a light sentence for himself in exchange for cooperating with them against Knapp. The buyer was actually an undercover agent from the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (Department of Justice, 2011).

Knapp promised the undercover agent he could deliver multiple anti-gravity flight suits, an F-14 NATOPS emergency procedures manual for use in flight emergencies

---

<sup>8</sup> Knapp was charged with one count of violating the International Emergency Economic Powers Act, Title 50, United States Code, Sections 1702 and 1705(c), and Executive Order 13222, and Title 31, Code of Federal Regulations, Sections 560.204-560.205, and one count of violating the Arms Export Control Act, Title 22, United States Code, Sections 2778(b)(2) and 2778(c), and Title 22, Code of Federal Regulations, Sections 121.1, 123.1, and 127.1. Punishments for violating arms control export laws can be harsh: Knapp faced a possible maximum statutory sentence of 30 years' incarceration, followed by 3 years supervised release, a \$2,000,000 fine, forfeiture, and a \$200 mandatory special assessment.

## EMPLOYMENT AND CLEARANCE

in various U.S. military aircraft, multiple electronic versions of this manual, four AN/PRC-149 survival radios—which were hand-held search and rescue radios typically used by U.S. Navy pilots as emergency locator beacons, two F-14 aircraft pilot ejection seats and, most dramatically, an F-5B Tiger II fighter jet aircraft offered at \$3.25 million (Department of Justice, 2011). The agent documented Knapp explaining to him that prohibited customers for such sensitive U.S. military hardware, including Iran and, he hoped, China and Russia, could benefit by reverse engineering these technologies, or they could choose to “just listen in” to emergency beacon signals coming from downed American pilots (Immigration and Customs Enforcement, 2011). He saw himself “leveling the playing field” for his customers vis-a-vis the more advanced position of the United States (United States District Court for the District of Delaware, 2010).

Knapp insisted he and the agent use code words and false names to discuss their plans; he opened an offshore bank account to store his commission; he used only encrypted email. He grasped the complicated procedures and paperwork required to export something as sensitive and obvious as a jet fighter plane, and realized how to lie at the right places to proceed with it. He delivered several shipments of the smaller equipment to Hungary, his transshipment point to Iran; once on the ground in Hungary they were swiftly collected by ICE. Knapp was making his final arrangements to have the fighter jet flown to the east coast for crating when DHS arrested him on July 20, 2010. He pled guilty the following July and was sentenced in September 2011 to 46 months (3 years and 10 months) in prison (Immigration and Customs Enforcement, 2011).

Another five individuals without access to classified information themselves simply stole classified information. One of the “year of the spy” offenders from 1985, Randy Jeffries, took advantage of his employer’s lax security routines to take classified materials and try to sell them to the Soviets.

Jeffries worked as a messenger for the Acme Reporting Company in Washington, DC. Acme was a stenographic reporting service contracting with federal agencies and Congressional committees. Minutes, notes, documents, and testimony, all on paper and some of it classified Secret or Top Secret, would be picked up by messenger and brought to Acme to be transcribed, photocopied, and routed for publication or storage. Jeffries had worked in his low paid, routine job 2 months. He had no security clearance, since he was coming back from several years of drug rehabilitation after he lost an FBI clerk’s job, where he had held a clearance (Department of Defense Security Institute, 1990).

Instead, Jeffries set aside a stack of classified pages of testimony while he was working on destroying piles of papers by tearing them into four pieces and stuffing them into plastic bags and then into a dumpster available to all in an alley. (Part of the impact of this case came from learning about the egregious security environment the Acme Reporting Company had maintained by lying about its procedures as a cleared industrial security facility to Defense Investigative Service

## EMPLOYMENT AND CLEARANCE

(DIS) auditors. DIS revised its audit procedures as a result of these revelations.) Jeffries took a pile of classified pages home with him and called the Soviet Military Office saying he was coming to speak with them. The FBI noted his arrival and his visit, then a second visit, and they called Jeffries while they posed as Soviets offering to meet in a hotel to discuss an arrangement. Jeffries told the FBI undercover agents that he had already given over 40 pages of samples and had not yet been paid, and asked for \$5000. The FBI arrested him. He pled guilty to passing national defense information to a person not entitled to receive it and was sentenced in March 1986 to between 3 and 9 years in prison (Department of Defense Security Institute, 1990; Dolan, 1986).

The last two of the eight categories of persons convicted of espionage-related offenses without holding a security clearance or access to classified information each have only two instances.

Edward Buchanan and Shabaan Shabaan claimed to potential buyers of information that they had access to classified information that they wished to sell, but in fact neither one did. While still a student in Air Force training in 1985, Buchanan offered the East Germans and the Soviets classified information for sale. Air Force Office of Special Investigations agents conducted a sting, and learned that as a student Buchanan had no classified documents, but he did have plans to commit espionage as soon as his TS-SCI clearance, then in process, came through. He was court-martialed and sentenced to 30 months of confinement (Crawford, 1998).

Shabaan, a naturalized U.S citizen originally from Palestine, traveled to Iraq before the U.S. invasion there in 2003 and offered to provide Iraqi intelligence with the names of all the American spies operating in Iraq, which he falsely claimed he could procure from his classified sources. He also offered them a band of sympathizers he claimed he could organize as human shields against the coming invaders (Federal Bureau of Investigation, 2006). He was convicted at trial of acting as an agent of a foreign power without notifying the U.S Attorney General as required by law, violating the economic sanctions against Iraq, fraudulently procuring U.S. citizenship, and tampering with a witness (he threatened to behead the person, his brother). In May 2006, Shabaan was sentenced to 160 months (13 years and 4 months) in prison (United States Department of Justice Southern District of Indiana, 2006; Corcoran, 2006).

Jeffrey Charlton and Brian Orr worked in jobs that required access to classified information and they held security clearances, but each saw they would be losing that access. They put aside classified documents to save for sale later after they lost their access, and when they did lose it, they made offers to sell their stockpiled documents.

Charlton was an engineer at Lockheed Corporation in the 1980s and retired early in 1989, but he was disgruntled over the retirement terms offered and took with him a

## EMPLOYMENT AND CLEARANCE

cache of classified documents relating to U.S. Navy stealth and anti-submarine programs. In an FBI sting, on five occasions Charlton offered to sell these for \$100,000. He was arrested, pled guilty, and was sentenced in April 1996 in 2 years in prison, 5 years of supervised release, and fined \$50,000 (Chu, 1996). Brian Scott Orr worked as a civilian computer engineer at the U.S. Air Force Research Laboratory in Rome, NY, between 2009 and 2011. He held Top Secret clearances in order to work on the Air Force Satellite Control Network, the computer network that controls military satellites. Orr's access was withdrawn in 2011 and he reacted by retiring, taking with him training course materials for the computer network, and sensitive technical data that could have allowed someone to seriously disrupt or destroy the military satellite system. Orr negotiated a deal with an FBI undercover agent that he thought was a representative of the People's Republic of China, and sold him two thumb drives' worth of data for \$5000. He was arrested and pled guilty in a plea bargain in March 2014 to retention of stolen government property. He was sentenced in September 2014 to 37 months in prison (3 years and 1 month), 3 years of supervised release, and fined \$10,000 (Federal Bureau of Investigation Los Angeles Division, 2014).

The proportion of espionage-related offenders who did not hold current security clearances increased to almost half of the recent cohort—44%—in part because the variety of available espionage activities is proliferating.<sup>9</sup> It is more inaccurate than ever to assume that espionage-related offenses have been or only can be committed by security clearance holders, or that the information at issue would necessarily have been classified. The examples underline 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 because they relied on accomplices, memory, theft, lies, or retention to collect and transmit classified information. The examples also illustrate that it is quite possible to be convicted of espionage-related offenses for collecting and passing unclassified information. As illustrated in the Shemami and Soueid cases, foreign agents are recruited and sustained in the United States by countries interested in surreptitiously collecting publicly available information and spying on immigrant communities. As observers have noted, the scattered and partially overlapping and contradictory statutes governing espionage activities cry out for reorganization and revision by Congress itself or a Congressional commission (Epstein, 2007; Barandes, 2007).

---

<sup>7</sup> Beginning in the 2008 technical report in this series on espionage, espionage of types other than classic were discussed. For example, Ronald Hoffman's sale of dual-use technology produced under an Air Force contract was included. Since 2008, prosecutions for acting as an agent of a foreign government, for leaks of classified information to the press, for violations of export controls, and for economic espionage have all increased notably, and so there are a higher proportion of such cases included in the database in 2015.

## ELEMENTS OF THE ACT OF ESPIONAGE

Of the five sections in Part 1 of this study, four of them capture information about the 209 individuals themselves—their demographic characteristics, employment and clearance status, the consequences they suffered for their crimes, and their motivations. The focus of this section is different in that it reports details of what these individuals did to commit espionage and what kind of spies they were, i.e., did they volunteer, were they intercepted, and which country did they try to contact. By collecting data on basic dimensions of their acts of espionage, it may be possible to discern trends in how espionage has been conducted by Americans over time.

Table 6 presents some of the basic dimensions of espionage committed by the persons in the three cohorts used in this study, defined by when a person began to commit an espionage-related crime.

## ELEMENTS OF THE ACT OF ESPIONAGE

**Table 6**  
**Elements of the Act of Espionage**

Characteristics	1947-1979		1980-1989		1990-2015	
	<i>n</i> =68	%	<i>n</i> =74	%	<i>n</i> =67	%
Intercepted or passed information						
Intercepted	6	9	29	39	19	28
Passed information	62	91	45	61	48	72
Duration						
Intercepted	6	9	29	39	19	28
Less than 1 year	14	20	10	13	14	21
1 to 4.9 years	23	34	16	22	22	33
5 or more years	25	37	19	26	12	18
Volunteer or recruit	<i>n</i> =67				<i>n</i> =66	
Volunteer	34	51	47	64	39	59
Recruited	33	49	27	36	27	41
Recruited by	<i>n</i> =33		<i>n</i> =27		<i>n</i> =27	
Family	2	6	3	11	3	11
Foreign Intelligence	26	79	15	56	16	59
Friend	5	15	9	33	8	30
Method used to begin espionage	<i>n</i> =66		<i>n</i> =72		<i>n</i> =56	
Contact foreign agent	9	14	10	14	1	2
Contact foreign embassy	17	26	28	39	13	23
Go-between	5	7	3	4	1	2
Other methods	2	3	3	4	8	14
Internet	0	0	1	1	6	11
Recruited	33	50	27	38	27	48
Location where espionage began	<i>n</i> =66		<i>n</i> =73			
Outside U.S.	27	41	16	22	12	18
U.S. east coast	28	42	27	37	32	48
U.S. west coast	6	9	19	26	12	18
Other locations in U.S.	5	8	11	15	11	16
Location where espionage began outside the U.S.	<i>n</i> =27		<i>n</i> =16		<i>n</i> =12	
Western Europe	20	74	11	69	1	8
Asia and Southeast Asia	4	15	3	19	5	42
Eastern Bloc/Soviet Union	3	11	1	6	0	0
Africa	0	0	1	6	0	0
Middle East	0	0	0	0	3	25
Central and South America	0	0	0	0	3	25
Attempts and transmissions of information to recipients by region*	<i>n</i> =69**		<i>n</i> =80**		<i>n</i> =77**	
Western Europe	2	3	1	1	4	5
Soviet Union/Russia	42	61	39	49	9	12
Eastern Bloc	15	22	14	17	1	1

ELEMENTS OF THE ACT OF ESPIONAGE

Characteristics	1947-1979		1980-1989		1990-2015	
Asia and Southeast Asia	4	6	10	13	22	29
Africa	1	1	2	3	0	0
Middle East	3	5	3	4	15	20
Central or South America	1	1	5	6	11	14
Al Qaeda	0	0	1	1	4	5
USA (information revealed publicly)	0	0	0	0	7	9
Recipient unknown	1	1	5	6	4	5

\* For several individuals, it has not been revealed whether they contacted government officials or private businessmen in some of the countries they dealt with. In one instance, Noshir Gowadia, court documents show that he named multiple countries he had contacted and attempted or did pass information to, but the documents only list 6 countries by name, so 2 of the 4 attempts reported in the third cohort listed as “recipient unknown” are Gowadia’s.

\*\* Some individuals transmitted information to two or more recipients, so the number of instances of actual or attempted passing of information in this section of the table is greater than the number of individuals in each of the three groups.

Table 6 demonstrates that during the 3 decades of the first cohort of espionage offenders considered here, almost all—91%—transmitted information to a recipient. This success rate among American spies fell sharply during the 1980s when younger, enlisted military volunteers attempted and usually failed at espionage while trying to make themselves some money (Herbig, 2008). The recent cohort of offenders, acting since 1990, has passed their information more often than the second but less often than the first cohort. Seventy-two percent of espionage offenders since 1990 have transmitted information, less than the 91% of the first cohort, but more than the 61% of the second cohort.

The duration of espionage careers reinforces the finding that the 1980s were an anomaly in the patterns of American espionage. Looking at the first two categories, that is, intercepted before passing information and passing information for less than a year, shows that in the 1980s, 52% of American spies never got their spying started or were quickly caught. In the first cohort, less than one-third of offenders had such short careers. The most recent cohort shows fewer interceptions than during the 1980s (28% rather than 39%) but 21% offenders were quickly caught within 1 year.

The pattern for offenders who spied between 1 year and 4.9 years echoes the impact of the 1980s: one-third of the first cohort had these mid-length espionage careers, while only 22% of the 1980s cohort did so, and again one-third of the recent cohort spied between 1 year and 4.9 years.

In a heartening finding for counterespionage, the trend among long duration espionage careers is consistently downward. Among the first cohort, 37% spied for 5 or more years. In the second cohort this fell to 26%, and in the most recent cohort since 1990, long duration espionage is down to 18%, half that of the early cohort who spied between 1947 and 1979.

## ELEMENTS OF THE ACT OF ESPIONAGE

There have always been more volunteers to commit espionage than recruits among American spies, but the proportions have varied over time. The early cohort was roughly half volunteers and half recruits. During the 1980s, volunteers increased to 64% of the total. Fifty-nine percent of offenders since 1990 volunteered to commit espionage while 41% were recruited, making this cohort more volunteers than the first but less than the second cohort.

Recruitment of American spies by a foreign intelligence service predominated among recruits in the first cohort during the early Cold War, with 79% of those recruited, followed by 15% recruited by a friend and only 6% by a family member. This proportion changed during the 1980s and has remained so since 1990. In the second cohort, foreign intelligence services recruited 56% of recruits while the percentages recruited by family or friends each doubled when compared with the first group. The third cohort mirrors the second, with 59% recruited by a foreign intelligence service, 11% by a family member, and 30% by a friend.

Among the methods of first contact to a recipient typically used by volunteer American spies, contacting the potential recipient's embassy is the most common. One-quarter of offenders telephoned or walked into embassies to volunteer as spies in the first cohort, while 39% of volunteers in the 1980s approached an embassy as did one-fourth of volunteers in the most recent cohort, even though it has been widely reported in the press that the FBI watches the entrances of embassies that would be likely recipients of information, such as that of the Soviet Union, and also attempts to place taps on their telephones and communications. Despite this,

Another common method to try to begin espionage was contacting a foreign agent, which usually meant a nation's military intelligence officials or an attaché. A few offenders in each cohort worked through a go-between to an intelligence service.

As the Internet has become increasingly useful and convenient since 2000, more volunteer spies have turned to the Internet as a means to approach prospective recipients. In the most recent cohort since 1990, 8 individuals used the Internet to make contact with recipients. Paul Hall, who took the name Hassan Abujihad, is one example.

Paul Hall grew up in San Bernardino, CA, and joined the U.S. Navy in 1995 when he was 19. He converted to Islam, changed his name to Hassan Abujihad (Abujihad means "father of holy war" 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, having been honorably discharged, 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, Abujihad stood trial and on March 6 he was convicted on both charges ("Former sailor," 2008).

Abujihaad allegedly contacted the Azzam Publications website late in 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 the Islamist fighters in one of his videos, he wrote

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 [sic] 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 [from the attack on the *U.S.S. Cole*] taking a toll on junior and high ranking officers...[they were] running around like headless chickens very afraid (United States District Court for the District of Connecticut, Warrant, 2007).

Authorities stumbled on Abujihaad by following links from two other terrorism arrests. One link led to him from 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 Hartford, Connecticut, because that was where one of the website's Internet service providers was located. The two website owners fought extradition to the United States in the British courts starting in 2004 (Whitlock, 2005; Associated Press, 2012). Shortly before their arrest, a raid 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.<sup>10</sup> The material on the disk also pointed out vulnerabilities in the

---

<sup>10</sup> The case of Babar Ahmad, which is outside the scope of this study since Ahmad is a British citizen, nevertheless illustrates the potential for linkages between espionage and terrorism. 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 arrest in 2004, Ahmad worked from prison to publicize his plight and to advance the Islamist cause to a wider audience. Working with relatives and friends outside who put his material onto his new website, Ahmad argued that if he were extradited to Connecticut (because a server for his website had been located there), he would end up a casualty of the U.S. war on terror, and would be imprisoned in Guantanamo Bay. British public figures, antiwar activists, Muslim support groups, and entertainment notables came 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;

## ELEMENTS OF THE ACT OF ESPIONAGE

ships' defenses and the best locations from which to attack the fleet. Prosecutors alleged this classified information was sent by Abujihad, who held a Secret clearance, who was passing it along to his friends at Azzam Publications (United States District Court for the District of Connecticut, Warrant, 2007; United States Attorney's Office District of Connecticut, 2007).

The second link led to Abujihad from a terrorism arrest in the greater Chicago area. Abujihad 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 (White, 2007). While under arrest Shareef reported to investigators that 2 years earlier, his roommate, Abujihad, 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. This information, added to the evidence of the classified fleet transit plan and the emails that had been exchanged with Azzam personnel, led to Abujihad's arrest in Phoenix in March 2007. At the time, Abujihad was working for United Parcel Service as a deliveryman and supporting two small children (White, 2007).

Abujihad was convicted on March 6, 2008, of providing material support to terrorists and of disclosing classified information related to the national defense to those unauthorized to receive it. A year later, a judge granted a defense motion for his acquittal on the charge of providing material support to terrorists based on the judge's application of the law's language. On April 3, 2009, Abujihad was sentenced to 120 months (10 years) in prison on the remaining charge of disclosing classified information about the battle group plan of transit to the publishers at the Azzam website, Ahmad and Ahsan (U.S. Department of Justice Press Release, 2009; Mahony, 2009).

The remaining 6 persons in the most recent cohort used various methods to contact recipients, including meetings in person, sending offers through the mail, and in one instance, granting foreign nationals access to export-restricted materials in a

---

140,000 people signed another in 2012. In 2005, Ahmad ran for Parliament from his cell, garnering 2% of the vote in his district (Whitlock, 2005). He won £60,000 in damages for injuries he received from the police during their raid on his apartment and his initial arrest. Extradited to the United States in 2012, he pled guilty in December 2013 in a plea bargain to providing material support to terrorists, and was sentenced in July 2014 to 12 and ½ years in prison. Since he had already been held in 10 different jails and prisons either in the U.K. or in the U.S. for over 11 years, many in solitary confinement, he spent just another 13 months in prison and was released to return to the UK in July 2015. He maintains that although the classified battle plan was found in his apartment, he never did anything with it or passed it to anyone else (Kundnani & Theoharis, 2014; Ratcliffe, 2015).

## ELEMENTS OF THE ACT OF ESPIONAGE

laboratory working on U.S. Air Force weapons contract developing drones. John Reece Roth, a 72-year old emeritus physics professor at the University of Tennessee and expert in plasma technology, headed a lab researching plasma actuators for drones as a subcontractor for Atmospheric Glow Technology, Inc., the company that held the Air Force contract.

Despite being warned that he was violating the law, Roth insisted on including promising foreign graduate students, one from China and the other from Iran, on the research, even though the contract specified that any technology to be developed was export controlled and could not be shared with foreign nationals. Roth also sent documents based on the research via email to professional contacts in China, and took other documents with him to China to present their findings in person. He was charged with conspiring with the company to defraud the Air Force, 15 counts of violating the Arms Control Export Act, and one count of wire fraud. Convicted on all counts on September 3, 2008, Roth was sentenced in July, 2009, to 48 months in prison (4 years) followed by 2 years of supervised release (Satterfield, 2008; United States Department of Justice, 2008; United States Department of Justice, 2009).

Offenders in the first cohort in Table 6 were most likely to begin their espionage either overseas (41%) or on the East Coast of the United States, where government agencies and intelligence headquarters are concentrated. There has been a steady decline over time in the proportion of espionage cases begun overseas, such that in the recent cohort since 1990 only 18% began outside the United States, while roughly half originated on the East Coast. The remainder was divided between the West Coast and other U.S. locations.

Looking specifically at the small numbers of individuals who began espionage overseas and in what region of the world these persons were physically located when they first acted, there is a large shift between the first two cohorts and third cohort of offenders. In the first two cohorts, most overseas cases began in Western Europe, in the Eastern Bloc, or in Soviet Union. In a few cases, they began in Asia or Southeast Asia.<sup>11</sup> In the most recent cohort since 1990, only one case has been initiated in Western Europe, 5 have started in Asia or Southeast Asia, and 3 each have started in the Middle East or in Central or South America. Americans looking to commit espionage appear to have spread around the globe as customers for their information have expanded.

The shift in recipients of espionage-related offenses by Americans coincided with the collapse of the Soviet Union in 1991. Eighty-three percent of the attempts or actual transmissions by individuals in the early Cold War cohort went to the Soviet Union or to the Eastern Bloc countries, which sent them as a matter of course to

---

<sup>11</sup> This variable reports the location of initial contact, but not the nationality of the recipient; many instances that occurred in Western Europe were Americans interacting with Soviet or Eastern European contacts.

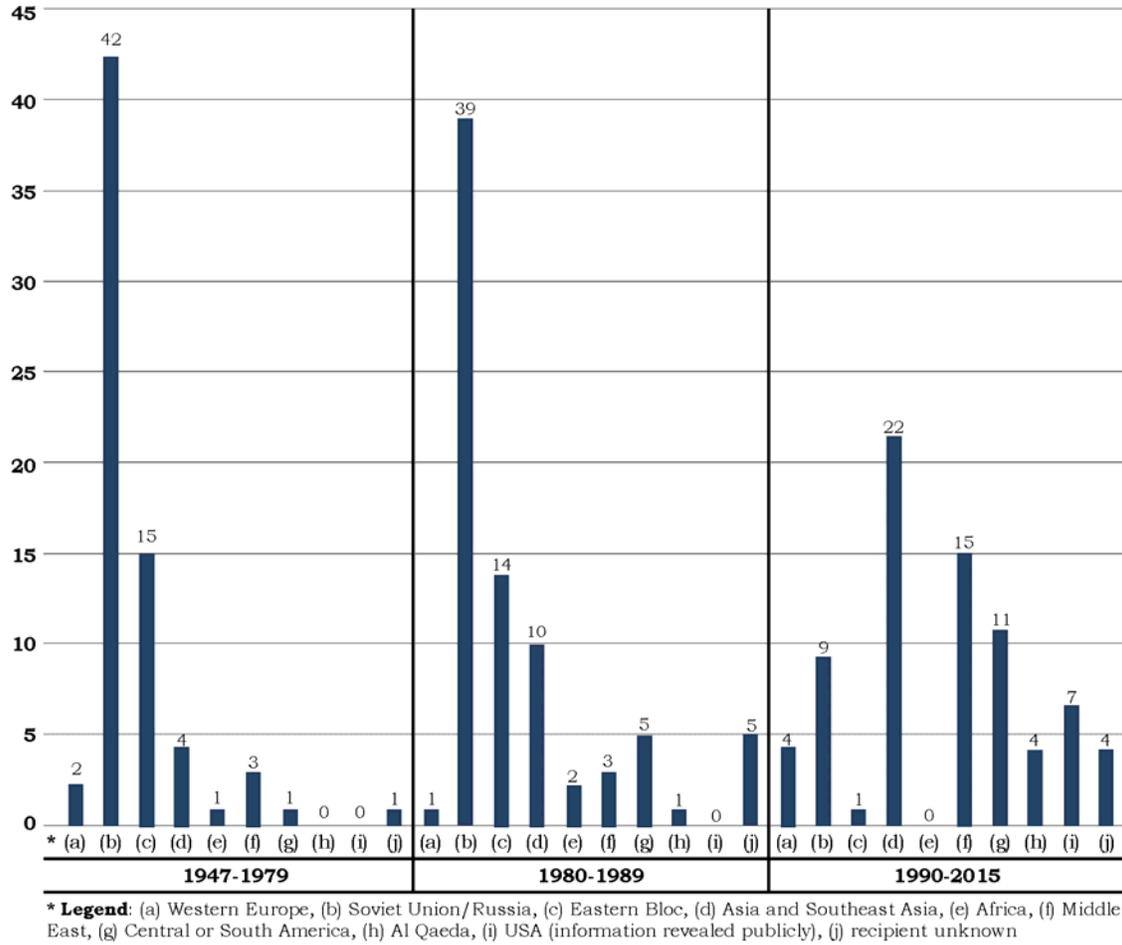
## ELEMENTS OF THE ACT OF ESPIONAGE

the Soviets. Soviet predominance as the recipient for American espionage also remained high in the later Cold War decade of the 1980s, with 66% attempts or transmissions to the Soviet Union or to the Eastern Bloc. In the third cohort since 1990, the Soviet Union or Russia and the Eastern Bloc nations declined as recipients to 13% of attempts or transmissions.

Only a few Western European nations received the fruits of American espionage in each of the three cohorts; the most recent cohort since 1990 is the largest with four Western European recipients. Countries in Asia and Southeast Asia, predominantly China, have been more common recipients of American espionage since 1990, with the percentages of attempts or transmissions to the Far East increasing from 6% in the first cohort to 13% in the second to 29% since 1990. The Middle East and the countries of Central and South America likewise grew in popularity as recipients: from 5% and 4% in the first two cohorts the Middle East increased to 20% of attempts or transmissions, while Central and South America increased from 1% and 6% to 14% since 1990. Finally, Al Qaeda served as the recipient of information from Americans in four instances since 1990, and in seven instances Americans attempted or transmitted information to other Americans, usually journalists or public news sources, which then resent the information out into the world.

A chart of these data on recipients of espionage by Americans in Figure 1 illustrates the prevalence of the Soviet Union and their Eastern European allies during the first two periods, and the shift to a greater variety of recipients in the recent cohort.

## ELEMENTS OF THE ACT OF ESPIONAGE



**Figure 1 Number of Attempts and Transmissions of Information to Recipients, by Region<sup>12</sup>**

The more equal-opportunity competition for American secrets among recipients since 1990 implies more challenges for American counterespionage, since there are different strong foreign intelligence services to counteract and more foreign interests to watch. The Russians continue their traditional espionage activities, China invests heavily in its distinctive information gathering efforts, and Cuba fields effective intelligence service activities inside the United States. The three largest recipient countries for American espionage in the recent cohort since 1990 are China with 15 attempts or transmissions of information, the Soviet Union or Russia with 9, and Cuba with 7. However, there are also a larger number of recipients of even one or two instances of offers from Americans, including Cambodia, Iraq, Iran, Israel, Syria, Taiwan, Venezuela, France, South Korea, and Saudi Arabia. Approaches to these countries were not uniformly welcomed or accepted.

<sup>12</sup> This graph includes both attempts and completed transmissions of information.

## ELEMENTS OF THE ACT OF ESPIONAGE

### How Information Has Been Transmitted

Table 7 reports on three variables that capture details about the transmittal of information during espionage-related acts: (1) the media in which the information was prepared for transmittal; (2) the method that was used to transmit it; and (3) the location of the spy when the information was transmitted. These variables sometimes reflect knowledge that was gained by counterintelligence or law enforcement officers in the course of their investigations, and since they may reveal the sources or methods that were used, such information is often withheld or vaguely described in open sources. As such, there are much missing data in these variables. Even if an entry is coded “no,” that is, there is no mention in open sources of its use in the case, one cannot be certain that it was not used, only that it was not revealed publicly.

Therefore, these variables are not reported for each individual; we cannot know for sure that additional methods were not also used, and an individual may have used more than one medium, method, or location. Instead, all the entries in each variable that were mentioned are reported in the three cohorts as choices, and the sum of those reported methods is then used to derive the percentages listed by entry within a cohort.

**Table 7**  
**What, How, and Where Information Was Transmitted**

<b>Characteristics</b>	<b>1947-1979</b>		<b>1980-1989</b>		<b>1990-2015</b>	
Media transmittal choices	<i>n= 73</i> <i>choices</i>	<i>% of 73</i>	<i>n= 91</i> <i>choices</i>	<i>% of 91</i>	<i>n= 106</i> <i>choices</i>	<i>% of 106</i>
Original documents or photos	37	51	39	43	32	30
Photos, films, or videos of originals	16	22	13	14	5	5
Photocopies	8	11	9	10	14	13
Parts or equipment	0	0	4	4	3	3
Microfiche or via short wave radio	6	8	5	5	7	7
Memory	4	5	11	13	15	14
Electronic files	2	3	10	11	30	28
Method transmittal choices	<i>n= 73</i> <i>choices</i>	<i>% of 73</i>	<i>n= 102</i> <i>choices</i>	<i>% of 102</i>	<i>n= 77</i> <i>choices</i>	<i>% of 77</i>
Meeting in person	46	63	35	34	44	57
Courier	10	14	13	13	3	4
Telephone	2	2	11	11	11	14
Dead drop	7	10	5	5	5	6
Mail or telegram	7	10	11	11	7	9
Not attempted	1	1	27	26	7	9
Location transmittal choices	<i>n= 49</i> <i>choices</i>	<i>% of 49</i>	<i>n= 76</i> <i>choices</i>	<i>% of 76</i>	<i>n= 80</i> <i>choices</i>	<i>% of 80</i>
Out of country	25	51	22	29	25	31
Out of town from residence	6	12	9	12	11	14
Hotel or motel room	0	0	0	0	10	13
P.O. Box	0	0	1	1	3	3
Embassy	7	15	8	11	8	10
Parking lot	2	4	1	1	1	1
Not attempted	6	12	27	35	3	4
Other	3	6	8	11	19	23

Among the types of media transmitted by the persons in the first cohort, those active between 1947 and 1979, half of the media types were original documents. This declined in the second cohort to 43% and to 30% in the third cohort as photocopying and electronic transmission grew common starting in the 1980s. Taking photographs or filming original documents comprised almost one-quarter of the media transmitted in the first cohort, but this declined to 13% in the second and then to only 5% in the third. The incidence of sending photocopies (13% for the third cohort), actual parts or equipment (3% for the third cohort, and microfiche or shortwave radio transmissions (7% for the third cohort) remained roughly same

## ELEMENTS OF THE ACT OF ESPIONAGE

across the three time periods. Reliance on one's memory doubled from the first to the second cohort and almost tripled in the third to 14%. Not surprisingly, since 1990, the transmission of information by electronic files increased dramatically in the most recent cohort to 28%.

Meeting a recipient in person has been by far the most common method of transmission. More than three-fifths (63%) of methods chosen by those in the first cohort were meetings, and in the most recent cohort, meetings were the choice of 57% as well. In the second cohort, active during the 1980s, at a time when more young amateur spies tried their hands at espionage, the predominance of using meetings declined to 35%, but the proportion of instances with no attempt to transmit information—because the person had been prevented or intercepted before the attempt—increased to one-quarter of the total. Use of the telephone to transmit information increased over time, while the use of a courier, dead drops, and the mail or telegrams all declined.

Locations chosen for transmission, usually during meetings, have most commonly been outside the United States, either because the spy was already located abroad or in order to evade the monitoring and counterespionage activities undertaken by authorities in this country. Half of the locations for transmittal in the first cohort were outside the country, while in the second and third cohorts this decreased to roughly one-third of the locations, but they remained the most common choices.

A location out of town from where the spy lived or worked was the second most popular choice for transmitting information by the first cohort with 12%, and remained the choice of 12% and 14% in the second and third cohorts. Post office boxes and parking lots have not been common choices in any cohort. Going to a foreign embassy has been the location for 15% of instances in the first cohort, 11% in the second, and 10 % in the third. Hotel or motel rooms were no spy's choice of location in the first two cohorts, but since the FBI has honed its sting techniques to collect evidence by recording conversations in hotel rooms, these locations were used by at least 10 individuals in the recent cohort, to their regret. As in the previous variable on methods of transmission, there were more instances of interceptions before transmittal was attempted in the second cohort during the 1980s; this increased to 35% of the total for the second cohort. There has also been a steady increase in other locations of transmittal and this became one-quarter of the total for the most recent cohort, including transmission while in restaurants, in grocery stores, in cars, and by downloading over the Internet from classified networks while at places of work or by sending emails from home.<sup>13</sup>

---

<sup>13</sup> When the PERSEREC Espionage Database was first being developed in 1978, the possibilities of classified networks, downloading information over an Internet, or sending information or documents as attachments by email did not commonly exist. As these resources gradually became available during the 1990s and in the following decades, these new methods and locations used in espionage-related actions were coded in the database as "other." This initial lack of interest in the details of emerging methods in itself illustrates that our coders did not at first

CONSEQUENCES OF ESPIONAGE

The consequences American espionage-offenders suffer for their crimes vary from light punishments to life in prison. Occasionally, the rewards for espionage have been generous, but most often they have been disappointing. Table 8 reports available data on how espionage-offenders were detected, and then on trends in payment, initial prison sentences, and outcomes other than prison.

**Table 8**  
**Consequences of Espionage**

Characteristics	1947-1979		1980-1989		1990-2015	
	<i>(n = 66 methods)</i>	%	<i>(n = 85 methods)</i>	%	<i>(n = 107 methods)</i>	%
Known methods of detection <sup>14</sup>						
Surveillance	21	32	24	28	38	36
Tip	22	33	25	30	24	22
Confession	4	6	11	13	9	9
Offer for sale	2	3	8	9	8	7
Telephone tap	2	3	7	8	10	9
Other	15	23	10	12	18	17
<hr/>						
Payment						
none	19	35	41	60	34	68
\$50 – \$999	3	5	7	10	0	0
\$1,000 – \$9,999	7	13	7	10	4	8
\$10,000 – \$99,999	15	28	8	12	9	18
\$100,000 – \$999,999	7	13	4	6	3	6
\$1 million or more	3	5	1	1	0	0
<hr/>						
Initial prison sentence, in years						
None	15	22	6	8	3	4
.1 – 4.9 years	8	12	15	21	28	42
5 – 9.9 years	10	15	14	20	13	20
10 – 19.9 years	13	19	14	20	11	17

recognize during this period the import of the shift to reliance on information technology, and the large impact it would have on espionage. The shift happened gradually.

<sup>14</sup> This variable shows the number of known methods of detection, not the number of individuals as in the subsequent variables in this table. All methods of detection mentioned for each individual are coded, and an individual may have used more than one method. So, for example, among the first cohort of 68 individuals, there were 21 instances of surveillance leading to detection. There were 22 tips, 4 confessions, 2 offers to sell information, 2 wire taps, and 15 other methods of detection described in open sources for these 68 persons, for a total of 66 methods mentioned for the persons in this cohort. To get a percentage, each method is divided by the number of that type of method for the cohort, i.e., for surveillance in the first cohort: 21 / 66 = 32% of the methods mentioned for the first cohort included surveillance.

## CONSEQUENCES OF ESPIONAGE

Characteristics	1947-1979		1980-1989		1990-2015	
20 – 29.9 years	4	6	10	14	2	3
30 – 39.9 years	4	6	6	8	5	8
40 years	2	3	1	1	0	0
life in prison	11	17	6	8	4	6
	<i>n=14</i>		<i>n=5</i>		<i>n=2</i>	
		%		%		%
Outcomes other than being sentenced to prison at trial						
Discharged	2	14	0	0	2	100
Defected	5	36	3	60	0	0
Granted immunity	1	7	2	40	0	0
Suicide	4	29	0	0	0	0
Died	1	7	0	0	0	0
Exchanged	1	7	0	0	0	0

The first variable in Table 8 reports on known methods of detection rather than on numbers of individuals as the remaining variables in this table do. How a person who was planning or committing espionage was detected is a sensitive piece of information that usually is withheld from the public by counterintelligence and law enforcement authorities in order to protect the sources and methods they use. What does appear in open sources may be vague, implied, or even doctored by those authorities. There are much missing data for this variable. Since in each cohort more methods were mentioned for roughly similar numbers of spies, and persons may have been detected by the use of more than one method, these data reveal little about changes over time. For each cohort, roughly three-fifths of the known methods of detection were either surveillance or getting a tip. The other methods coded here, confession to the crime, making an offer for sale, and use of a telephone tap, were less common. A variety of methods of detection were coded as “other,” including discovery by various kinds of monitoring (video, Internet, and counterintelligence monitoring), physical search by police in the course of responding to another crime, captured documents from the Iraq War, suspicious polygraph results, financial analysis of a person under suspicion, discovery in the course of committing another crime, or as part of the investigation of a crime by an accomplice, and a recipient of information who turns the person into the authorities.

Espionage-related crimes by Americans are a loser’s game. The proportion of spies who received no payment at all increased over time from 35% of the first cohort, to 60% of the second cohort during the 1980s, to 68% of the recent cohort starting in 1990. Across all three cohorts, one-half of those who received no payment were intercepted before they could transmit information and receive payment for it (46 of 94 individuals)<sup>15</sup>. Another one-fourth of persons who were not paid acted from an

<sup>15</sup> Interceptions are reported in Table 6.

ideological commitment or from divided loyalties to another country or cause, and these 24 offenders did not seek payment for their activities.

The amounts of money paid to offenders who did get paid has also uniformly decreased for those in the most recent cohort compared to the first cohort when, for example, 22 individuals made between \$10,000 and \$100,000. Since 1990 only 12 persons have made that much money. Three spies in the first cohort, who began between 1947 and 1979, became millionaires from their crimes (Larry Wu-Tai Chin, John Walker, and Clyde Conrad) and one did so who began in the 1980s (Aldrich Ames), but no one has received that much money for espionage-related crimes who began since 1990.

On the other hand, while it is poorly paid, espionage by Americans usually ends in prison. Individuals who received no prison sentence have declined across time from 22% of the first cohort to 8% of the second and 4% of the third. The two lowest categories of prison time, 1 to 5 years and 5 to 10 years, both show increased numbers of persons over time, especially the 1 to 5 category where 12% of the first cohort increased to 21% of the second and 42% of the third. The next four categories of between 10 to 40 years in prison generally declined over time as espionage drew somewhat lighter sentences and the types of laws used in prosecutions grew more varied. Eleven spies in the first cohort received life sentences, six did so in the second, but only four in the third.

In the decades of the first cohort, outcomes for espionage other than a prison sentence were more common, but these have declined starting in the 1980s. The numbers in this variable are very small. Two individuals in the first and two in the third cohort have been discharged, usually for prosecutorial misconduct or failure. Five persons in the first and three in the second cohort defected to the country to which they sent information before they could be prosecuted. One person in the first and two in the second cohort were granted immunity from prosecution. Four persons committed suicide before they could be prosecuted; all of them were in the first cohort. One person, Ruby Schuler, died from alcoholism during the investigation into her crime as an accomplice of James Harper. One person in the first cohort was exchanged for another prisoner.

## MOTIVATIONS

### MOTIVATIONS

It is challenging to distill into a limited number of categories a person's motivations for taking such a risky and consequential action as to commit espionage against one's country. Even when the categories appear to fit a crime as closely as possible, the nuances, the flavor, the idiosyncratic elements that a person brings to motive are unique. Therefore, the analyses here try to capture two related dimensions of motivations: first, the main thrust of the espionage offenders' motives in "strong motivations," which are either the person's only motive or the primary motive; and second, the wider picture of all motivations over time, including secondary and minor motives, held by the 209 persons under study here.

#### **Strong Motivations for Espionage**

The strong motivations of individuals to commit espionage-related crimes over the three time periods are reported in Table 9. This table differentiates between the number of persons who had a sole motive, which presumably would also be the strong one, and the number of persons with multiple motives among which has been identified the primary motive for each variable. Where evidence suggested it, multiple motives were coded as primary, secondary, or tertiary. This was necessarily a subjective judgment since it was based on written open sources and not on personal interviews. If possible, it is most historically accurate to determine motivation from evidence available while the crime was being committed, rather than from the self-justifications of the offender after the fact.

Once caught, spies tend to justify their actions to themselves and to others. They see their own past intentions and the pressures that may have affected their behavior in a changed and often generous light. For some individuals however, their retrospective justifications are the only available evidence about their motives. Since each person who had more than one motive has had one of them designated as primary by coders, Table 9 depicts the strong motives of all 209 persons in the database. It does not, however, present secondary or tertiary motives, and so it is not the complete picture. Secondary and tertiary motives are accounted for in Table 10.

**Table 9**  
**Strong Motivations for Espionage**

<b>Characteristics</b>	<b>1947-1979</b>		<b>1980-1989</b>		<b>1990-2015</b>	
Persons in each cohort	<i>n</i> =68		<i>n</i> =74		<i>n</i> =67	
Number persons with a sole motive	44		34		22	
Number persons with multiple motives	24		40		45	
	<i>n</i>	%	<i>n</i>	%	<i>n</i>	%
Money						
Sole motive	20	29	26	35	7	10
Primary among multiple motives	10	15	21	28	18	27
	30	44	47	63	25	37
Divided loyalties						
Sole motive	8	12	3	4	9	13
Primary among multiple motives	7	10	10	14	15	22
	15	22	13	18	24	35
Disgruntlement						
Sole motive	7	10	2	3	2	3
Primary among multiple motives	5	7	3	4	8	12
	12	17	5	7	10	15
Ingratiation						
Sole motive	4	6	1	1	3	4
Primary among multiple motives	1	1	6	8	4	6
	5	7	7	9	7	10
Coercion						
Sole motive	4	6	0	0	0	0
Primary among multiple motives	1	1	0	0	0	0
	5	7	0	0	0	0
Thrills						
Sole motive	1	1	1	1	0	0
Primary among multiple motives	0	0	0	0	0	0
	1	1	1	1	0	0
Recognition or ego						
Sole motive	0	0	1	1	1	1
Primary among multiple motives	0	0	0	0	0	0
	0	0	1	1	1	1

## MOTIVATIONS

Money has been the strongest motive for espionage by Americans. In the first cohort, 44% of persons had a strong motive to spy for money. This predominance increased during the 1980s when 63% of persons in the cohort held money as their strong motive. The 1980s earned the label “decade of the spy,” because of the apparent flood of cases of espionage by Americans who were spying for money (Lentz, 1985; Molotsky, 1985; Brock, 1987). Commentators expressed concern about a decline in American values when, during a Cold War, so many more young people were willing to betray their country’s secrets for money (Lentz, 1985). However, in the recent cohort that began espionage-related crime since 1990, money as a strong motive has declined somewhat, to 37%. This decline mirrors an increase in divided loyalties as a motive.

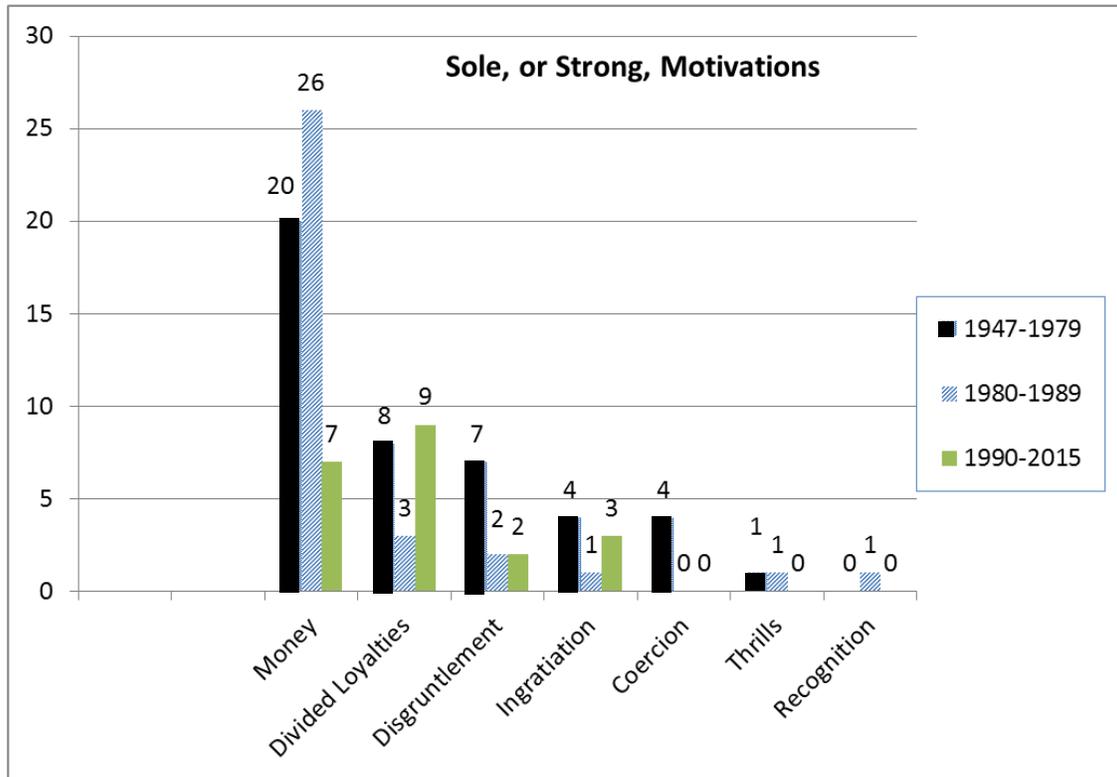
Divided loyalties is defined here as a commitment by American citizens to another country or cause that they put before the United States. This would include supporting terrorist groups or ideological systems such as Communism, as well as helping other nation states. While spying from divided loyalties was a less important motive in the first two cohorts, in which it was 22% of the first and 18% of the second cohort, it grew in importance among those in the most recent cohort. It rivaled money: among those who began espionage since 1990, a total of 35% spied from divided loyalties (combining sole and primary motives), compared to 37% for money.

Why are there more divided loyalties among those who began since 1990? In part, the increase would seem to reflect (1) the knitting together of the peoples of the world with improved transportation, communications, and the Internet, all of which helps to foster and maintain foreign ties, (2) an increase in the proportion of persons with ties to foreign nations in jobs with access to sensitive or classified information, and (3) the broadening of the categories of espionage in this analysis to include not just national security but also other types of espionage-related offences including leaks, economic espionage, foreign agent prosecutions, and export control cases.

Disgruntlement is the third most common motive for American espionage, although it is often mixed with other motives where it is a secondary or tertiary motive. It is defined as feelings of betrayal, disappointment, or resentment, at treatment usually experienced in a job or professional setting. Only 11 individuals across the three time periods committed espionage-related crimes solely from disgruntlement, but 16 others did so primarily from disgruntlement mixed with additional motives such as money or thrills.

The remaining variables show smaller numbers of individuals whose strong motive, sole or primary, was ingratiation, coercion by someone else (such as blackmail), thrills, or recognition. Ingratiation strongly motivated 10% or less in each cohort; coercion was a strong motive only in the first cohort with 7%, and thrills and recognition only served as strong motives for 1% of individuals in two of the three cohorts.

Figure 2 illustrates the pattern of strong motivations for espionage across the three cohorts. Here strong motivations are defined as having only one motive. The predominance of money in the first two cohorts is apparent.



**Figure 2 Sole, or Strong, Motivations**

**Motivations through Time**

Table 10 presents the data on motivations in a different way. Whereas Table 9 looked at the numbers of persons who held strong motivations (defined as sole motives or primary motives), Table 10 depicts motivation of any strength across cohorts. It answers the question, for example: “how many persons were motivated by money in the first cohort, no matter how exclusively or how strongly they held this motive?” This approach combines the persons with sole motivations with those who had multiple motivations, and so it accounts for motives that usually appear as secondary or tertiary in the coding of relative importance. It recognizes that inferring the relative importance of motives in a person’s action, no matter how carefully researched the available sources and how discerning the judgment, is subjective and inexact. For completeness, it is important to include all the motives spies have presented.

In Table 10, the unit reported is motivations, not persons. The number of motivations held by each cohort is reported at the top of the table, and within that total is shown the number and percentage of each motive held in each of the three

## MOTIVATIONS

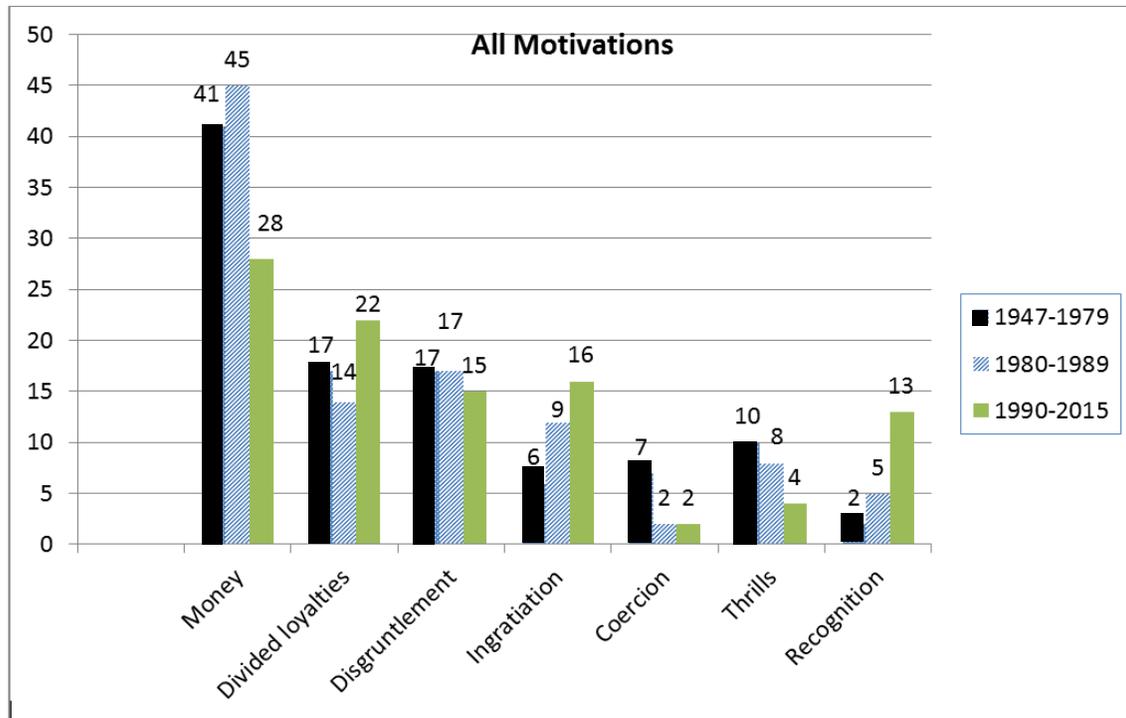
cohorts. Since some persons had multiple motives, those persons are counted for each of their motives and thus more than once.

**Table 10**  
**Motivations for Espionage through Time**

<b>Characteristics</b>	<b>1947-1979</b>		<b>1980-1989</b>		<b>1990-2015</b>	
Total motivations in each cohort	<i>n=100</i>	%	<i>n=129</i>	%	<i>n=134</i>	%
Money	41	41	58	45	37	28
Divided loyalties	17	17	18	14	30	22
Disgruntlement	17	17	22	17	20	15
Ingratiation	6	6	12	9	22	16
Coercion	7	7	2	2	2	2
Thrills	10	10	10	8	5	4
Recognition or ego	2	2	7	5	18	13

The findings in Table 10 reinforce those reported in Table 9. Money remains the predominant motive for Americans to commit espionage-related offenses, but in the recent cohort since 1990, it has declined in predominance from 41% in the first cohorts and 45% in the second to 28% in the third, with divided loyalties in the recent cohort a close second, disgruntlement and ingratiation almost tied for third, and recognition growing in importance.

Figure 3 depicts these data for all motivations, not differentiated by strength or primacy, in graphic form.



**Figure 3 All Motivations**

### Examples of Spying for Money

Because there are numerous motives in the espionage case of Tai Shen Kuo and his accomplices—ingratiation, recognition, divided loyalties, thrills—it provides a good example of multiple motives, but the primary motive in the case was money. Kuo came to the United States in 1972 from his native Taiwan on a tennis scholarship to attend college in Louisiana. After he graduated he stayed in New Orleans, where he opened a tennis club, a restaurant and then an import furniture store and became a naturalized citizen. Starting in the late 1980s, Kuo capitalized on his natural ability to make friends and develop useful contacts by expanding his business to China. Eventually he established an office in Beijing, becoming a “matchmaker” who could put American businessmen in touch with powerful Chinese officials (Arrillaga, 2011).

He marketed American products and services to China for other friends. A mutual friend put him in touch with a contact in China, “a good person to know,” who worked with one of the government-backed “friendship associations” that promote stronger ties with foreign nations while collecting intelligence by hosting visits to China. This contact worked for the Chinese government, and he became Kuo’s backer and handler. He encouraged Kuo to find out from friends with government jobs about the U.S. government’s attitudes toward the People’s Republic of China (PRC) and about its plans and intentions toward Taiwan (Klopott, 2009; Arrillaga,

## MOTIVATIONS

2011; U.S. Attorney's Office Eastern District of Virginia, 2008).<sup>16</sup> Kuo gradually developed government sources that could provide him with such information, as well as with the answers to his contact's specific questions. One such source was his neighbor, James Fondren Jr.

Kuo met Fondren in the late 1990s at the country club in Houma, LA, where they both lived and belonged to the club. Fondren had recently retired from the Air Force as a Lieutenant Colonel and was trying to start a consulting business. Kuo proposed to Fondren that he try writing opinion papers for his Chinese contact, who he described as a friend in Hong Kong who worked in academia (Arrillaga, 2011). Fondren began writing papers based on his expertise on Asia, and Kuo would pass along payment for these papers, ranging from \$800 to \$1500. Fondren wrote 30 reports between 1997 and 2008 which prosecutors later characterized as "thinly disguised regurgitations of classified military reports." Soon after he started producing opinion pieces, Kuo invited Fondren to be his guest on a trip to China, where they met Kuo's contact, and all three played golf together and enjoyed a scenic boat trip. Fondren's consulting business continued to boast only his first client, Tai-shen Kuo. For several years after that trip, Fondren and the Chinese contact exchanged dozens of emails on specific topics of interest to the People's Republic of China (PRC) (Barakat, 2009).

In 2001, Fondren returned to work for the federal government as deputy director of the Washington liaison office of United States Pacific Command. In that role he regained his Top Secret security clearance. He stopped corresponding with the contact by email and worked only through Kuo. Kuo's contact in China demanded that Kuo send him more and better sensitive information. Fondren wrote about topics that included official reactions to visits by Chinese military, joint Chinese-United States military exercises, intentions and plans for Taiwan, and insights into official American attitudes toward China. Some of these papers incorporated information classified Confidential or Secret. To assuage concern, Kuo told Fondren that his papers were being sent to government officials in Taiwan, but it is unlikely Fondren fell for that given his own relationship with the contact in China (United States District Court for the Eastern District of Virginia, Indictment, 2009; "Pentagon officials charged," 2009).

Kuo next developed Gregg Bergersen as a second source. Bergersen was introduced to Kuo in 2006 at a party during one of Kuo's regular visits to northern Virginia. Bergersen, a Navy veteran, worked in the Pentagon as a weapons analyst for the

---

<sup>16</sup> In 2009 the press was identifying Kuo's contact in China as Lin Hong, a Chinese intelligence officer (Klopott, 2009). In 2011, an article in the *Miami Herald* amplified that this contact named Lin Hong had worked for the Guangdong Friendship Association in addition to being an intelligence officer (Arrillaga, 2011). However, the affidavit filed in the Eastern District of Virginia for Kuo, Bergersen, and Kang identifies the contact only as "PRC official A" but places him as based both in Guangzhou, PRC, and in Hong Kong (Affidavit, 2008). Guangzhou is the capital city of Guangdong province, also known as Canton, in the south of the PRC.

Defense Security Cooperation Agency, which oversees foreign military equipment sales and tracks global weaponry. He and Kuo found each other mutually promising: Bergersen was thinking about retiring from the government and hoped his next step would be into a lucrative consulting job, while Kuo told him he was just setting up a defense consulting firm in Taiwan that would need partners like Bergersen. Kuo wanted another government source with a Top Secret security clearance and access to information on weapons policies and Taiwan; Bergersen fitted his needs perfectly. Bergersen believed Kuo's story that his information would be sent to Taiwan, and was thus taken in by Kuo's "false flag" operation against him (Montlake, 2008; Markon & Johnson, 2008).

Kuo cultivated Bergersen's friendship by taking him out to restaurants, on outings to various cities, and paying for their trips to Las Vegas, where he underwrote Bergersen's gambling habit. Soon Kuo asked his friend to show him open source reports and plans from his office, and then asked for more restricted or even classified documents. In an infamous video taken in a rental car by a hidden camera, Bergersen and Kuo discuss the classified report for which Kuo pays by putting a bundle of folded bills into Bergersen's shirt pocket. In the video Bergersen is conflicted, claiming he will go to jail if anyone finds out he has shared this report, and Kuo assures him he will only take notes from it. Kuo then takes the report into a restaurant and copies out large sections from it while Bergersen sat waiting for him in the car.<sup>17</sup> Among other documents, Bergersen passed Secret information to Kuo about Taiwan's upgrades to its C4ISR systems and about the United States' 5-year plan for military sales to Taiwan (Lewis, 2008; "Caught on Tape: Selling America's Secrets," CBS News, 2010).

Although he used email and phone calls to communicate with his Chinese contact, Kuo also sent his reports and documents to China using a "cut out," a young Chinese woman, Yu Xin Kang, who was also his employee at the furniture store and his lover. A cut out, as the name implies, is used to create a gap between the supplier of information and the recipient in an espionage transaction. Kang was a Chinese national, an intelligence officer, and a legal permanent resident alien in the United States. At Kuo's request, in 2007, she came to New Orleans to help him and serve as a courier for his information, traveling back and forth between New Orleans and her apartment in Beijing, where she would meet Kuo's contact to hand over materials (Morris, 2008).

The FBI learned of the espionage operation by Kuo, Bergersen, and Kang in 2007 in the course of investigating another Chinese espionage operation, this one in southern California, which focused on Chi Mak, an electrical engineer at a defense contracting company who had been passing information as a Chinese sleeper agent

---

<sup>17</sup> This FBI video became the source for a segment on the CBS television show *60 Minutes* on February 25, 2010, in which the video was shown interspersed with commentary by FBI and counterintelligence officers. The video was made public and is still available on the Internet, as is the *60 Minutes* segment.

## MOTIVATIONS

for decades.<sup>18</sup> The FBI secretly searched Chi Mak's home and found names in his address books that included Tai-Shen Kuo and Kuo's Chinese contact. They began to run surveillance on Kuo during 2007 and 2008, following him to his meetings with Bergersen, tapping his phone and tapping his email, and tailing Kang—during this time they bugged Kuo's rental cars to get the incriminating videos of his meetings (Markon, 2008).

The FBI arrested Tai-Shen Kuo, Gregg Bergersen, and Yu Xin Kang on February 11, 2008. Ironically, Kuo's arrest took place at the home of James Fondren Jr., the friend whom Kuo had come to visit. This prompted the FBI to look into Fondren, who was arrested in turn in May 2009. Kuo pled guilty to conspiracy to deliver national defense information to a foreign government and was sentenced to 188 months in prison (15 years and 7 months) and forfeited \$40,000. In 2010 his sentence was reduced to 5 years based on his "complete cooperation" in the prosecution of Fondren, his good behavior in prison, and the relative seriousness of the information he betrayed. Bergersen pled guilty to conspiracy to disclose national defense information and was sentenced to 57 months in prison (4 years and 9 months) and 3 years supervised release; Kang pled guilty to aiding an unregistered agent of a foreign government (Kuo) and was sentenced to 18 months in prison and 3 years supervised release (Associated Press, 2010).

Fondren was indicted in May 2009, went to trial in September, and was convicted of unlawful communication of classified information to an agent of a foreign government and lying to the FBI. He was sentenced in February 2010 to 36 months (3 years) in prison and 3 years supervised release (U.S. Attorney's Office Eastern District of Virginia, "New Orleans Man Sentenced," 2008 [Kuo]; U.S. Department of Justice, 2008; "Former Defense Department Official Sentenced," 2008 [Bergersen]; U.S. Department of Justice, "Jury Convicts Defense Department Official," 2009 [Fondren]; U.S. Department of Justice, "New Orleans Woman Sentenced," 2008 [Kang]).

Kuo's motivations were first money, then divided loyalties to China, and finally the thrills he got from balancing the precarious and complicated parts in his life as both an American entrepreneur and a spy for China. Bergersen's motivations were also first money, although he denied this at trial and blamed his alcohol and gambling addictions, then ingratiation with his generous friend Kuo, and perhaps equally important, the recognition and career boost he expected from Kuo's offer to make him a partner in the projected defense contracting business in Taiwan. Money seems to have been Fondren's motivation, perhaps mixed with recognition. Kang's motivation was professional, and also a desire to ingratiate herself with Kuo,

---

<sup>18</sup> The Chi Mak case has been widely written up, and it is discussed in detail in the previous PERSEREC technical report "Changes in Espionage by Americans 1947-2007," (2008).

on whom she had an emotional dependence. As an intelligence agent for China, her loyalties were not divided.<sup>19</sup>

Wanting money may be the most common motive for espionage, but in turn, it can express some underlying need or unacknowledged motive, as was played out by most of the individuals in the Kuo case. Wanting money can express various psychological forces that were preying on the spy. While this study does not take a psychological approach and does not reflect access to conversations or clinical interviews with convicted spies, other studies do report on insights that were gained from this type of access, and this type of study may usefully expand on the basic motives discussed here.

Based on clinical interviews with three spies who wanted money, Earl Pitts, Robert Hanssen, and Brian Regan, one psychiatrist finds that while money may be the usual superficial motive, the underlying motive for espionage is most often fear of failure, which he ascribes particularly to men. He explains that “The only meaningful fact is whether the prospective insider spy feels like a failure to the point of it being intolerable for him....” This author goes on to describe ten stages he sees in the evolution a spy from initial motive to acting on that motive in an act of espionage (Charney, 2010).

Another student of espionage emphasizes that as it applies to money, “Espionage is a crime with complex, multi-faceted motivational factors that do not lend themselves to easy explanations,” and the factors reflect “intersecting psychosocial forces” (Thompson, 2014). His interviews with convicted spies suggest that the personal and cultural meanings of money may be as motivating as the typical categories of financial need, greed, or debt.

The study notes that explaining a money motive may require understanding what not having the trappings of money—success, social status, and power—implies to the individual. For example, the ostensible motive of Aldrich Ames to commit espionage was to get \$50,000 to pay off his debts, but in interviews later he was more self-aware: “I did it for the money...not because of what it could buy but because of what it said about me... It said Rick Ames was not a failure” [Thompson, quoting Earley, 1997]. Thompson goes on to discuss other psychological dimensions of espionage, but comes back to money to make the point that some spies act from a simple pressing need for money coupled with an inability to delay gratification or to plan their future in a way that addresses this need without crime. Espionage can solve such a problem almost immediately, for a while (Thompson, 2014).

A third study elaborates on the typical motives for espionage, such as money, by exploring how they may be intertwined with deeper human impulses. It applies

---

<sup>19</sup> Since Yu Xin Kang is a Chinese national, she is not entered in the PERSEREC Espionage Database, and is discussed here only in her role as a co-conspirator in the espionage of the others who were American citizens.

## MOTIVATIONS

Robert Cialdini's six principles of interaction to how case officers successfully recruit agents to be spies by playing on their motives.<sup>20</sup> Cialdini's principles are described as "patterns of behavior that occur in the same order and sequence every time a given stimulus is introduced," so they apply to any human interaction (Burkett, 2013). The discussion applies each of six principles to the task facing a recruiter of spies. For example, one can see the principle of reciprocation at work as a recruiter begins an approach to a potential agent because he or she typically will try to do a small favor or provide a service for the potential new friend. Once the person has been helped, he or she feels obligated to reciprocate and help the recruiter in turn, which may lead to a series of exchanges that escalate into the sharing of ever more sensitive information. Cialdini argues that responses to the initial stimulus—the favor—generate reciprocal assistance, and this cycle of helping is automatic and built into the structure of human interactions<sup>21</sup>. The responses would operate beneath the new spy's conscious awareness; these impulses to help would be motives operating beneath other conscious motives that would be typical, such as a need for money or wanting revenge at work (Burkett, 2013).

### Examples of Spying from Divided Loyalties

Table 10 shows that divided loyalties has been the second most important motive in two of the three cohorts, the first and the third, but by including secondary and tertiary motives in this table, disgruntlement emerges for the first two cohorts as equally predominant with divided loyalties. Individuals are often both disgruntled and moved to act by another, stronger motive. Instances of divided loyalties that have motivated espionage-related offenses by Americans have almost doubled between the second and the most recent cohort.

Gwendolyn and Walter Kendall Myers, discussed earlier as examples of espionage by a spy who had access to classified information and an accomplice with no access, were also examples of divided loyalties. Taking no money, they spied for Cuba for 3 decades from an ideological commitment to the Cuban revolution and the Communist regime that sustained it (Clark, 2010). Another example of divided loyalties is the puzzling case of Ben-Ami Kadish and his arrest for espionage in 2008.

Kadish was born in 1923 in Connecticut, but at the age of 4 he was taken to British Palestine and grew up there. He fought for Israeli independence and served in both the British and the American militaries in World War II (Newman, 2008). He returned to the United States and became a mechanical engineer. Starting in 1963, Kadish worked at the U.S. Army Armament Research, Development, and Engineering Center at the Picatinny Arsenal in Dover, New Jersey, where he held a

---

<sup>20</sup> Cialdini's six principles are reciprocation, authority, scarcity, commitment and consistency, liking, and social proof.

<sup>21</sup> This is not to claim that reciprocation would automatically lead to espionage, but only that it would automatically lead to some helping response, such as an innocuous return favor.

Secret security clearance (Department of Justice, “Man arrested,” 2008). In 1990, Kadish retired and moved with his wife to a New Jersey retirement community, “The Ponds,” where he participated in veterans’ activities and support groups, organized religious events, delivered Meals on Wheels, and joined in sports and community activities with his retiree neighbors (Newman & Fahim, 2008). Eighteen peaceful years after he left his Army job, the FBI came to his home and arrested Kadish, charging him with committing espionage for Israel between 1979 and 1985 while he worked at the Picatinny Arsenal (Johnson, 2008).

Kadish eventually admitted the essential outlines of the case the FBI made against him, and he pled guilty to one count of participating in a conspiracy to act as an unregistered agent for Israel. From 1979 through 1985 he had worked with Yosef Yagur, then a science advisor at the Israeli consulate in New York, who would telephone Kadish asking him for specific titles of classified documents and reports that Yagur wished to collect. Kadish would remove the requested documents from the classified library at the Arsenal and take them home. Yagur would come to Kadish’s home and photograph the documents in Kadish’s basement, then return to his own home in the Bronx (Cowan & Chan, 2008; Department of Justice, “Man arrested,” 2008). Among the roughly 150 documents Kadish shared with Yagur were materials on nuclear weapons classified “Restricted Data,” information on the modified F-15 fighter jet with the caveat NOFORN, and a Secret document regarding the U.S. Patriot missile air defense system (Department of Justice, “Man arrested,” 2008). While Yagur was working with Kadish in the mid-1980s, he was also one of several handlers working with Jonathan Pollard, whose work as an analyst at the Naval Intelligence Command gave him access to highly classified naval intelligence. In the same method Yagur used with Kadish, but on a much larger scale, Pollard carried boxes of classified documents from his office for his handler to photocopy at Pollard’s apartment (Neumeister, 2008).

This flow of information from both Pollard and Kadish ended abruptly in late November 1985, when Pollard and his wife, Anne, were arrested and charged with espionage, and Yagur fled from the United States to Israel. The Pollards’ attempt to evade capture by claiming asylum in the Israeli Embassy, only to be turned away by the guards at the Embassy gate, is one of the iconic espionage images of 1985 from the “year of the spy” (Olive, 2006). Thereafter, Yagur lived in Israel and Kadish lived in New Jersey, but they maintained their relationship long distance, and Kadish visited Yagur in Israel in 2004. After his arrest in 2008, Kadish telephoned Yagur, who told him to lie to the FBI and say he did not remember events so long ago. Kadish did initially lie, and he was charged with lying to the FBI, though this charge was later dropped along with several others. Having pled guilty to the one count, in May 2009, a judge sentenced Kadish, then 85 years old, to no prison time and no probation but to pay a fine of \$50,000, to which at his hearing Kadish replied, “No problem” (Neumeister, 2009; Neumeister, 2008). He returned to his wife and his retired life at The Ponds.

## MOTIVATIONS

The puzzling aspects of Kadish's arrest and prosecution were the timing and the motive of the authorities for pursuing him after so long. The case set off considerable speculation in the press about whether there had been or continued to be more sources working for Israel in the United States, including a "super mole," long after the Pollards' arrest (Stein, 2008); whether Kadish's trip in 2004 to Israel to see Yagur had set off this investigation into his actions decades earlier; whether the timing reflected political issues then-current in 2008 between the United States and Israel; or possibly if the timing was meant to affect the upcoming leak trial of two lobbyists, Steven Rosen and Keith Weissman, who worked for the American Israel Public Affairs Committee (AIPAC). (In May 2009, prosecutors withdrew charges against Rosen and Weissman after a series of unfavorable judicial rulings (Lewis and Johnston, 2009). Since Jonathan Pollard's supporters and the state of Israel itself have waged a vigorous effort to get his life sentence for espionage reduced and to obtain his release from prison, others speculated that prosecuting Kadish had something to do with preventing Pollard's release<sup>22</sup> (Meiman, 2008; Neumeister, 2008). These speculations were not satisfied and the mysteries about Kadish's prosecution remain. Kadish provided classified documents to his Israeli handler over the course of 6 years from divided loyalties. He did not take money, although there are hints that after he retired and during his prosecution he was quietly taken care of. At his sentencing hearing he is quoted as explaining to the judge that "It was a mistake. It was a misjudgment. I thought I was helping the state of Israel without harming the United States" (Neumeister, 2009).

Table 11 depicts potential associations between holding a divided loyalties motive, having native or naturalized citizenship, and three variables on foreign preference.

---

<sup>22</sup> Jonathan Pollard was released from prison on parole on November 20, 2015, after serving 30 years. The terms of his parole include his wearing an ankle bracelet for authorities to track his location and remaining in the United States for 5 years during the parole (Baker & Rudoren, 2015).

**Table 11**  
**Divided Loyalties Motivation, Citizenship, and Foreign Preference<sup>23</sup>**

Characteristics	1947-1979		1980-1989		1990-2015	
	n=68	%	n=74	%	n=67	%
Citizenship						
Born in U.S.	53	79	62	84	44	66
Naturalized	15	21	12	16	23	34
Persons with a divided loyalties motivation						
Born in U.S.	8	12	10	13	13	20
Naturalized	9	13	8	11	17	25
	17	25	18	24	30	45
Persons without a divided loyalties motivation						
	51	75	56	76	37	55
Person had foreign relatives						
Born in U.S.	21	31	8	11	9	13
Naturalized	15	22	10	13	22	33
No or unknown	32	47	56	76	36	54
Person had foreign connections <sup>24</sup>						
Born in U.S.	6	9	6	8	19	28
Naturalized	6	9	8	11	20	30
No or unknown	56	82	60	81	28	42
Person had foreign cultural ties						
Born in U.S.	1	2	6	8	14	21
Naturalized	5	7	5	7	20	30
No or unknown	62	91	63	85	33	49

As discussed in earlier tables, in the most recent cohort both the incidence of naturalized citizens and the incidence of divided loyalties as a motive almost doubled compared to each of the previous two cohorts. Naturalized citizens by definition would have ties to their country of origin, so it is not surprising that most

<sup>23</sup> The variables report the number and percentage of persons with foreign relatives, connections, or cultural ties within the two categories of 1) those born in the U.S., or 2) those who were naturalized citizens. A person may have more than one of these three ties, or may have none of them. Most persons in the database did not have these ties, or it was unknown whether they had them. Since by definition naturalized citizens come from a different country of origin that would lead to such ties, the interesting data in these variables are any similarities between the native born and the naturalized citizens.

<sup>24</sup> Foreign connections are defined as business or professional relationships or acquaintances. Foreign cultural ties are defined as the person speaks the language of origin at home, maintains memberships in groups with a focus on the country of origin, or takes political or educational activities in the country of origin.

## MOTIVATIONS

naturalized citizens do have foreign relatives, foreign connections, or foreign cultural ties.

More revealing in Table 11 are the notable percentages of native born American citizens who had these ties. In most instances, the proportion of those with these three types of foreign ties, no matter whether they were native or naturalized citizens, increased in the recent cohort since 1990. These data suggest that while there has been an increase in naturalized citizens in the recent cohort of spies, the increase in divided loyalties should not be attributed only to them.

When people have divided loyalties, they feel allegiance to more than one entity, usually to two nation states, but it may also be to two ideologies, two causes, or two non-state groups—or even to one or more of each. Ben-Ami Kadish was an example of someone who seemed to effortlessly hold allegiances to two nations, the United States and Israel. Walter and Gwendolyn Myers held two allegiances, one openly to the United States, and the other secretly to Fidel Castro and the Cuban revolution. As a nation of immigrants, the United States has long experience with welcoming immigrants and turning them into new citizens, while recognizing that ties of sentiment, financial support, and personal involvement with their countries of origin will persist (Spiro, 2008). In some periods of American history, recognition of those continuing ties has been generous, and at other times it has been grudging, with demands that the ties to the homeland be weakened in order to prove the new allegiance to the United States (Herbig, 2008). Individuals whose divided loyalties motivated them to commit espionage-related offenses often said they just wanted to help the other country or cause, while they downplayed or dismissed the harm their actions would do to the United States. Ben-Ami Kadish stated as much at his sentencing hearing.

### **Ingratiation, Coercion, Thrills, and Recognition**

The findings on ingratiating strengthen when Tables 9 and 10 on motivations are compared. Although not important as a strong motive in Table 9, when secondary and tertiary motives are included in Table 10 along with sole and primary motives, ingratiating increases as a motive across the three time periods. From 6% in the first and 9% in the second cohort, ingratiating was a factor in 16% of motives in the recent cohort, with 22 individuals motivated to some degree by trying to ingratiate themselves with a family member, a friend, or a handler.

Coercion has declined in frequency as a motive over time from seven persons in the first cohort to just two persons in the second and third cohorts who were motivated at all by coercion, and no one had coercion as a sole or primary motive in the second or third cohorts. The two most common pressures that had been used to coerce someone into espionage largely disappeared starting in the 1990s. First, the Berlin Wall fell after November 1989, and thereupon the Soviets abandoned the Iron Curtain that had kept people trapped in Eastern Europe from which their relatives in the West could be blackmailed. Secondly, the legal and social

acceptance of homosexuality began to accelerate in the United States. Threatening to harm a person's relatives living under Communist control in Eastern Europe, or threatening through blackmail to publicly reveal one's sexual orientation, have not been effective coercion strategies to make people commit espionage among persons in the last two cohorts. Given the new configuration of transnational terrorism, with its potential and ambition to reach into the United States, different kinds of coercion involving the threat of violence are conceivable.

Spying for the thrill of it has not been a strong motive, nor has it increased over time, yet it has persisted as a secondary or tertiary motive in the mix of various individuals' motives. Some spies enjoyed an emotional rush from the danger they faced while spying, and some, Robert Hanssen for example, thrived on beating the system for as long as that lasted, until they were caught (Vise, 2002).

The increase in recognition as a motive for espionage in the recent cohort since 1990 is telling. Recognition refers here to a desire to be recognized and rewarded for one's accomplishments or talents. This may be public recognition, experienced in benefits such as awards, promotions, or gaining a better job, or it may be private recognition—satisfaction—from playing the role of an expert, source, or advisor to an admired or powerful person. Recognition does have elements of a motive labeled in typical discussions of espionage as “ego,” since recognition involves gratifying the sense of self, but recognition is a more specific idea and better captures how this motive plays out in recent espionage-related offenses: as ambition for advancement in job or career, or striving to exert more influence and make more of a mark in the world.

### **Helping and Ingratiation**

Helping is a common theme in the explanations of espionage-offenders' actions. “We weren't motivated by ‘anti-Americanism,’” Walter Kendall Myers said at the sentencing hearing for him and his wife, “our objective was to help the Cuban people defend their revolution” (Perez, 2010). “I thought I was helping the state of Israel without harming the United States,” Ben-Ami Kadish said about his actions (Neumeister, 2009). “I believe our government's policy towards Cuba is cruel and unfair,” Ana Montes explained at her sentencing in 2002, noting that “I felt morally obligated to help the island defend itself from our efforts to impose our values and political system on it” (Golden, 2002). Individuals acting on divided loyalties reject the exclusive commitment of allegiance, and often claim they were above the petty demands of allegiance to a single nation. By helping another country, they imagined they were climbing onto a higher moral plane of international cooperation. “I'm Chinese, I'm American,” Dongfan Chung's wife<sup>25</sup> told a journalist after her

---

<sup>25</sup> Ling Chung must have known about her husband's actions in taking Boeing Corporation's proprietary materials related to defense weapons systems, since the papers were piled throughout her home. She also knew that her husband was sending materials to China and making

## MOTIVATIONS

husband's sentencing for economic espionage, "How beautiful is that! Why make it a confrontation?" (Bhattacharjee, 2014).

However, a desire to help is not limited only to those whose divided loyalties led them to commit espionage-related offenses. As noted earlier, Table 10 shows that ingratiating as a motive for espionage has gradually increased with time, from 6% and 9% of the first two cohorts to 16% of the most recent cohort who began since 1990. To ingratiate is to establish oneself in another person's good graces or favor, usually through deliberate effort.

The individuals who spied to ingratiate themselves with someone else usually claimed that they were trying to help the other person. Rosario Ames, Virginia Baynes, and Marjorie Mascheroni were helping their husbands or their lovers to spy (Miller & Pincus, 1994 [Rosario Ames]; O'Harrow, Jr., 1992 [Baynes]; Department of Justice, 2013 [Marjorie Mascheroni]). Frederick Hamilton, Michael Schwartz, and Lawrence Franklin were, they thought, sharing information with confidants to assist a close ally of the United States or even prevent a possible war (Hamilton in a confrontation between Ecuador and Peru; Schwartz by helping Saudi Arabia, an ally of the United States during the recent Gulf War; Franklin by heading off a war he thought was coming between Israel and Iran) (Gertz, 1993 [Hamilton]; "Norfolk Naval officer," 1995 [Schwartz]; Gertz, 2009 [Franklin]). Nathaniel Nicholson was helping his imprisoned father (Denson, 2001 [Nathaniel Nicholson]). Donald Keyser was helping his lover with her graduate research—unfortunately she was also a Chinese intelligence agent (Gerstein, 2006 [Keyser]). Ryan Anderson and Hassan Abujihad were trying to help people in Al Qaeda to advance the group's goals by sharing classified military intelligence (Kershaw, 2004 [Anderson]; United States Department of Justice, 2009 [Abujihad]). Gary Maziarz was helping the Los Angeles County Terrorist Early Warning Center by sharing classified intelligence with uncleared task force members (Rogers, 2008 [Maziarz]). John Kiriakou was helping journalists by acting as an expert source, but he got carried away with the role and shared the names of CIA officers and other classified information with the press (Coll, 2013 [Kiriakou]). In the eyes of others and in one's own eyes, seeing an act of espionage, the giving away of secrets, as helping is a lot more comfortable than seeing it as betrayal.

In addition to the theme of spying to help another country or cause from divided loyalties, and spying to help in order to ingratiate oneself with someone, there is often a personal exchange of helping in an espionage case. When a spy offers or is recruited to supply information, typically the recruiter becomes the spy's first handler and serves as his or her link to the consumer of the information. The role of handler is a demanding and delicate one, requiring management of the spy's anxieties, responding to crises that may interrupt the smooth course of the

---

presentations based on them in China. She was not indicted for economic espionage along with him. Chung's case is discussed in the following section on economic espionage.

espionage, and encouraging the spy to continue in a perilous activity. Because he or she is in a vulnerable position, the spy becomes dependent on the handler and may want to help him or her in return for care and protection.<sup>26</sup> One CIA study of the psychological dimensions of espionage describes the intimate relationship that can develop between spy and handler as follows:

Adept professional handlers depict themselves not only as willing to reward espionage but also as capable of safeguarding their agent. Good professional “handling” is designed not only to collect classified information but also to stabilize and reassure the spy in the interest of sustaining his or her capacity to commit espionage for as long as possible. As a result, the relationship between an agent and a handler is frequently highly personal, intense, and emotional, at least from the perspective of the spy, and the nature of this relationship is often a powerful force behind an individual’s choice to spy (“The psychology of espionage,” n.d.).

For example, Robert Hanssen developed an emotional relationship with his various Russian handlers over the 15 years, off and on, that he passed them highly classified documents from several government agencies. Cautious to the point of obsession and insistent that everyone should follow the contact procedures he had specified to ensure his security, Hanssen would be upset when a mistake or an unexpected event caused a missed communication. In March 2000, less than a year before his arrest, he wrote to his handler and left the letter at a drop site in his neighborhood park:

... I have come about as close as I ever want to come to sacrificing myself to help you, and I get silence. I hate silence... Please, at least say goodbye. It’s been a long time my dear friends, a long and lonely time... (United States District Court for the Eastern District of Virginia, *United States of America v. Robert Philip Hanssen*, Affidavit, 2001).

And in November of that year, he explained his anxiety to his handler in more detail, in words that sound like a lover who fears rejection:

... (For me breaks in communication are most difficult and stressful.) Recent changes in U.S. law now attach the death penalty to my help to you as you know, so I do take some risk.... I had no regular way of communicating [with you]. This needs to be rectified if I am to be as effective as I can be. No one answered my signal [at the drop site]. Perhaps you

---

<sup>26</sup> Two of Robert Cialdini’s six principles (discussed earlier) seem to apply in this discussion of helping: reciprocity, the obligation to help that is elicited by having an initial favor done for one, and liking, the principle that people like others who are like, or similar to, themselves. Recruiters, and later handlers, deliberately emphasize their similarities to the spy; they use flattery, and they try to develop a warm personal relationship so that the spy may come to feel that “the case officer is one of the few people, perhaps the ONLY person, who truly understands him.” (Burkett, 2013).

## MOTIVATIONS

occasionally give up on me. Giving up on me would be a mistake. I have proven inveterately loyal and willing to take grave risks which could even cause my death.... (United States District Court for the Eastern District of Virginia, United States of America v. Robert Philip Hanssen, Affidavit, 2001).

An overview of research on fraud, a crime that is often similar to espionage, notes that “We like to help each other, especially people we identify with. And when we are helping people, we really don’t see what we are doing as unethical” (Joffe-Walt & Spiegel, 2012). In frauds, as in espionage, the long term consequences tend to be distant and abstract, while the immediate benefits of the activities are much clearer. A spy contemplating the consequences of committing espionage knows at some level that these would be drastic, but also that they are in the future and they well may not even happen, while the reinforcement from helping a close friend is immediate (Thompson, 2014). Ironically, winding through espionage, which is one of the most serious crimes and usually means that one is betraying one’s country, are themes of helping out, sacrificing oneself to benefit another, and taking comfort from seeing one’s actions in an altruistic light.

---

---

**PART 2**

**TYPES OF ESPIONAGE BY AMERICANS**

---

---

## FIVE TYPES OF ESPIONAGE

### FIVE TYPES OF ESPIONAGE

There used to be just one type of espionage. It was the type described in spy novels like those written by John le Carré or Graham Greene. It was the type reported in newspapers when someone with a security clearance like Aldrich Ames or John Walker stole a classified report or a cryptographic key card and handed it over for cash to an agent working for a foreign nation. It was the type everyone understood as what was meant by the term “espionage.” It was classic espionage.

This report distinguishes among five current types of espionage by Americans. One of them, the most numerous and best documented by cases in the data collected here, is classic espionage. The other four types share basic elements with the classic type—and thus are recognizably espionage—but they differ from the classic in obvious ways, and they also differ from one another. These types have proliferated during last several decades.

The five types of espionage that will be explored here are:

- Classic espionage;
- Leaks of classified information;
- Acting as an agent of a foreign government;
- Violations of export control laws; and
- Economic espionage.

The type most recently recognized in law, economic espionage, gradually became a federal crime prosecuted as its own type of espionage based on the passage in 1996 of the Economic Espionage Act (EEA). Congress acted to protect industrial and commercial information that forms the economic base of the nation from theft by other nations in the same way that the espionage statutes protect national defense information that forms the civic and military defense base. The act criminalizes the misappropriation of trade secrets; one section applies to thefts done with knowledge or intent to benefit a foreign nation, and a second section applies to thefts done with knowledge or intent to injure the owner of the secret. The definition of a trade secret was based on the Uniform Trade Secrets Act (as amended 1985), and specifies that such a secret can be many things:

the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily

## FIVE TYPES OF ESPIONAGE

ascertainable through proper means by the public (Title 18 U.S.C. section 1831)

The other three types of espionage are not based on such recent legislation, but instead are based on new, different, or more rigorous applications of older laws.

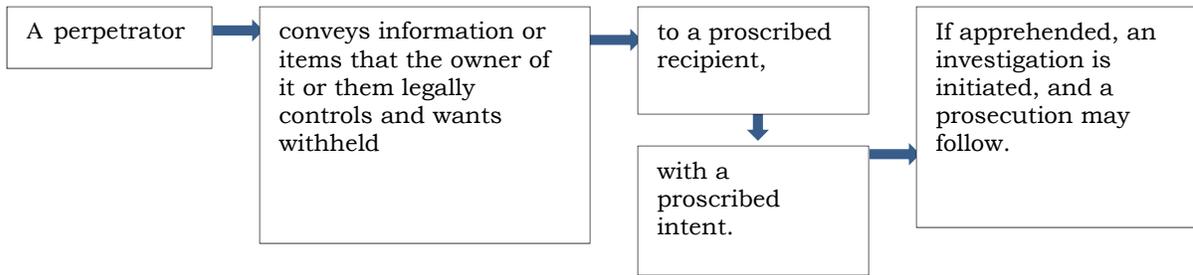
Individuals who surreptitiously collect information in the United States, or who advocate on behalf of and at the behest of a foreign power, have been legally required to register with the Attorney General of the United States since 1938 under the Foreign Agent Registration Act (18 U.S.C. section 1951). The act exempts persons acting openly; the concern is with those acting secretly for the interests of other nations. Information need not be classified. Some classic espionage cases were prosecuted in the past under both the Espionage Act statutes and under the Foreign Agent Registration Act, but as this study suggests, in the recent past, the number of persons who were collecting information and sending it abroad and who were prosecuted simply as foreign agents has noticeably increased. In part, intelligence documents recovered during the Iraq War have fueled this development.

The type of espionage defined by export control laws can be even more complicated than foreign agent espionage. An example of one of the main statutes protecting defense articles and technology dates from 1976 in the International Traffic in Arms Regulation, or ITAR. It authorizes publication of a United States Munitions List on controlled technologies that includes 20 categories including specific weapons systems, aircraft and vessels, military electronics, nuclear weapons, space technology, satellites, and related technologies. This information also need not be classified. Over the past 15 years, prosecution decisions have applied the export control laws to various cases that involved selling systems that were on the Munitions List to foreign powers, in effect, espionage.

The fifth type of espionage discussed here, leaks, also reflects trends in prosecution. There were only a few leak cases, in which controlled official information, almost always classified, is shared with the press or others not authorized to receive it, in the decades before 2009 and the start of the administration of Barack Obama. Under President Obama's Attorney General, at least a dozen prosecutions of leaks have been brought, not always successfully. All of the prosecutions have applied the Espionage statutes to American citizens who leaked information to other American citizens, who in turn published the information more broadly in the media or passed it to others.

These five types of espionage share elements that are intrinsic to an act of classic espionage. These elements and their sequence can be modeled as:

## FIVE TYPES OF ESPIONAGE



**Figure 4 A Model of Espionage Elements Based on Classic Espionage**

The elements in this model will be discussed in each of the five types of espionage considered in order to discern what they have in common and how they are distinctive. In addition to this model, cases that exemplify each of the five types will be explored, and for some of these examples, a standard checklist of elements, based on classic espionage, will be applied to them in order to highlight how the classic espionage elements have played out in the four other types as well.

Each of the five types of espionage discussed is presented in more detail later in this report to make an argument for seeing the current field of espionage by Americans in these terms. This five-part structure is not the only way to understand current espionage, its activities, its laws, and its prosecutions. One could choose to lop off one or more of the types, on the grounds that one or another type is too distinctive and thus too different from the other types to fit. Only this structure, however, describes current American espionage whole, with all its interrelationships, its contradictions, and its gaps.

Table 12 summarizes the types of espionage by the 209 Americans that are the focus of this report, in the three cohorts by the time period in which they began their activities. It would be convenient if each of the five types could be clearly differentiated from the others, but this is not the case. Each offender's charges and conviction determined into which type or types of espionage he or she was coded. Descriptions of what the person is reported to have actually done, even if evidence to prove it in court was lacking, was also considered.

Since classic espionage was the first and predominant type over the time period of study, the majority of cases here are classic. Increasingly in the recent past, however, prosecutors have charged individuals using both the Espionage statutes and charges of a second type. Therefore cases are reported by whether they seem to fall into just one type or whether they are two types.

**Table 12**  
**Types of Espionage by Americans**

Characteristics	1947-1979	1980-1989	1990-2015
	<i>n=68</i>	<i>n=74</i>	<i>n=67</i>
<b>Number of Persons Coded as One Type of Espionage</b>			
Classic	56	68	42
Foreign Agent	3	1	11
Export Control	0	1	4
<b>Number of Persons Coded as Two Types of Espionage</b>			
Classic + Leak	0	0	7 + Snowden <sup>27</sup>
Classic + Foreign Agent	8	2	2
Classic + Export Control	0	0	1
Economic + Foreign Agent	1	0	0
Export Control + Foreign Agent	0	2	0

The predominance of classic espionage in the 209 cases is apparent in Table 12, as are the ways classic espionage has been combined with prosecutions for other related types of espionage.

Table 13 presents the percentages of the classic cases, and the classic cases combined with other types of espionage, across time, which shows the predominance of classic espionage even more dramatically:

**Table 13**  
**Percentages of Classic Espionage Cases**

Characteristics	1947-1979		1980-1989		1990-2015	
	<i>n=68</i>	%	<i>n=74</i>	%	<i>n=67</i>	%
Classic	56	82	68	92	42	63
Classic + Foreign Agent	8		2		2	
Classic + Export Control	0		0		1	
Classic + Leak	0		0		7 + Snowden	
Totals of Classic cases	64	94	70	95	52	78

<sup>27</sup> Edward Snowden fled and has not been tried or convicted of a crime, but his actions merit some mention here.

It is not surprising that in Table 13 almost all of the cases, 94% and 95%, in the first two cohorts were classic espionage cases, some of which were combined with another type, because espionage involving national defense information, most of it classified, was the expectation before 2000. If people were prosecuted for espionage, they were usually prosecuted under the Espionage Act statutes, Title 18 U.S.C. sections 792 through 798, which are the core legal definition of classic espionage. Only in recent decades have different types of espionage been recognized, not always by that name, defined by other statutes that have come into greater use, or existing statutes have been applied to other crimes that reflect evolving technologies and communications that are seen to be more like espionage.

The most recent cohort, those individuals who began between 1990 and 2015, demonstrates the proliferation of types of espionage in the recent past. From 94% and 95% classic cases in the first two cohorts, classic cases drop in the recent cohort to 78% of the total. Exploring why this has happened requires comparing these various types of espionage in more detail, which will be the focus of the following sections.

In January 2008, J. Patrick Rowan, the Deputy Assistant Attorney General in the National Security Division of the Department of Justice, testified before a United States House of Representatives subcommittee. He began his remarks on the enforcement of federal espionage laws in a way that neatly introduces the comparison of types of espionage that follows:

It is my pleasure to appear before you today to discuss the National Security Division's enforcement of Federal espionage laws. As you know, the clandestine intelligence collection activities of foreign nations include not only traditional Cold War style efforts to obtain military secrets, but, increasingly, sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons. Accordingly, these activities and others implicate a wide array of Federal criminal statutes. But no matter what form of espionage is being used, or which statutes are implicated, there is one common denominator: our national security is always at stake (United States House of Representatives Committee on the Judiciary, 2008).

## ELEMENTS OF CLASSIC ESPIONAGE

There are many compelling studies of classic espionage and no need to attempt to add to them. The goal here is simply to identify basic elements in an act of classic espionage, so that as other types of espionage are discussed it will be possible to recognize many of these classic elements in them.

Typically, classic espionage is defined as activities (1) done for national government “A,” which (2) acts through an agent, who (3) clandestinely collects secrets, (4) from national government “B” that wants to control those secrets, and who (5) turns them over to national government “A.” Espionage is a subset of intelligence gathering; it is the illegal subset from the point of view of the government whose secret information is covertly being collected. Gathering information about potential adversaries involves some aspects that are legal and open, but usually these just support the other, clandestine aspects. Put together, the legal and the illegal may become useful intelligence. The United States, like many advanced nations, deploys a technologically sophisticated global intelligence gathering effort with the goal of ensuring American national security and, as one part of that effort, it sends identified but also unidentified agents to various places to collect information that the host would prefer remain under its control. These American agents, and their sources that provide information to them, are working for the United States and its interests; they are our spies (Sulick, 2013; Volkman, 1994).

This intelligence is not the classic espionage being considered in this report and in this section, because all of the persons discussed here were American citizens who conveyed to another country or cause information the American government wanted to remain under its control. They were not American agents working for their government; indeed, they were Americans working against their government. So while these cases share basic elements of typical espionage being performed on behalf of the nation, they also differ from that espionage in a crucial way: to their fellow Americans and to the American government, these individuals are criminals whose activities are a betrayal of America and American interests.

These are the spies that counterintelligence officers seek to counter by tracking and deterring foreign intelligence activities and identifying these Americans who are working as their agents (Van Cleave, 2013). In a broad sense, this is classic espionage done by insiders, that is, by American citizens. Typically, the term “insider” refers to a restricted type of membership in a group that provides special, privileged knowledge or access. Simply being an American citizen produces an awfully large group of potential insiders, although legally, only American citizens are eligible for access to classified information. Classified information is the major target of espionage against the United States, so some studies of espionage reflect that fact by focusing only on those with eligibility for access to classified information. This seems too narrow, however, since espionage, even classic espionage, does not exclusively involve information that has been classified. Because espionage is serious and may damage the well-being of the nation, when

## ELEMENTS OF CLASSIC ESPIONAGE

done by American citizens against the United States it is treated as a crime of betrayal of the allegiance they owe to their country of birth or adoption.

The context of classic espionage is a competition, a contest, or a struggle (CI Glossary, 2012; Manual for Courts-Martial, 2012)<sup>28</sup>. At its most extreme, the context is international warfare. This means that espionage takes place in a context of “us vs. them,” and an action that is reprehensible and illegal to those on one side of the contest will be judged admirable or even heroic by those on the other side. For example, the United States imprisoned CIA officer Aldrich Ames for life for his crime of espionage. In gratitude for his valuable spying services to them, the Soviet Union funded a generous reward for Ames of \$2 million, which is now held for him in Russian banks (Earley, 2001).

Classic espionage is secret, and it is secret in two senses: (1) in what it collects and (2) in how the collection is done. On the one hand, collecting information is done clandestinely and secretly because in order to obtain information the other side wants to keep under its control, an agent must not let the adversary know what he or she is trying to do. An assumption underlies this interaction, which is that governments protect and most strenuously control information they value most and which makes them most vulnerable in the contest. It follows that, secondly, the information to be collected is itself a secret. To find out what is really going on with the competitor or adversary, what their plans, intentions, and capabilities are, the assumption is that it is necessary to penetrate layers of security and denial created by the adversary to pluck out the secrets kept within.

The secrets in classic espionage are political or military in nature. Classic espionage has an ancient pedigree; examples can be found in the Bible and in ancient Greek and Chinese warfare and then throughout history in the wars and struggles between peoples up to the present. Consistently across that long history, the secrets sought through espionage are about military capabilities, new technologies or organizational structures, and foreign policies dealing with intentions, goals, and relative strengths and weaknesses. In the serious competition between nations, this is the type of information that could tip the balance of national life or death.

In recent decades since the end of World War II, governments have realized that economic health is also so vital to a nation’s future that they treat economic information as the third kind of secret which, along with political and military secrets, needs to be protected from covert collection by adversaries. It was a short step from that recognition to seeing the need to keep from adversaries’ awareness a nation’s technological advances, improved manufacturing methods, scientific breakthroughs, innovations in weaponry, space, and aviation, and the many thousands of other developments in a vibrant national economy that would be advantageous in international competition. From the triad of secrets in classic

---

<sup>28</sup> The summary of elements of classic espionage that follows is drawn from these sources.

espionage—political, military, and economic—the need to protect additional kinds of secrets would grow.

Classic espionage usually involves theft. Stealing the secrets is an obvious and time-honored method for taking control of them and sending or transporting them to a recipient. Physically stealing secret documents or objects has recently been supplemented by electronically stealing secret files, plans, or communications such as email. Other elements of classic espionage include surveillance and indirect theft. Observing, watching, and collating patterns of activities can often yield useful information, as can listening in by planting electronic devices or performing computer sweeps where the adversary communicates unguardedly.

Subterfuge is commonly a part of classic espionage, which is to be expected given that it is both illegal and clandestine. The need to disguise and deceive plays out in many ways in the lives of espionage agents. They will be busy creating and enacting cover stories and false identities, protecting the true purpose of their activities from observers and their targets, perhaps deceiving their sources about who will actually receive the information being supplied, and many other ploys. Whether individuals volunteered to spy or were recruited by a foreign intelligence service,<sup>29</sup> when they became spies they took up lives of double-dealing and its burdens. Because classic espionage is illegal and reviled by society as betrayal, the effort to maintain a false persona and to stay vigilant against possible discovery and arrest takes a psychological toll. What might at first seem like a romantic or thrilling adventure—to become a spy—seldom remains so as time passes.

Christopher Boyce, for example, spied for the Soviets for almost 2 years starting in 1975 at the age of 22. He stole highly classified documents from the Sensitive Compartmented Information Facility (SCIF) where he worked for the defense contractor TRW and handed them to his friend, Andrew Daulton Lee. Lee traveled to embassies abroad and sold them to the Soviets. In August 1977, Boyce was convicted of espionage and sentenced to 40 years in prison. In April 1985, an invitation broke his prison monotony when he was asked to testify before a Senate subcommittee investigating federal government security clearance programs (Lindsey, 1979; Serrano, 2003). Boyce detailed for the subcommittee the numerous security flaws and violations in his workplace and his recommendations for improvements. He then told the Senators what it was like for him to already be a spy for the KGB while he sat in his company's security briefings:

[The briefer] stood there entertaining all those naïve, impressionable youngsters around me with tales of secret adventure, intrigue, huge payoffs, exotic weaponry, seduction, poisons, hair-raising risks, deadly gadgetry. It was a whole potpourri of James Bond lunacy, when, in

---

<sup>29</sup> Almost 60% of American spies who began espionage since 1990 were volunteers.

## ELEMENTS OF CLASSIC ESPIONAGE

fact, almost everything he said was totally foreign to what was actually happening to me.

Where was the despair? Where were the sweaty palms and shaky hands? This man said nothing about having to wake up in the morning with the gut-gripping fear before steeling yourself once again for the ordeal of going back into that vault... None of them knew, as I did, that there was no excitement; there was no thrill. There was only depression and a hopeless enslavement to an inhuman, uncaring foreign bureaucracy. I hadn't made myself count for something. I had made my freedom count for nothing (United States Senate Committee on Governmental Affairs, 1985).

Yet after Boyce made his public statement in 1985, at least 97 additional Americans attempted espionage or espionage-related crimes against the United States. One who tried it was Glenn Duffie Shriver.

Shriver attracted the attention of Chinese intelligence agents seeking to recruit Americans who could be groomed to access classified information in the United States. Their approach and cultivation of Shriver illustrates a common element of classic espionage, recruiting the agent.

Shriver was interested in China. He spent parts of his college years at various Chinese study abroad programs in Shanghai, and after he graduated in 2004 he returned to China, proficient in Mandarin, to look for work. In October of that year he answered an English-language advertisement looking for people to write "political papers." (This was the same innocuous-sounding gambit used by Tai-Shen Kuo at the beginning of his efforts to recruit James Fondren, Jr.). Shriver submitted a paper on relations between China, North Korea, and Taiwan to a woman named Amanda, who told him the paper was good. She asked if he would like to meet some other Chinese friends. These turned out to be Mr. Wu and Mr. Tang, and the four of them met many times to get acquainted. The two men were curious about Shriver's career plans—had he considered applying for a job with the federal government, perhaps in law enforcement or diplomacy? Although he recognized a subtext of recruitment, one day Shriver asked them bluntly what they wanted, and he received an equally forthright answer: "If it's possible, we want you to get us some secrets or classified information," the friendly Chinese men replied (United States District Court for the Eastern District of Virginia, "Statement of Facts", 2010; Wise, 2012).

Shriver agreed to try to get a job that would provide him with access to the kind of information the Chinese wanted. He applied to the Department of State (DoS) and took the Foreign Service examination twice, but failed it in 2005 and again in 2006. Each time he took the test, the Chinese paid him for his trouble: \$10,000 the first time, and \$20,000 the second. In 2007, he applied online to work for the Central Intelligence Agency (CIA) in their clandestine unit—to become a CIA spy—and he requested payment from the Chinese. Later that year he visited China again, and

his friends gave him the additional \$40,000 in cash he asked for. While he waited on the CIA's processing for several years, he worked other jobs, including supplying tattoo shops in Los Angeles and teaching English in South Korea. At some point during this period, he began to use the email codename "Du Fei," a play on his middle name "Duffie," indicating with this bit of subterfuge that he was well aware that he was slipping into the orbit of espionage. In late 2009, the CIA did invite him to Washington, DC for interviews and the supposedly final job processing. These took place in early May and June 2010 (Wise, 2012).

On June 21, 2010, as he boarded a plane to fly back to his job in South Korea, Shriver was arrested and charged with 5 counts of making false statements. In his CIA application he had lied about having had any contact with foreign representatives during the previous 7 years, and about his travel to China in 2007 and, of course, about the \$70,000 he had taken from them so far (United States District Court for the Eastern District of Virginia, "Statement of Facts," 2010; Wise, 2012).

In October 2010, after interviews with the Federal Bureau of Investigation (FBI), Shriver was charged in a plea bargain with one count of willfully conspiring with others, known and unknown, to obtain lawful possession of, access to, and control over documents and information relating to the national defense, which information the defendant would have reason to believe could be used to the injury of the United States and to the advantage of a foreign power, and thereafter to communicate, deliver, and transmit said documents and information to a person not entitled to receive it.<sup>30</sup> He pled guilty, agreed to cooperate in debriefings, and was sentenced to 48 months (4 years) in prison (United States District Court for the Eastern District of Virginia, "Plea Agreement," 2010). He never saw a classified document or gained access to any classified information, and although not acknowledged, it is likely that the CIA saw through his lies well before the interviews and the polygraph exam (Wise, 2012). Shriver was naïve, but he was also greedy, and with his eyes open he allowed himself to be recruited as an agent of China, expecting that he would be able to send the Chinese "some secrets" as soon as he could get a job with access.

Shriver's case was an attempt at classic espionage. It was also an unusually bold effort by China's Ministry of State Security, the foreign intelligence agency, to groom and plant an American agent in the CIA to work for them. It illustrates many of the elements of classic espionage that were outlined earlier, including:

- A context of competition. The United States and the People's Republic of China are in a vigorous if not always open international, economic, and geopolitical contest.

---

<sup>30</sup> This reflects the language in Title 18 U.S.C. sections 793(d) and 793(g).

## ELEMENTS OF CLASSIC ESPIONAGE

- Secret, clandestine actions. Shriver lied on federal application forms, smuggled cash payments back into the United States from China, and agreed to collect and transmit information to a foreign power in exchange for payment.
- Secrets. The Chinese intelligence service agents he met with were open with Shriver about their goal that he should collect secrets for them, and he was open with them about his attempts to get a job with classified access to obtain secrets.
- Political, military, or economic secrets. By encouraging Shriver to apply to the Department of State and to the CIA, the Chinese agents demonstrated that they wanted diplomatic or intelligence insights.
- Theft. Shriver was prevented from the theft of secrets that he intended by being caught before he gained access to them.
- Subterfuge and surveillance. By being apprehended, Shriver was also prevented from exercising his tradecraft.
- Illegality. Shriver was convicted under two subsections of Title 18 U.S.C 793, one of the two most commonly applied Espionage statutes.
- Psychological toll. Although he was not yet in a position to damage American interests, Shriver felt he had suffered from the attempt. At his sentencing he said: “By the time I came to realize I was in this situation, it was too late... I cannot tell you what it’s like to carry a dark secret like this for so many years” (Baracat, 2011).

About the same time that Glenn Shriver was taking and failing the Foreign Service examination in 2004 and 2005, a young U.S. Navy enlisted man was similarly embarking on a quixotic career as a spy. As Ariel Weinmann had approached his high school graduation in 2003, he had a steady girlfriend whom he wished to marry, but her parents opposed a possible son-in-law who intended to join the military. Leaving his girl behind but secretly engaged to her, he did join the Navy in 2003. He explained he was “looking for an adventure and I guess a degree of honor, something to make my life meaningful.” He applied for a linguist rating but failed the tests, and became a submariner instead. He deployed as a Fire Control Technician 3<sup>rd</sup> Class on his first submarine in 2004 (McGlone, 2006).

Weinmann soon found that he disliked many aspects of life on the sub, such as the fierce competition, the corruption in the petty bribery and favoritism he observed, and the inefficiency in the simplest activities. Slightings and setbacks upset him and they built into a simmering resentment against the Navy. His setbacks were real enough: when the sub returned to port, he drew orders to stand guard on the deck and thus missed his first homecoming port celebration, which he bitterly resented. The first time he and his fiancée met once he got home to Salem, OR, she handed back his engagement ring, broke off their relationship, and announced that her parents were sending her to college in Switzerland so she would be far away from him (Amos, 2006).

His response demonstrated the immaturity of a 22-year-old, but also his impulsiveness. On the spot, he began to think about how to desert the Navy and move to Austria, where he could use his fluent German, to be close to his girlfriend in Switzerland and try to win her back. Before he left the sub to desert, on July 1, 2005, he stole a laptop and downloaded classified files onto it, including biographical compilations about 29 Austrians and technical manuals for the sub's Tomahawk cruise missile system. He intended to barter this information for expedited asylum in Austria. He took his passport, his life savings, and a one-way ticket and boarded a plane for a series of flights that would take him to Vienna. (Amos, 2006).

When Austrian officials at the airport would not consider his request for expedited asylum, Weinmann settled into Vienna, drifting around waiting to hear from his girl, who did not call. He took up with a group of young Socialists meeting in a park, including some Russians, and they became friends. Dropping the girl along with the notion of asylum in Austria, he decided to move to Russia, and in order to do that, he entered the Russian embassy in Vienna with a print-out of one of the manuals he had stolen. He handed the manual to the embassy officer, but then left with only his promise that the embassy would be in touch—without securing the quid pro quo he sought: Russian citizenship, a train ticket, and admission to a Russian university in trade for his information. Realizing after he left that he had given away his only leverage, he next decided that instead of just moving there, he would defect to Russia and live there permanently. He prepared to leave Vienna by smashing the hard drive of the laptop to destroy the evidence of what he had downloaded (McGlone, 2006).

On a series of flights on his way to Russia, Weinmann first flew to Mexico City. Sources are ambiguous as to whether he may have tried to sell classified information there. He also tried to arrange to be smuggled across the border into the United States, but he did not have enough money to pay a coyote (a smuggler of people) to take him. When a customs officer noticed his name on a warrant for military deserters, he was arrested as he landed at the Dallas-Fort Worth airport. After an international counterintelligence investigation that took months, he pled guilty to desertion, failure to obey a general order, espionage, copying classified information, larceny, and destruction of military property (Wiltrout, 2006b). Two additional counts of espionage were dropped. The military court sentenced Weinmann to 25 years in prison, reduction in rank to E-1, forfeiture of all pay and allowances, and a dishonorable discharge, but in a plea bargain, he would be serving only 12 years, and would be eligible for parole in 4 (White, 2006; Amos, 2006).

Weinmann was not a very savvy spy. In 2005 and 2006, he was still young and inept. Yet he was persistent and audacious, and he managed to steal classified information on a current weapons system and turn it over to a rival foreign power without being identified or stopped. Compared to the long-running espionage activities with major consequence of John Walker, Robert Hanssen, or Aldrich

## ELEMENTS OF CLASSIC ESPIONAGE

Ames, Weinmann's case was probably minor, yet it demonstrates the elements of classic espionage:

- A context of competition. The United States and Russia have been major adversaries first in the Cold War and since then in a geopolitical and military contest that has waxed and waned for several decades.
- Secret, clandestine actions. Weinmann surreptitiously downloaded classified files from the Secure Internet Protocol Network while on his submarine. He planned to desert the Navy and use the information to his advantage by trading it to the Russians.
- Secrets. The manuals for the Tomahawk missile system and the biographies that he downloaded were classified Secret.
- Political, military, or economic secrets. Weinmann downloaded the manuals because they could be attractive to an adversary in a confrontation, when they could provide a military advantage to a foreign power. He meant the classified biographies of Austrians to be useful as a bargaining chip for expedited asylum in his original scheme to settle in Austria.
- Theft. Weinmann stole a laptop computer from the sub, onto which he downloaded Secret files that he also stole.
- Subterfuge and surveillance. Weinmann had to be covert as he stole the laptop, and he tried to be unobtrusive in his international movements by taking a series of flights on his way to his actual destinations. He flew to Chicago and then to Warsaw, Poland, before he landed in Vienna, and when he decided to defect to Russia, he first flew to Mexico City and then attempted to travel to Vancouver, Canada through Dallas.
- Illegality. Weinmann was charged and pled guilty to Articles 85 (desertion), 92 (failure to obey an order or regulation), 106a (espionage), and 134 (general activity that prejudices good order and discipline of the service) of the Uniform Code of Military Justice (U.S. Fleet Forces Command, 2006).
- Psychological toll. After his arrest, the Navy held Weinmann for 4 months during his investigation, and he was not in contact with anyone who could report publicly on his state of mind (Wiltrott, 2006a). He is not reported to have made a statement at his sentencing, so his psychological status as he left for prison is undocumented.

### Classification and Legal Dimensions of Classic Espionage

Most classic espionage cases involve classified information, since by definition this is supposed to be the most sensitive, valuable, and important of a nation's information. If it were compromised, classified information by definition would damage the United States to various degrees: the loss of Confidential information is defined as causing damage to national security; Secret information is defined as causing grave damage to national security; and Top Secret information is defined as causing exceptionally grave damage (Executive Order 13526). Of the 209

individuals under consideration in this report, 186 persons, or 89% of the total, are coded as committing classic espionage, either because what they did was in the classic pattern alone or because it is described as classic plus one other type.

Table 14 reports the clearance status at the start of their classic espionage of the 186 individuals in this study who held security clearances. It shows that 88% of the persons committing classic espionage had access to classified information.<sup>31</sup> This includes the 134 persons who held clearances at the start of their espionage, plus the 10 who used their former clearances in their espionage, and the 20 who used an accomplice’s access to classified information.

**Table 14**  
**Security Clearance Status at Start of Classic Espionage**

<b>Security Clearance</b>	<b>n</b>	<b>%</b>
Total persons in this study	209	100
Persons coded as committing classic espionage	186	89
Of 186 persons who committed classic espionage,		
Number holding security clearances at start of espionage	134	72
Number using their former security clearances at start	10	5
Number using the access of an accomplice	20	11
Total classic spies with access to classified information	164	88
Number who held no security clearance, e.g., stole information	13	7
Number for whom security clearance status is unknown	9	5

Access to classified information is a grant of legal as well as moral trust. Three elements are required in order to grant eligibility for a security clearance and to receive access to classified information: (1) a person must demonstrate eligibility in a personnel security process that includes a background investigation and an adjudicative decision based on that investigation performed under the authority of a government agency head, who then becomes the sponsor of that clearance; (2) the person must sign a nondisclosure agreement that legally binds the clearance holder in a contract to uphold the security requirements that apply to the information to which he or she has access; and (3) a person must have a need to know specific classified information, as determined by the local agency holding that information

<sup>31</sup> These figures refer only to classic espionage, a subset (186) of the total (209). The discussion earlier in this report of employment and clearance includes all 209 of the individuals. Therefore these figures differ from those in that earlier section.

## ELEMENTS OF CLASSIC ESPIONAGE

(Executive Order 13526). The 144 individuals being considered here who held or previously held access to classified information but betrayed the trust invested in them broke the legal contract they signed in their nondisclosure agreements. For persons who held clearances, many criminal complaints for espionage begin by referring to their signature on this legal promise not to disclose the information. It becomes one of the bases for prosecution.

Table 14 shows that 20 individuals in classic espionage cases who did not themselves hold security clearances were accomplices of someone else who did have access to classified information. Most of these 20 accomplices were discussed in Table 4 (several other accomplices in Table 4 were not part of a classic espionage case and therefore are not included here). The clearance status for another 9 individuals in the classic espionage group is unknown. Another 13 persons did not hold security clearances or access to classified information, and these constitute only 7% of the classic espionage cases. Several of those without clearances or former clearances stole information; others attempted classic espionage without current access (several were applying for or planning to secure clearances); and some passed information that was not classified but was based on surveillance.

Classification of information has not always been a requirement of espionage. The laws on espionage date from the early 20th century and they have evolved in a process more like accretion than revision, with new layers laid upon existing layers. The statutes governing espionage date from 1911 with passage of the Defense Secrets Act, which was the first law aimed at protecting the government's secrets. As the United States entered World War I, Congress enacted the Espionage Act in June 1917. This adopted the approach that had been taken in 1911 and incorporated many of its key phrases—which means that the statutes based on the 1917 act that are now in use and little revised are more than 100 years old (Elsea, 2013).

The series of provisions based on the Espionage Act are found in Title 18 U.S.C. section 792 through 798. Two of the sections most frequently used in espionage prosecutions are section 793, "Gathering, transmitting, or losing defense information," and section 794, "Gathering or delivering defense information to aid foreign governments."

Section 793 makes it a crime to disclose or attempt to disclose to "unauthorized persons" "national defense information" "with intent or reason to believe that the information is to be used to the injury of the United States or to the advantage of any foreign nation." It does not mention classified information, since classification of information did not exist in 1917 and was not introduced and standardized until World War II, starting with an executive order in 1940. It also criminalizes gathering or losing national defense information, terms that add to the broad yet

vague problem with the statute. Penalties under section 793 include a fine and imprisonment for no more than 10 years (Elsea, 2006)<sup>32</sup>.

Section 794 proscribes passing national defense information to a foreign nation, or to any group within a foreign nation, “with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation.” Since it was written decades before transnational groups appeared on the international scene inflicting terrorism and other crimes, it does not specifically provide for such a contingency as the recipient of espionage being a transnational group. It treats conspirators who participate in the crime as equal to the actors who actually commit it. This provision is more serious than the previous section 793 because it involves passing national defense information “to aid foreign governments,” and so authorizes prison sentences of any length including life in prison or, if the crime resulted in the deaths of American covert agents or the compromise of major weapons systems including nuclear weapons, with a death sentence (Elsea, 2006)<sup>33</sup>.

As the early Cold War intensified during the late 1940s, and concerns about Soviet espionage grew, Congress passed a large and complicated piece of legislation, the Internal Security Act of 1950, which gave the espionage statutes the most thorough revision they have received. Three elements of the Act are important in this discussion. (1) This legislation added another section to the Espionage statutes inherited from the 1917 act. This became section 798, titled “Disclosure of Classified Information,” which was added to the existing series of statutes in Title 18. Section 798 does specifically refer to information that has been classified, but the section applies only to information relating to codes, ciphers, and intelligence communications systems. (2) The Internal Security Act also introduced in Title 50 of the U.S.C., a new section 783, titled “Communication of Classified Information by Government Officer or Employee,” which defined it a crime for “government officers or employees who, without proper authority, communicate classified information to a person whom the employee has reason to suspect is an agent or representative of a foreign government.” This provided a second section that protects classified information by name, but again, its scope is limited in both the type of information protected and the category of persons to whom it applies (Elsea, 2013). (3) The Act incorporated its third important revision to the espionage statutes by separating one subsection of 793 that dated from 1917 into two subsections, introducing new

---

<sup>32</sup> The following description of the statutes used to prosecute classic espionage is based on the excellent series of reports by legal scholar Jennifer Elsea for the Congressional Research Service (2006; 2013).

<sup>33</sup> Other sections in the Espionage Act series criminalize specific and antique actions, such as photographing installations from the windows of an airplane: section 792 concerns harboring or concealing foreign agents; section 795 punishes photographing and sketching defense installations; section 796 calls out the use of aircraft in photographing defense installations; section 797 punishes publication and sale of photographs of defense installations (Title 18 USC sections 792-798).

## ELEMENTS OF CLASSIC ESPIONAGE

ambiguities in the process. The new subsections, (d) and (e), are, according to the most careful students of espionage law, “undoubtedly the most confusing and complex of all the federal espionage statutes” (Edgar & Schmidt, Jr., 1973). In trying to distinguish between persons with lawful possession (subsection d) and those with unauthorized possession (subsection e) the revisers introduced differences in wording that required courts in subsequent cases to parse them word by word, often reaching differing results (Barandes, 2007).

These four laws, Title 18 U.S.C. sections 793, 794, and 798 and Title 50 U.S.C. section 783 are the four that are most frequently used to prosecute classic espionage. However, there are many other statutes that may also be applied, depending on the circumstances of the crime and the nature of the evidence available. Other statutes commonly used include:

- 18 U.S.C. section 952, which punishes employees of the United States who, without authorization, willfully publish or furnish to another any official diplomatic code or material prepared in such a code, or coded materials in transmission between a foreign government and a United States diplomatic mission, with a fine or a prison sentence of up to 10 years, or both.
- 18 U.S.C. section 1030(a)(1) punishes the willful retention, communication, or transmission, of classified information retrieved by means of knowingly accessing a computer without (or in excess of) authorization, with reason to believe that such information could be used to injure the United States or aid a foreign government. This provision also imposes a fine or imprisonment for not more than 10 years, or both.
- 18 U.S.C. section 1924 prohibits the unauthorized removal of classified material. It applies to government officers or employees who “knowingly take material classified pursuant to government regulations with the intent of retaining the materials at an unauthorized location,” and it imposes a fine of up to \$1,000 and a prison term of up to 1 year.
- 18 U.S.C. section 641 punishes the theft or conversion of government property or records for one’s own use or the use of another. It does not explicitly prohibit disclosure of classified information, yet it has been used in such cases. Violators may be fined or imprisoned for not more than 10 years, or both.
- 42 U.S.C. section 2274 punishes the unauthorized communication by anyone of “Restricted Data,” that is, data dealing with nuclear weapons or systems, or an attempt or conspiracy to communicate such data. If done with the intent of injuring the United States or in order to secure an advantage to a foreign nation, it calls for a fine of not more than \$500,000, a maximum sentence of life in prison, or both. Other provisions punish with lesser sentences attempts or conspiracies to disclose such data.
- 50 U.S.C. section 421 protects information concerning the identity of covert intelligence agents. Intentional disclosure, learning the identity through exposure to classified information and revealing it, or learning the identity

through a “pattern of activities intended to identify and expose covert agents” is subject to prison sentences of varying lengths from 3 to 10 years, and fines. “To be convicted, a violator must have knowledge that the information identifies a covert agent whose identity the United States is taking affirmative measures to conceal. An agent is not punishable under this provision for revealing his or her own identity, and it is a defense to prosecution if the United States has already publicly disclosed the identity of the agent” (Elsea, 2006).

Critics argue that the current espionage statutes are both too sweeping and general in scope, yet at the same time apply too specifically to technologies of the past, so that they cannot cover the new permutations to espionage that have developed in recent decades. They urge reforms (Vladeck, 2010). It is a real legal challenge to prosecute someone for espionage in the United States because of the inconsistencies and gaps in the statutes that are available (Bowman, 1995; Roth, 2001). Illustrating that challenge, the Counterespionage Section of the Department of Justice describes itself on its website as “providing legal advice on all matters within its area of responsibility, which includes 88 federal statutes affecting national security” (United States Department of Justice, Counterespionage/Counter Proliferation, 2015).

Of the 186 individuals described in Table 14 as committing classic espionage, 140 were charged, among other offenses, with one of the four main espionage statutes discussed earlier, that is, U.S.C. Title 18 sections 793, 794, and 798 and Title 50 section 783. Another 21 persons were charged under the Uniform Code of Military Justice either under article 106a (espionage), or article 106 (spies).

The remaining 25 individuals were charged under an array of statutes—often more than one—that are related to the activities of espionage, including<sup>34</sup>: Title 18 section 2071 (concealing, mutilating, or destroying government records); section 1001(a) (making false statements to a government official); section 1030 (willful retention, communication, or transmission of protected information obtained by accessing a government computer); section 1924 (unauthorized removal of classified information by government employees, contractors, or consultants); section 641 (theft or conversion of government property for one’s own use or the use of another); under Title 50, section 421(a) (disclosing information that identifies a covert agent); and under the Uniform Code of Military Justice, article 81 (conspiracy, in this case, conspiracy to communicate classified information to a foreign agent); article 92 (failure to obey lawful orders or regulations); article 85 (desertion); article 134 (general provisions, in this case, copying and attempting to deliver classified information to a person not authorized to receive it); article 108 (selling government property); and under the Atomic Energy Act, Title 42, section 2274 (communication of Restricted Data) (Elsea, 2013; United States Department of Justice, Criminal

---

<sup>34</sup> The list that follows are the most commonly used statutes but is not exhaustive of the various statutes charged in classic espionage cases.

## **ELEMENTS OF CLASSIC ESPIONAGE**

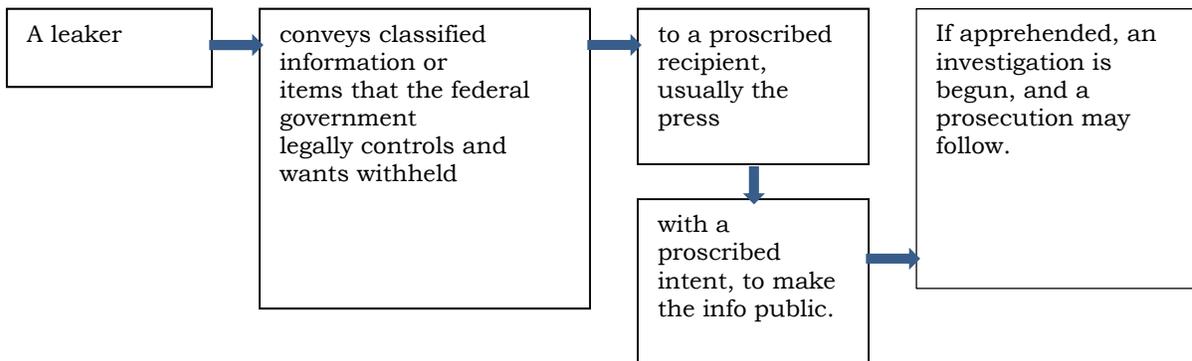
Resource Manual, 2015; United States Department of Justice, Counterespionage/Counter Proliferation, 2015; Uniform Code of Military Justice, 2015).

Of course, being charged with various crimes is only an early step toward being convicted of them. The 209 individuals under study in this report, and specifically the 186 persons in classic espionage cases, were convicted of one or more espionage-related crimes, though sometimes they were not convicted of the core espionage statutes. Plea bargains, good defenses, and the lack of robust evidence to prove the most severe charges have often led to convictions and sentences that were reduced from the initial charges.

**LEAKS AS A TYPE OF ESPIONAGE**

Leaks are disclosures of classified information to the public. They are usually accomplished through the press or by publication in books or other print media, and recently, also in blogs and social media. The form of a leak follows the form of classic espionage except that the recipient is different. Instead of being given to an agent of a foreign power or transnational adversary, leaks go out to the American public and then, through modern communication channels, immediately out to the rest of the world as the information is re-published, translated, and the fact of the leak is explored in further press coverage. Both the content of the information and the fact that this particular information is no longer controlled are made available to anyone, including adversaries who systematically monitor the American press for insights<sup>35</sup>.

The general model of espionage elements that was introduced earlier in the discussion of classic espionage applies to leaks as well.



**Figure 5 Leaks in a Model of Espionage Elements**

The proscribed recipient of a leak, the person “not authorized to receive it” in the language of the Espionage statutes, is anyone who does not have the eligibility for a security clearance, the grant of access, and the need to know the classified information in the leak. Often the proscribed intent of the leaker is to make the information public in order to achieve a policy outcome or a personal goal the

<sup>35</sup> Department of Defense, *DoD Information Security Program: Protection of Classified Information, Glossary*, Manual 5200.01-Volume 3, Enclosure 6, February 24, 2012a (as amended) defines an “unauthorized disclosure” as “communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.” Three levels of security incidents related to unauthorized disclosures are differentiated: 1) Infractions, defined as a failure to comply with requirements that does not result in loss or compromise; 2) Violations: security incidents that indicate knowing, willful, and negligent action that does or could result in loss or compromise; and 3) Compromise: security violation in which there is an unauthorized disclosure of classified information (where the recipient does not have a valid clearance, authorized access, or need to know). Loss is defined as a condition in which classified information cannot be physically located or accounted for. (Summarized in Bruce & Jameson, 2013). The federal government considers classified information that has been made public to continue to be classified.

## LEAKS AS A TYPE OF ESPIONAGE

perpetrator wants and cannot get while the information remains controlled. However, there are a variety of motivations for recent leaks and it is instructive to compare them.

Leaks are a controversial phenomenon. Since the releases of classified information by Bradley (Chelsea) Manning in 2010 and Edward Snowden in 2013, the impact and implications of those leaks and of all leaks has been widely debated<sup>36</sup>. Leaks are quite common, and trying to plug leaks has also been common. For example, between 2005 and 2009, 153 cases were referred to the Department of Justice (DoJ), which opened 26 cases and identified 14 suspects, yet not one led to an indictment (LaFraniere, 2013; Harris, 2010). Starting in the administration of President Barack Obama, who personally expressed a hatred for leaks, the U.S. Attorney General has prosecuted roughly a dozen individuals, thus prosecuting more leaks than in all the previous decades since 1945. This stepped-up prosecution, and the aggressive use of mining electronic records that has enabled them, makes this Administration's new legal approach controversial (Lichtblau & Risen, 2009; Harris, 2010).

Some argue these prosecutions can be unfair because leaks of classified information are a common currency in the relationship between reporters and government officials. They point to quantifications showing that annually there are hundreds of leaks from the government, many of them originating with the government, so why should a few individuals be singled out for punishment while most go free. Some of these "normal" leaks may be trial balloons of policies or efforts to shape public perceptions before a competing policy becomes known. Others may serve the personal aggrandizement of the leaker, or simply reflect carelessness or callous disregard for security regulations (Caplan, 2013; Benkler, 2014).

The point of such arguments often is that on balance, leaks can serve democratic governance, in their way, by preventing absolute government secrecy, which can wander astray without the corrective of debate among various points of view. The prosecutions and prison sentences for recent leaks seem to persons who argue in this way to endanger the mechanism of leaking itself, which to them is necessary to check government overreach. In this view, leakers are often whistleblowers who show courage and initiative by revealing information they decide needs to be made public (Prepared statement of Gabriel Schoenfeld, 2010).

---

<sup>36</sup> Many scholarly articles and book-length treatments of issues that have been provoked by the increased prosecutions of leaks have been published in the last 5 years. An admirably comprehensive article on legal, philosophical, and practical considerations of leaking classified information is David E. Pozen, "The leaky leviathan: Why the government condemns and condones unlawful disclosures of information," *Harvard Law Review*, December 2013, 127(2), 513-635. Another useful and full discussion is by Gary Ross, "Who watches the watchmen? The conflict between national security and freedom of the press," Washington, DC: National Defense University, 2011.

On the other hand, others support prosecution for leaks of classified information and hope it will lead to drying up leaks because, by definition, classified information was classified for a reason that involves national security, and releasing it without authorization by the classifying authority endangers that national security. The foreign policies of the nation and its relationships with other nations, the weapons systems the nation depends on for its defense, the intelligence collected on other nations and the people who collect it, the strategies and plans the nation holds for the future—elements of all these and many others vital to national life have been leaked away. People who argue for the strict prosecution of leaks emphasize the harm they have done and can do. To these commentators, leakers put their personal moral judgment above their legal responsibilities to comply with the rules on classified information that they agreed to, and therefore are more like miscreants, or even traitors, than they are whistleblowers (Bruce, 2002; Wittes, 2014).

The problems of over classification, that is, classifying information at a higher level than warranted, and the classification of too much information, buttress those who argue for value from leaks and against criminalizing the acts of leakers. If what is claimed to be highly sensitive information that requires control using all the safeguards of the classification system turns out in fact to be readily available open source information, or agency gossip, or self-serving protection for poor agency decisions, then faith in the system is undermined and leaks look more justifiable. “When everything is classified,” Justice Potter Stewart wrote in the Pentagon Papers decision in 1971, “then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion” (Quoted in Statement of Thomas Blanton, 2010). This is a thorny issue in the prosecution of leaks, since if the classified information leaked was not actually sensitive, the leaker may try to argue it was improperly classified. Deciding in a court case what was properly classified and what was not is another contentious dimension of leaks (Smith, 2010; Caplan, 2015).

A further element in the controversy over leaks is the tension between the need for government secrets and the First Amendment to the U.S. Constitution’s protection of freedom of the press. Not all leaks go to the press, but many do. The first action in a leak is that of the person with access to classified information who transmits it to someone not authorized to receive it, likely the press; usually, the second act is the publication of that information in public media. Defenders of the rights of the press argue passionately for minimal restrictions and maximal trust in the judgment of the press not to release information that is truly damaging. Those who wish to curtail leaks argue instead that the press also should come under legal sanctions when, ignoring its classification, they publish sensitive information that does do damage—even if they do not realize it (Reporters Committee for Freedom of the Press, in Bruce, 2002).

## **LEAKS AS A TYPE OF ESPIONAGE**

This brief overview demonstrates that the issues fueling controversy over leaks of classified information express deeply held legal and political differences that will not be completely resolved, but could be rebalanced, especially if calls for a reform of the Espionage statutes bear fruit. Many commentators point to ambiguities in the laws as foundational to the argument about leaks.

Among the 209 cases under study here there are seven individuals prosecuted for leaks. Edward Snowden is also discussed here briefly, although he is not included in the study since he has not been tried or convicted of a crime. A summary of their cases is presented in Table 15.

**Table 15**  
**Leaks**

	<b>Name/Age</b>	<b>Arrest Date</b>	<b>Employed by</b>	<b>Info Transmitted to</b>	<b>Type of Information</b>
1	Lawrence Franklin Age 52	2005	DoD OSD, International Security Affairs, civilian employee	Steven Rosen and Keith Weissman, lobbyists for AIPAC	Classified information on Iran and Iraq
2	Matthew Diaz Age 41	2006	U.S. Navy, Judge Adjutant General Corps	Barbara Olshansky, attorney with the Center for Constitutional Rights, a NYC nonprofit for legal rights	Names of all the detainees at Guantanamo Bay, Cuba, detention center
3	Shamai Leibowitz Age 39	2009	FBI, as a contractor	Richard Silverstein, an Internet blogger	FBI embassy transcripts on U.S. intelligence on Israel
4	Pfc. Bradley (Chelsea) Manning Age 22	2010	U.S. Army	Julian Assange and the Wikileaks website	U.S. State Dept. cables; U.S. Army reports and videos from Iraq and Afghanistan wars
5	Steven Kim Age 42	2010	U.S. State Dept., as a contractor	James Rosen, a Fox News reporter	Intelligence reports, analysis on N. Korean nuclear plans
6	John Kiriakou Age 42	2012	Former CIA civilian employee	Scott Shane, a NYT reporter, and two other reporters	Identities of CIA intelligence officers; interrogation methods in use against terrorist suspects
7	Donald Sachtleben Age 51	2013	FBI, as a contractor	An Associated Press reporter	Details on explosives used by the “underwear bomber,” and FBI analysis of related bombings
8	Edward Snowden <sup>37</sup> Age 29	2013	NSA, as a contractor	Glenn Greenwald, a reporter for <i>The Guardian</i> , and Laura Poitras, a documentary filmmaker	Details of NSA domestic surveillance of communications, and U.K. and Israeli programs that were cooperating with NSA; ongoing revelations are continuing

<sup>37</sup> Although he is discussed here, Edward Snowden is not included as a case in the data of this report because he remains in Russia and, although he has been charged, he has not been tried or convicted of a crime. He is listed in this table as a sort of placeholder. He is discussed only briefly in this report because he has talked openly about his actions, they are already widely reported and studied, and they have had an important impact on information security and the prosecution of leaks.

## LEAKS AS A TYPE OF ESPIONAGE

Five of the seven instances of leaks included in this study involved giving classified information to a member of the press, one person gave classified information to two lobbyists for the American Israel Public Affairs Committee (AIPAC), and one person sent the names of detainees held at Guantanamo Bay, Cuba to a legal rights firm in New York City. Each of these cases illustrates distinctive aspects of the motives and circumstances that lead to a leak and each will be considered here in some depth.

### **Shamai Leibowitz**

Shamai Leibowitz, a lawyer with dual American and Israeli citizenship, moved to Silver Spring, MD, in 2004. He worked for the Department of State teaching Israeli law and culture to diplomats for several years, and also for the Department of Defense Language Institute. From January to August 2009, he worked as a contract Hebrew linguist for the FBI, where he held a Top Secret security clearance. A blogger himself on topics of political activism and moral and religious issues, in April 2009, Leibowitz shared with another blogger and friend, Richard Silverstein, some 200 pages of classified transcripts from FBI wiretaps of conversations that took place inside the Israeli Embassy in Washington, DC. While not a surprise that the FBI monitors communications of Israel, a close American ally, as it does other embassies, it is a sensitive practice that the FBI would prefer not be discussed in the press. Silverstein then used some of the material from Leibowitz in his own online publication. The FBI began investigating Leibowitz soon after the leak in the summer of 2009, and on December 17, 2009, he pled guilty to one count of violating Title 18 U.S.C section 798, providing communications intelligence to a person not authorized to receive it. In May 2010, he was sentenced to 20 months in prison, but the court granted him 60 days to prepare to leave his dependent family (Kredo, 2010; Glod, 2010; Shane, 2011b).

Leibowitz admitted that several concerns motivated his leak of the embassy transcripts to a fellow-blogger. One was his uneasiness with Israel's determined efforts to shape American public opinion and to lobby Congress, which he thought overreached. The second was his fear that, as reflected in the press of the time, Israel would attack Iran's nuclear facilities, thereby escalating an international crisis for the United States as well as for Israel. Based on the transcripts, Silverstein described in his blog telephone interactions between Israeli embassy officials and Jewish activists, members of Congress, and Administration officials that could have embarrassed them. When he realized the FBI was investigating Leibowitz in 2009, Silverstein burned the secret transcripts in his backyard and took the reports off his website, but he came forward publicly in 2011 to argue that Leibowitz had acted from a noble motive by trying to stop a rash attack on Iran. "I see him as an American patriot and a whistle blower, and I'd like his actions to be seen in that context," Silverstein told a reporter (Shane, 2011b). Leibowitz, on the other hand, wrote to the judge in May 2010

While working for the FBI, I came across information that troubled me very much and caused me to make a bad decision. I allowed my

idealism and misguided patriotism to get ahead of me... I made a mistake but only because I believed it was in the best interests of the American people (Kredo, 2010).

### **Stephen Jin-Woo Kim**

Like Shamai Leibowitz, Stephen Jin-Woo Kim, a nuclear proliferation specialist, was also working in 2009 as a federal contractor. Starting in 2008, he had been detailed to the DoS's Bureau of Verification, Compliance, and Implementation from his job at the Lawrence Livermore National Laboratory. Kim was a respected senior intelligence analyst. He had served as an adviser to various federal agencies on strategic nuclear deterrence, specializing in North Korea. Born in Seoul, South Korea, Kim immigrated to the United States with his family at the age of 8 and thrived, earning degrees from Georgetown, Harvard, and Yale. He became a naturalized American citizen. Ironically, he tended to avoid the press and expressed concern about press leaks to colleagues, but when a State Department public affairs officer asked Kim in March 2009 to talk about North Korea with James Rosen, a reporter for Fox News, the two struck up an acquaintance (Apuzzo, 2010; Hsu, 2010; Marimow, 2013).

On June 11, 2009, the same day a Central Intelligence Agency's (CIA) analysis on North Korea that was classified Top Secret-Sensitive Compartmented Information (TS-SCI) was released to only 95 specified analysts, including Kim, James Rosen reported in an Internet article that "the Central Intelligence Agency has learned, through sources inside North Korea," that the North Koreans would respond to a United Nations Security Council resolution condemning North Korea for its nuclear and ballistic missile tests by launching another nuclear test, reprocessing their spent fuel, speeding up their uranium enrichment, and launching an intercontinental ballistic missile (Shane, 2011b; Pincus, 2013). The leak's reference to CIA sources and methods that had been used to obtain intelligence inside North Korea incensed the CIA. Kim was investigated, questioned by the FBI, and indicted late in August 2010, when he was charged with Title 18 section 793(d), disclosing national defense information to a person not authorized to receive it, and Title 18, section 1001(a)(2), lying to federal officials, the FBI (Apuzzo, 2010; Hsu, 2010; Marimow, 2013).

An affidavit supporting a request for a search warrant of May 28, 2010, demonstrates that the DoJ investigators had already pulled together electronic and communications records to startling effect. Rosen was working from a press office in the DoS building where Kim also worked in a secured section. The investigators correlated security badge access and egress records with Kim's office desk telephone calls, office computer files, and emails to Rosen's cell phone and office desk phone, emails of all Rosen's interactions with Kim, and finally, a late-night search of Kim's office. From these data, they reconstructed a detailed timeline of a developing relationship between the reporter and the analyst over the months between March and June, 2009 (Marimow, 2013; United States District Court for

## LEAKS AS A TYPE OF ESPIONAGE

the District of Columbia, Affidavit, 2010). The affidavit documented the dates, times, and durations of calls between Kim and Rosen and who initiated the call, dates and times for when each man left the building and when he returned, and incriminating emails illustrating how Rosen made Kim a source. Both men showed they were aware their interaction was potentially sensitive. At Rosen's suggestion, Kim agreed to refer to Rosen in emails with the codename "Alex," and to respond to the codename "Leo Grace" in return. They emailed one another using coded signals on Rosen's Google account: one asterisk meant proceed with a communication plan, two meant hold off (Marimow, 2013; United States District Court for the District of Columbia, Affidavit, 2010.)<sup>38</sup>

This affidavit quotes an email from Rosen to Kim on May 22, 2009, which gives insight into Rosen's persuasiveness and his goals, including

"Thanks, Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors. I want to report authoritatively, and ahead of my competitors, on new initiatives or shifts in U.S. policy, events on the ground in [North Korea], *what intelligence is picking up*, etc. ...I'd love to see some *internal State Department analyses* about the state of [North Korea].... In short: Let's break some news, and expose some muddle-headed policy when we see it—or force the administration's hand to go in the right direction, if possible. The only way to do this is to EXPOSE the policy, *or what [North Korea] is up to*, and the only way to do that authoritatively is with *EVIDENCE*" (United States District Court for the District of Columbia, Affidavit, 2010.)  
[Capitals are in the original and italics are in the original where they were meant to denote potentially classified information, now declassified.]

---

<sup>38</sup> DOJ investigators stepped around the law in order to gain access to Rosen's emails in submitting a successful search warrant from them. A news report notes that "Privacy protections limit searching or seizing a reporter's work, but not when there is evidence that the journalist broke the law against unauthorized leaks. [In the Kim case], a federal judge signed off on the search warrant" after the FBI claimed that the evidence suggested that Rosen had also broken the law, "at the very least, either as an aider, abettor and/or co-conspirator" (Marimow, 2013). The DOJ later admitted they had never intended to prosecute Rosen—but had only claimed as much to portray him as a potential co-conspirator in order to get the search warrant and access to his emails with Kim. In July 2013, the U.S. Attorney General published new guidelines on leak investigations. "The new rules forbid the portraying of a reporter as a co-conspirator in a criminal leak as a way to get around the legal bar on search warrants for reporting materials" (Savage, 2013a; Savage, 2014). The possibility of prosecuting a reporter (Rosen) for receiving a leak of classified information (from Kim), which has never been done, caused an outcry from defenders of the freedom of the press, who argued that in order to gather information in the course of their doing their jobs as national security reporters, they need to be able to discuss issues and receive information from officials in grey areas of classification and attribution. Lawyers for Kim argued that the Department should drop the case or the judge should dismiss it, since Rosen's email records could not have been accessed under the new guidelines, but the DOJ refused and the judge refused to dismiss it on grounds the guidelines were only advisory and discretion remained (Marimow & Leonnig, 2013).

On March 29, 2010, in a second interview with the FBI, Kim tried to explain himself to the FBI as they laid out their timeline to him; he also tried to claim that he did not have an ongoing relationship with Rosen, nor was he the source of the leak. In FBI notes of the interview, Kim is quoted as saying

“I did not purposely discuss the [Intelligence Report], but might have discussed [some of the topics discussed in the Report].”

“Maybe I inadvertently confirmed something...too stubborn to not...[I] just don't know...someone values my views, listens up...maybe I felt flattered. [The Reporter] is a very affable, very convincing, persistent person. [The Reporter] would tell me I was brilliant and it is possible I succumbed to flattery without knowing it. Maybe it was my vanity. [The Reporter] considers me an expert and would tell me...could use my insight....The IC is a big macho game but I would never say I'm read in to this and you are not. I would never pass [the Reporter] classified.”

“[The Reporter] exploited my vanity.”

“My personal and professional training told me not to meet people like [the Reporter]. I felt like while on the phone I was only confirming what he already knew. I was exploited like a rag doll. [The Reporter] asked me a lot of questions and got me to talk to him and have phone conversations with him. [The reporter] asked me a lot, not just specific questions. [The Reporter] asked me how nuclear weapons worked.”... [United States District Court for the District of Columbia, Affidavit, 2010.] [Bracketed elements are in the original transcript of notes.]

Early in February 2014, Kim pled guilty to leaking classified information to James Rosen and to lying about it to the FBI. He signed a statement saying he was not a whistle blower. In early April, he was sentenced to 13 months in prison. At the sentencing hearing, his defense argued that his interactions with Rosen were the normal conversations between government officials with reporters, and “many of those conversations include the disclosure of classified information.” The prosecutor countered that the “everyone-does-it argument” was not an excuse, and instead, Kim “was motivated not by an altruistic purpose but by his own ego and desire for professional advancement” (Marimow, 2014).

### **John Kiriakou**

Actions in 2008 and 2009 (which was the time frame for both Leibowitz's and Kim's leaks) also led to John Kiriakou's eventual prosecution for leaking classified information. Kiriakou had served with the CIA as a case officer and counterterrorism specialist from 1990 through 2004, at which point he retired. His CIA career had been eventful—he published a memoir of his experiences—and it included recruiting agents in Athens while dodging assassination attempts there, and assisting in the capture of Abu Zubaydah in Pakistan. He moved from the

## LEAKS AS A TYPE OF ESPIONAGE

Agency to working for Deloitte in corporate intelligence, and he also consulted on movies that had intelligence or terrorism themes (Coll, 2013).

In December 2007, Kiriakou agreed to give a taped television interview with an ABC reporter on interrogation methods being used on terrorism suspects, a controversy then gathering strength in the news. Although Kiriakou had not himself participated in interrogations, based on what he had heard from others in the Agency, he confirmed that waterboarding was being used and that it had been used against Abu Zubaydah. ABC claimed the interview made him the first CIA officer to confirm that the Agency used waterboarding, which had been a classified technique. In the interview, Kiriakou both defended the CIA and the technique as having been fruitful for gaining valuable intelligence, and also admitted that he thought waterboarding was torture and probably should be discontinued (Coll, 2013; Shane, 2013a).

From this interview Kiriakou's troubles unfolded over the next several years, but it took time to recognize them as trouble. After his interview late in 2007, he instantly became a favorite of news reporters who were looking for background on intelligence stories, confirmation of story lines, and names of others who could help develop stories. It was a heady position for someone developing a career as a consultant, to be sought after as an expert, and he appeared to enjoy the attention. Among the contacts he fielded from the press, several of his conversations would turn out to include his having passed along classified information or the names of covert agents who were still under cover. The CIA appears not to have been forgiving of slips by Kiriakou, if they were slips, since this was the former CIA employee who had confirmed the Agency's reliance on waterboarding in interrogations, a technique that was soon being widely denounced in public as torture (Coll, 2013; Shane, 2013a).

The incident that led to Kiriakou's prosecution for leaking illustrates a web of relationships between reporters, defense lawyers, and investigators hired by them. A reporter asked Kiriakou a question about who at the CIA had led a program for the rendition of terrorism suspects to secret locations. At first he could not recall, but a few weeks later, Kiriakou sent the reporter an email in which he passed along the name he had just remembered. When asked, the reporter in turn passed the name to an investigator working for defense lawyers representing detainees at Guantanamo Bay. The investigator was collecting names and photos of CIA personnel who might have participated in interrogations of detainees. The lawyers he worked for wanted those names as potential witnesses who could be called at future military trials of their clients, where the lawyers hoped to develop the argument that the detainees had been subjected to torture during their interrogations and therefore any admissions by them were illegal and the detainees should be released. Defense lawyers submitted a classified filing in January 2009 as a motion to compel discovery that asked for CIA documents to be used by the defense. The filing included classified information that they did not get from the government, including the 81 names of CIA personnel the investigator had compiled

(Coll; 2013). Some of those names were openly available, others not. Detainees themselves were found to have lists of names and accompanying photos of CIA personnel, which were being passed around for them to see by their lawyers to determine whether they could recognize their interrogators (Shane, 2013a; Federal Bureau of Investigation Eastern District of Virginia, 2012).

The CIA and the DoJ reacted to finding these lists in Guantanamo Bay with considerable concern, since covert agents could be in danger from retaliation from Al Qaeda if their identities were revealed. The FBI worked to trace how these names and photos had ended up in the cells of the detention facility. The lawyers and their investigator explained their actions and methods, and convinced the FBI that they had been respectful, careful, and had kept within the scope of their role as the legal defense. The investigator pointed to the reporter as a source, and after the FBI got a search warrant for Kiriakou's email accounts, it became apparent that he had sent the name to the reporter in his email (Shane, 2013a; Coll, 2013).

After the FBI traced various other contacts the press had had with Kiriakou, he was initially charged in January 2012 with three unauthorized disclosures of classified information, disclosing the name of a covert agent, and lying to the CIA and to federal officials. On October 23, 2012, Kiriakou pled guilty in a plea bargain to one count of violating the Intelligence Identities Protection Act, and the other counts were dropped. He agreed to serve 30 months in prison. At his sentencing, the judge noted that she found the sentence "way too light" (Coll, 2013; Associated Press, 2012).

The flash points of American experience in the early 21<sup>st</sup> century run through John Kiriakou's leak of classified information, including the wars in Iraq and Afghanistan, the interrogation of suspected terrorists and their detention at Guantanamo Bay and other sites, and the legality of interrogation techniques that had been created in the frantic years after 9/11. Initially he became a favorite press resource after he talked openly, if ambivalently, about waterboarding as torture. From that minor fame came more opportunities to help the press and to serve as an expert, and more opportunities for a garrulous person not always in control in the moment of what he said to cross a line by revealing classified information. While Kiriakou seemed ambivalent about waterboarding in 2007, when his case was adopted by protestors objecting to torture, Kiriakou shifted his views and became a strong advocate for his supporters' position against the use of torture by the government. From being a retired intelligence officer and press consultant who talked too freely, he transmuted himself into a whistle-blower on torture and a martyr who was being punished by the government for it. "After I blew the whistle on the CIA's waterboarding torture program in 2007," Kiriakou wrote to the *Los Angeles Times* from prison in 2014, "I was the subject of a years-long FBI investigation," which, he argued, considering all the highly placed officials who reveal classified information without penalty, had been unfair and discriminatory (Kiriakou, 2014).

## LEAKS AS A TYPE OF ESPIONAGE

### Donald Sachtleben

A fourth recent instance in which classified information was leaked to a reporter developed in May 2012. Its antecedents had begun several years earlier in 2009 with the thwarted Christmas Day bombing attempt in an airliner approaching Detroit. A fight broke out onboard when a bomb in one of the passenger's clothing malfunctioned, allowing passengers to overpower the bomber. The bomb came from Yemen and had been built into the man's underwear, so it became known as the "underwear bomb." In late April 2012, the CIA intervened in a similar plot in Yemen by the Al Qaeda of the Arabian Peninsula (AQAP) group, which intended to bring down a plane using a new and improved underwear bomb designed without metal. Before the hapless bomber could buy plane tickets, the CIA seized the bomb and ended the plot. The bomb, full of technical and intelligence value, was flown to the FBI Laboratory in Quantico, VA, for forensic analysis, arriving on May 1 (Associated Press, 2012; United States District Court Southern District of Indiana, Indianapolis Division, 2013).

Donald Sachtleben, an FBI special agent bomb technician who had retired in 2008 after a 25-year career and returned to the FBI as a contractor, entered the lab on the morning of May 2 using his FBI access badge. He signed onto the computer system using his Top Secret access, and then walked across the hall from his workstation into the lab room where the bomb was being examined. At 10:25 a.m. he called a friend, an Associated Press reporter, who had been texting Sachtleben asking for any details on activities at the lab involving bombs from the Middle East. Sachtleben told the reporter that there had been an interception of a plot in Yemen, a bomb had been recovered, and the FBI at the lab was now busy with "an ongoing, secretive, and sensitive analysis of the bomb" that involved other U.S. government agencies besides the FBI (United States District Court Southern District of Indiana, Indianapolis Division, 2013). The fact of the foiled bomb plot and the fact of the FBI analysis of a bomb from Yemen on May 2 were classified information.

After the government argued that sensitive issues in Yemen needed time to be resolved, the Associated Press agreed to hold off publishing the story it had developed until May 7, the day before an official announcement about the incident was made. The FBI then began to investigate who leaked the classified information to the Associated Press. A year later, they had interviewed 550 people, but still did not have the evidence to identify the leaker (Gerstein, 2013). DoJ quietly asked a federal judge to subpoena the telephone companies for their records of 20 phone lines (cell, office, and home phones) of AP reporters and the Associated Press (AP) itself. By comparing these records with other information, the investigators found conversations between the AP reporter and Donald Sachtleben, the FBI technician, and thus were able to support their request for search warrants for his computer files, cellphone records, and his other electronic media (Savage, 2013c).

Investigators then discovered that the FBI already had custody of Sachtleben's computer. Nine days after he leaked the information from the FBI lab on May 2, the

FBI in Indiana had arrested him for possession and distribution of child pornography, and had seized his electronics as evidence. Sachtleben lived in Carmel, Indiana, and commuted periodically to work in the Washington, DC area. The two FBI investigations, one in Indianapolis, IN, for child pornography and the other in Washington, DC, for national security crimes, evolved separately; the investigators only became aware of each other because of the impounded computer, which had been searched for pornography-related evidence but not for anything related to national security, since that had not been relevant to the Indiana case. The two cases swiftly merged together, and Sachtleben pled guilty on September 23, 2013, to unauthorized disclosure of classified information and to retaining classified information at his home, and to one count each of possession and distribution of child pornography. In a plea bargain, he was sentenced to a combined 140 months (11 years 8 months) in prison, which included 43 months for the leak (Horwitz, 2013; United States District Court Southern District of Indiana, Indianapolis Division, 2013).

Sachtleben had enjoyed a notable career in the FBI as a senior bomb technician. It had put him at the scene and working on many of the recent terrorist attacks in and against the United States. He had worked on FBI investigations into “the Oklahoma City bombing, the first World Trade Center bombing, the Unabomber attacks, the United States Embassy bombings in East Africa, the U.S.S. Cole bombing, and the attacks of September 11, 2001” (United States District Court Southern District of Indiana, Indianapolis Division, 2013). He seems to have relished the role of an expert who was consulted by the press for details and developments for their news stories.

In addition to the immediate impact from revealing an ongoing terrorist investigation in Yemen, the Sachtleben leak had several other serious consequences. The subpoena for the 20 AP phone lines exacerbated public criticism building over the Stephen Kim case (discussed earlier), in which the FBI had seized a reporter’s email records using a search warrant. Criticism of these two leak episodes from vocal supporters of the Constitutional guarantee of freedom of the press combined to successfully put pressure on the Attorney General, who issued new guidelines in July 2013 that made such records more difficult for prosecutors to obtain (Savage, 2013a; Gerstein, 2013). Also, further elaboration in the press on the disrupted AQAP plot in Yemen suggested that actually there had been a Western mole planted in that terrorist group, he was the person designated to carry the bomb, and because the leak had prematurely revealed the plan, he had needed to be hurriedly extracted. Thus the rare benefits of having planted an informer in such a group were lost (Barrett, 2013; Gerstein, 2013).

## LEAKS AS A TYPE OF ESPIONAGE

### Bradley Manning

U.S. Army Pfc. Bradley Manning, age 22, deployed to the Iraq War with the 10<sup>th</sup> Mountain Division 2<sup>nd</sup> Brigade late in October 2009, and was stationed at Contingency Operating Station Hammer<sup>39</sup>, east of Baghdad. He had trained as an intelligence specialist and was granted a TS-SCI security clearance. The base was still in the combat zone. There he would spend 14-hour shifts in a windowless Sensitive Compartmented Information Facility (SCIF), sifting local intelligence reports and working with computer databases, trying to improve the security of local military operations (Barnes & Hodges, 2010; Nakashima, 2011).

During 4 months of increasingly erratic and disturbed behavior at the base, from November 2009 through February 2010, Manning explored online how he could contact Wikileaks, an Internet leak site that was run by Julian Assange, which billed itself as a secure, anonymous place to download secrets and see them published without fear of being traced. Assange cultivated Manning and helped him with technical aspects of his evolving ideas. In mid-February 2010, Manning began downloading large data files and whole archives of data onto writable CDs that he carried into the SCIF disguised as music CDs. He installed forbidden software on his work computers to assist search and identification of data and explored available contents widely (Dishneau & Jelinek, 2011). He stole some 150,000 Department of State diplomatic cables sent from embassies around the world, Army field logs from the Afghanistan War, an embarrassing video of a U.S. Army helicopter apparently shooting at civilians on the ground, and hundreds of thousands of documents related to the Iraq War, over 700,000 documents in total, all of them classified. The scale of the data stolen dwarfed all previous leaks (Nakashima, 2011; Shanker, 2010; Pilkington, 2013).

Manning's transfer of data to the Wikileaks site continued in bursts during March and April and into May of 2010. So did his outbursts of emotion and barely contained violence. Wikileaks published the helicopter video on April 5, 2010, to instant notoriety, and began putting more of the leaked information online in batches. It did not publish all the information Manning sent to the site. Manning was arrested on May 26, and held in pre-trial confinement as the potential source of the leaks, while an investigation began that lasted 7 months. After a psychological evaluation and a long, well-publicized trial, Bradley Manning was convicted on July 30, 2013, on 17 charges in their entirety of the 22 charges against him, and of amended versions of four additional charges. These convictions included six of the eight counts brought under Espionage Act statutes (Title 18

---

<sup>39</sup> This is also referred to as Forward Operating Base Hammer in press accounts. Manning later announced he was changing his gender several days after he was sentenced in August 2013. He took the name Chelsea Manning at that time. Since he acted and was reacted to as a male during the time period of this summary, which focuses on his leaks, this description uses his name at that time, Bradley Manning (Bernstein & Tate, 2013).

U.S.C section 793) for unauthorized disclosure of the Afghan and Iraq War logs, embassy cables, and files from Guantanamo Bay detention facility, “with reason to believe such information could be used to the injury of the US or the advantage of any foreign nation.” He was also convicted of “wrongfully and wantonly” causing the publication on the Internet of intelligence belonging to the United States “having knowledge that intelligence published on the internet is accessible to the enemy.” He was reduced in rank to E1, the lowest possible rank. He would forfeit all pay and would be dishonorably discharged. He was acquitted of the most serious charge, that of aiding the enemy by causing classified information to be published where the enemy would see it (Pilkington, 2013; Savage & Huetteman, 2013). On August 21, 2013, he was sentenced to 35 years in prison (Tate, 2013; Nakashima, 2011).

Manning’s massive leak of classified information to Wikileaks, a site dedicated to facilitating disclosures of sensitive information that would be published to a world readership, was a shock—both due to the scale of the leak and from the impunity with which Wikileaks published the information<sup>40</sup>. The repercussions of this action became clearer with time as the leaked documents were digested by the various stakeholders. One implication drawn from them was about how persons with broad access to automated systems and electronic files inside an organization could do serious damage to it. Manning’s leak became a watershed in the history of leaks. What had been trickles from previous leaks, compromising several or several hundred documents, now had become the torrent of gigabytes Manning released. He became “the first mass digital leaker in history,” according to one account (Pilkington, 2013). His leak shook largely unexamined assumptions that had evolved alongside automated technology, assumptions about trusting the employees who worked on an organization’s systems (Shanker, 2010). The federal government responded to the illustration provided by Manning and Wikileaks of what an employee with a press outlet could do by requiring each federal agency to develop an insider threat program to audit, monitor, and evaluate the use of government computer systems by their personnel (Walker, 2013; Executive Order 13587, 2011; Department of Defense Directive, 2014; The White House, Near-term measures, 2014).

---

<sup>40</sup> Wikileaks did at first attempt to screen the classified information by working with three international newspapers (*The New York Times*, *The Guardian* in Britain, and *Der Spiegel* in Germany). These newspapers surveyed the documents Assange provided to them in order to develop their own stories, but while doing so their staff readers tried to filter out information such as names that could endanger persons or betray particularly sensitive operations (Nakashima, 2010). This process of decrypting, screening, and publishing in segments went on for some months until a password itself was leaked, and Assange quickly released most of the remaining materials all at once without filtering them. Wikileaks itself evolved over the course of handling Manning’s information and the backlash the leak provoked. From a countercultural scapegrace reveling in telling secrets, Wikileaks was soon claiming that it was a legitimate publisher—which could claim all the protections of the freedom of the press—and was trying to act the part (Nakashima, 2010; Bumiller, 2010).

## LEAKS AS A TYPE OF ESPIONAGE

Because Manning took leaking classified information to a new level, his act has attracted the publication of hundreds of articles, character studies, government reports, legal treatments, and books.<sup>41</sup> Here only two aspects, seen in hindsight, of the many that can be studied in this episode are discussed. They were chosen because they suggest how and why he was able to accomplish the leak at the time, and they offer clues for mitigating vulnerabilities to leaks from troubled individuals in the future.

First, the information security practiced at Contingency Operating Station Hammer in Iraq was inadequate, even lackadaisical. Admittedly, a combat environment makes special demands on typical security procedures, but the base received a wide variety of classified and sensitive information over its Secret Internet Protocol Router network (SIPRnet) that nonetheless should have received more careful attention. With lax supervision, Manning was able to install proscribed software on his computer to access additional data he was not authorized to see, to bring removable devices—CDs labeled as music—into a SCIF and brazenly download archives of data while pretending to hum along to the tunes, then encrypt and upload the files to the Internet and Wikileaks. Better information security and management of personnel assigned to the SCIF would have prevented his theft (Nakashima, 2011; Jaffe & Nakashima, 2011).

Second, Manning's experience in the Army calls into question the approaches that were then in place to respond to troubled military personnel. Manning did not fit well in the military. He was short, slight, not athletic but very smart, and mercurial, shifting rapidly from glum introvert to outspoken smart-aleck. During his whole military career he was struggling with his sexual identity, during the very time when the military services locked down the whole topic of sexual orientation under the "Don't Ask Don't Tell" policy. While in the Army, he moved from being closeted to being more openly homosexual with friends and on Facebook; for the first time he fell in love with a man and then suffered a break-up from him. Eventually, he decided to live as a woman. He had a lot going on besides learning to be a soldier, and he complained repeatedly that he had no one to talk to about it. Not surprisingly, between periods of cheerful insouciance, he suffered from mood swings, depression, outbursts of aggression when frustrated, and threats of violence toward others and himself. Despite numerous short-term interventions in response to his angry infractions, officers overlooked the larger pattern in his episodes that suggested a seriously troubled individual and, because they desperately needed capable intelligence analysts, sent him to Iraq despite their qualms (Youssef, 2011; Nakashima & Tate, 2011; Savage, 2013b; United States v. Manning, Defense request, 2011).

---

<sup>41</sup> This brief summary does not attempt to summarize or even mention many of the dimensions developed in all of this material, which is usually available online.

With his gender identity crisis in the background, in the foreground of Manning's motivation for the leak was a swirl of current interests and reactions to events in his life. They included (1) the legal fight then taking place for gay rights at the state and federal levels and (2) his introduction, through his boyfriend, to the hacker culture in Boston and its proclamation that information is like a free spirit, which demands to be free of constraints like classification.

Once he arrived in Iraq, his disillusionment with the American war effort became acute—for example, not over discovering corruption in the local Iraqi police, but over his Army supervisor's utter disinterest in doing anything about it (Fishman, 2011). He knit these threads into a plan of action for himself: first he should show the world the video that had so shocked him when he had watched it in the SCIF, that of the helicopter shooting from the air at Iraqi civilians on the ground. Two Reuters journalists and some 12 Iraqi civilians had been killed in the incident in 2007. Then, so the world would know what was really going on in the wars, he would add to that revelation the logs of military operations over years of the Iraq and Afghanistan wars and thousands of diplomatic cables that revealed American foreign policy in candid detail. His disclosures would have implications of "global scope, and breath-taking depth," he told a hacker confidant, who later turned him over to the authorities (Nicks, 2010).

Manning claimed he was acting as a whistle blower, but he had no specific government misconduct in mind. What he was blowing about was so grandiose and so unfocused—American missteps in military interventions and foreign policies over last decade—that it is hard not to see a very young man's ego, idealism, and lack of judgment as underlying explanations for his actions (Fishman, 2011). Manning had time to consider the actions he took as a 22-year-old, since he was sentenced to prison for at least 8 years before becoming eligible for parole (Tate, 2013). On January 17, 2017, President Obama commuted all but 4 remaining months of Manning's sentence and he was freed on May 17, 2017 (Savage, 2017).

These five cases involved persons with access to classified information who transmitted some of it to an American member of the press—a journalist or reporter, a blogger, an online website—in order to facilitate (or at least with an awareness that the outcome would be) a release to the public. The last two cases discussed here each differ somewhat from the five press leak cases, as well as from each other<sup>42</sup>. In 2006, Matthew Diaz sent the names, classified Secret, of all 551 terrorist detainees who were then being held at Joint Task Force-Guantanamo Bay, Cuba, to a civil rights lawyer in New York City. From 1999 through 2004, Lawrence Franklin surreptitiously met with and orally conveyed classified information about Iran (which was his academic specialty and the focus of his DoD position as a

---

<sup>42</sup> Matthew Diaz and Lawrence Franklin were also discussed in the 2008 PERSEREC report "Changes in Espionage by Americans," and material from these earlier case summaries was revised and included here.

## LEAKS AS A TYPE OF ESPIONAGE

strategy analyst), to two American lobbyists for the American Israel Public Action Committee (AIPAC). In the short term, neither Diaz nor Franklin seems to have intended to see their information published, yet with their own purposes in mind, they deliberately made unauthorized disclosures to fellow Americans knowing that they violated the law.<sup>43</sup>

### Matthew Diaz

In 1995, Matthew Diaz joined the U.S. Navy's Judge Advocate General (JAG) Corps as a staff attorney. In June 2004, the Navy sent him to the Guantanamo Bay detention facility for a 6-month tour as the Deputy Staff Judge Advocate. A week before he arrived in Cuba to begin his 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, 2007; 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 offering to defend detainees based on the recent 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 divulge 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 were requesting it as potential defense counsellors. This assertion was based on a policy that "We do not publish lists of people captured in armed conflict" (Rosenberg, 2007a).

Early in January 2005, as Diaz's tour in Cuba was about to end, he saw himself in a "moral dilemma" (Scutro, 2007). He felt that 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,

---

<sup>43</sup> It could be argued that other individuals could be included as leak cases. The criteria used to determine inclusion here, or the timing of the case, prevented these others from being considered. Daniel Ellsberg and Anthony Russo leaked a classified history of American involvement in Vietnam to the press in 1971, but they were not prosecuted after the Supreme Court ruled that the government could not enjoin publication in advance. Samuel Morison sent two classified photographs to the British journal *Jane's Defense Weekly* in 1984, and was convicted of espionage; he sent classified information to British recipients, not to Americans, and is coded here as espionage, not a leak. Thomas Drake, an NSA contractor, was investigated for taking classified documents home and leaking some of them to a reporter for the *Baltimore Sun*. The documents concerned an National Security Agency (NSA) program that Drake claimed wasted public money and was ineffectual. Although he was indicted under the Espionage Act in 2010, the charges were dropped in June 2011 and he pled guilty to one misdemeanor, misuse of an NSA computer. Jeffrey Sterling, CIA employee, was convicted in January 2015 of leaking classified information to James Risen, a *New York Times* journalist and author, but his conviction occurred after the cutoff date for entering new cases for this report (Currier, 2013).

and the Supreme Court had just affirmed that right specifically for detainees. Given his own father's incarceration, Diaz felt this issue strongly and personally.<sup>44</sup> He was about to lose his access to the information about the detainees that was being denied. Diaz acted on his dilemma by printing out the database of names of 551 detainees from a file on the SIPRnet, the classified DoD network. His printouts listed the names, countries of origin, and various codes that reflected what if any intelligence had been gleaned and which interrogation team had been assigned to the individual (Scutro, 2007). He reduced the pages to index card size, cut the printout into 39 pages, wrapped them in a valentine hoping to disguise the package as it passed through the base Post Office, and on his last day in Cuba, sent them anonymously to Barbara Olshansky, a lawyer for the Center for Constitutional Rights in New York City (Golden, 2007).

The center is a nonprofit legal rights organization. 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 Diaz sent to her were not marked Secret, when Olshansky looked at them, she inferred she might not have a legal right to see them. Mystified about why they had come to her and who had sent them, she turned them over to the federal court in which her suit had been filed. The judge, in turn, notified the FBI that potentially classified information had been disclosed. The FBI used computer forensics, fingerprinting, and a national security letter that requested Diaz's emails to determine who had sent the pages of names (Wiltrout, 2007; Rosenberg, 2007b; "Navy lawyer," 2007).

Charges against Diaz were made public late in August 2006. During the subsequent investigation, he continued to work as a Navy lawyer in Jacksonville, FL. He was charged under the Uniform Code of Military Justice (UCMJ) 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: (1) 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; (2) knowingly and willfully communicating that information to someone not authorized to receive it, and (3) 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 already been made public in April 2006 in response to a Freedom

---

<sup>44</sup> Diaz's father was convicted of murdering 12 patients that had been in his nursing care by injecting them with Lidocaine, and he was sentenced to death in 1984. Despite his claim of innocence, he remained on California's death row until his death from natural causes in August 2010 (Cruz, 2010).

## LEAKS AS A TYPE OF ESPIONAGE

of Information suit (Wilttrout, 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 a discharge from the Navy, with the likelihood that his military pension would be forfeited due to the espionage-related conviction (Wilttrout, 2007).

“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 during the trial (Wilttrout, 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 about how he acted on his belief was wrong. He admitted that other avenues had been available to him to register his disapproval of his government’s policies, and he expressed shame that by sending the printout anonymously, he had not acted with the courage of his convictions (Wilttrout, 2007).

### Lawrence Franklin

Lawrence Franklin was a South Asia specialist who worked the Iran desk in the DoD Office of the Secretary of Defense, International Security Affairs Office. He had earned a Ph.D. in Asian Studies, held a TS-SCI security clearance for 3 decades, and, in addition to his academic and policy roles in the federal government, served as a Colonel in the Air Force Reserve. During the 1990s, he developed a strong disagreement with the trend of American foreign policy toward Iran. He complained that the National Security Council (NSC) was not taking the Iranian threat seriously enough, and fought an interagency battle between DoD, the DoS, and the CIA over the evolving policies toward Iraq (Gertz, 2009). Starting in April 1999, and continuing until August 2004, Franklin tried to influence foreign policy by sharing classified information with various Israeli contacts, including Israeli Embassy officials who were friends of his, and two lobbyists for the AIPAC, Steven Rosen and Keith Weissman.<sup>45</sup>

---

<sup>45</sup> Steven Rosen and Keith Weissman were themselves indicted for espionage for having received verbal classified information from Franklin and passing it along to foreign officials and journalists. Preparations for their trial caused lively debate among legal scholars about whether such a prosecution represented a correct application of the Espionage statutes, since it could be seen to threaten guarantees of freedom of speech and freedom of the press. The District court judge in the case, T.S. Ellis, issued numerous memoranda opinions leading up to a trial to clarify 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

The information he passed along verbally to these individuals in furtive meetings, which were held in Washington coffee shops, restaurants, and even at the Pentagon Athletic Club, usually consisted of insights into the secret internal deliberations among U.S. policymakers, but it also included intelligence on military plans and 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). Franklin worried that as an attack on Iraq approached, the foreign policy community was not properly considering the preparations by and the likely reactions of Iran (Gertz, 2009).

Israel, a close American ally, denied conducting espionage against the United States through its Embassy officials and American lobbyists, but starting in June 2003, when the FBI became aware of Franklin’s activities, agents began monitoring his movements and communications, collecting evidence against the three men. 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 the other suspects. Franklin’s wife was then confined to a wheelchair with multiple sclerosis and they had five children. Realizing that his actions had already clouded his family’s future, Franklin agreed to cooperate in FBI stings against Rosen, Weissman, and others to whom they, in turn, had passed the information. This included the political advisor to Ahmed Chalabi, a prominent exiled Iraqi politician who was then angling to become prime minister of Iraq (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 that he was withholding information from them, 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 he did not plead guilty to leaking to an Israeli embassy official who had also been identified), and one count of unlawful retention of national defense information, after a search revealed 83 classified documents stored in his home. (United States District Court for the Eastern District of Virginia, Criminal complaint, 2005; Markon, 2005a).

Franklin was sentenced on January 20, 2006, to 151 months (12 years and 7 months) in prison and fined \$10,000 (Johnston, 2006). However, in 2009, after the related case against the two AIPAC lobbyists was dropped, the judge reduced Franklin’s sentence to probation with 10 months of community confinement and 100 hours of community service, specifying that the hours should be spent giving

---

elements required to convict on espionage. His reading of the precedents, however, remains 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).

## LEAKS AS A TYPE OF ESPIONAGE

talks to audiences of young people on the rule of law (Markon, 2009; United States District Court for the Eastern District of Virginia, Motions hearing, 2009).

In 2005, the government had also indicted Steven Rosen and Keith Weissman and charged them with espionage on the grounds that they had conspired with Franklin to receive classified information from him, and then had passed it on to various members of the press and foreign officials. This was an unusual prosecution, since they were not government employees and they had no clearances with which to access classified information. A key point in trial preparations was whether the information Franklin passed to them was national defense information (the language specified in the statutes), and whether it was actually classified or not, since it had been delivered orally. It was the first time civilians who were not working for and had never worked for the government were prosecuted under the Espionage statutes (Pincus, 2009).

The complex case against Rosen and Weissman dragged on for years, with the defense threatening to call prominent government officials as witnesses, and the government repeatedly filing motions to clarify the parameters of the trial. A reporter following the case noted that “U.S. District Judge T.S. Ellis III presided over 40 hearings on the matter, and he delivered 12 published decisions. Seven separate trial dates were set and postponed [over] 3 ½ years....”(Pincus, 2009). Judge Ellis ruled that the prosecution would need to prove both that the defendants had acted “willfully,” and that they had acted “with reason to believe it could be used to the injury of the United States or to the advantage of any foreign nation.” Since the case involved *information* delivered orally rather than actual documents, according to Judge Ellis, the case would come under 18 U.S.C. section 793(e), the subsection added in 1950 to raise the burden of proof on the communication of *intangible* information [italics added.] (United States District Court for the Eastern District of Virginia, Memorandum opinion, 2006). The government dropped the case against Rosen and Weissman in May 2009, citing its concerns that classified information would be disclosed at trial and that the elements of proof required by the court made successful conviction unlikely (Markon, 2009).

Franklin’s case suggests various motives for his actions. His clandestine contacts with Rosen and Weissman took place over 5 years and involved a steady sharing of current policy positions and government intentions, a considerable and prolonged leak, suggesting that these meetings met a professional and personal need for Franklin, perhaps for like-minded colleagues with whom he could exchange views, that went beyond immediate concerns he may have had about Iranian reactions. He showed self-importance by taking American foreign policy into his own hands in leaking classified information to AIPAC lobbyists who were likely to pass it on to the Israelis, in the hope that the Israelis, in turn, would influence the NSC in the directions Franklin thought best. This was bolstered by his ambition to get a job with the NSC. He asked Rosen to “put in a good word for him” at the NSC when Rosen would lobby them to take the actions Franklin was recommending (United

## LEAKS AS A TYPE OF ESPIONAGE

States District Court for the Eastern District of Virginia, Superseding indictment, 2005).

The seven individuals discussed here as leakers of classified information were diverse. They ranged in age from 22 to 52 years of age: one person was 22, four persons were in their middle years (their 30s or 40s), and two persons were in their early 50s. They worked in various agencies: two were members of the military, (U.S. Navy and U.S. Army); two were civilian federal employees, current or former, (DoD Office of the Secretary of Defense and CIA); and three were contractors to federal agencies, (two to the FBI, and one to the DoS). They had reached different stages in their careers, from a precocious Army Pfc. to people striving to make a name and a place for themselves at mid-career to a respected senior Defense policy specialist.

The earlier case summaries describe various motives for their actions (and ultimately each person's mix of motives is unique), but three common motives run through the seven cases.

- The leakers strongly objected to something they saw being done in the course of their work. Franklin, Diaz, Leibowitz, Kiriakou, and Manning each objected to policies or actions by the federal government that they observed, and they chose to intervene, usually by making their objections public by releasing classified information.
- The leakers enjoyed playing the role of expert. Franklin, Leibowitz, Kim, Kiriakou, and Sachtleben each sought out opportunities (or responded eagerly to overtures by others needing their information) to share their expertise with journalists.
- The leakers wanted to help and saw themselves as helping. Diaz, Kim, and Manning, were, in their view, trying to help people whom they had befriended or with whom they sympathized.

To illustrate how leaks are a form of espionage in most ways, but not in every way, the elements of classic espionage that were discussed earlier are here applied to the actions of Lawrence Franklin. The details are from the "Superseding Indictment" of Franklin (United States District Court for the Eastern District of Virginia, 2005)

- A context of competition. Franklin's job was to monitor the hostile international relationship between the United States and Iran after its Islamic revolution in 1979. After 9/11, a debate simmered in his agency over preparations for the invasion of Iraq. Franklin argued that Iran's likely response would be hostile; his contacts with the two AIPAC lobbyists spanned the years of the run-up to the Iraq War.
- Secret means. Franklin conveyed highly classified information to the recipients orally in meeting held in public places where they were less likely to be observed.
- Goal is secrets. Rosen and Weissman sought out a well-placed contact in OSD who could provide them information. They were delighted to be receiving

## LEAKS AS A TYPE OF ESPIONAGE

classified information. Rosen is quoted as saying on the telephone “that he was excited to meet with a ‘Pentagon guy’ [Franklin] because this person was a ‘real insider.’”

- Political, military, economic secrets. The classified information Franklin leaked to Rosen and Weissman included CIA internal reports on Middle Eastern countries, internal deliberations by federal officials, policy documents, and national intelligence concerning Al Qaeda and Iraq.
- Theft. Franklin was not accused of passing stolen documents to the recipients, only oral information based on them. He was accused of stealing and taking home classified documents that were found stored at his residence.
- Subterfuge and surveillance. Franklin, Rosen, and Weissman held their meetings at various restaurants, coffee shops, sports facilities, baseball games, and landmarks in the Washington, DC area. They tried to remain unobtrusive. In one instance, they met at Union Station, moved to a restaurant, then moved to a second restaurant, and ended their conversation in a third.
- Illegality. Franklin was convicted of Title 18 U.S.C section 793(d) and (e).
- Psychological toll. In July 2004, after the FBI explained their evidence and the likely consequences of a prison term on his family, Franklin took the FBI’s bargain for leniency if he would “wear a wire” during his subsequent conversations with Rosen and Weissman. This proved a harrowing bargain for Franklin.

Franklin’s case tracks with most of the elements of classic espionage. Only some of the recipients, the two AIPAC lobbyists who were the focus of his case, differ in that they were American citizens, and even then, other of Franklin’s contacts appear to have been Israelis. Applying these elements to the other six leak cases discussed earlier reinforces this conclusion: leaks differ from classic espionage mostly in that the initial recipients typically are Americans, rather than foreign nations or their agents.

### Edward Snowden

Because so much attention in the intelligence community and the press has already been paid to Edward Snowden’s actions, it is appropriate to conclude this discussion of leaks with Snowden. As a fugitive, he has not been tried or convicted of crimes related to his leak, and so his case has not yet been coded into the data on which this report is based. Snowden claims to have been inspired by what Bradley Manning did before him. Then, watching what happened to Manning and to Thomas Drake (prosecuted for leaking NSA information until the case was dropped), he admits that he saw what the likely consequences of leaking would be and fled to avoid them. Also like Manning, Snowden received considerable support from Julian Assange at Wikileaks (Pincus, 2013; LaFraniere, 2013; Wilentz, 2014).

As a young man, Snowden parlayed his talent with computers into trusted information systems positions in the Intelligence Community—first with the CIA, and then with the NSA as an employee of the NSA contractor Dell. The more he saw of the expanded surveillance and foreign intelligence gathering secretly taking place in these agencies after 9/11, the more disillusioned he became. The use of torture in interrogations, and later the drone strikes against targeted individuals, offended him. In this as well, his path resembled Manning’s (Miller, 2013).<sup>46</sup> Snowden’s access as a trusted systems administrator to a wide variety of programs, his use of “web crawler” software to extend his search for more documents, and his claim<sup>47</sup> that he needed to use the passwords of others to do his job, allowed him to download an estimated 1.7 million documents onto hard disks, echoing Manning’s massive data theft (Wilentz, 2014; Bamford, 2014; Sanger & Schmitt, 2014; Hosenball & Strobel, 2013).

Snowden stole this archive gradually, apparently beginning in April 2012; he imagined releasing information from it nugget by nugget to the press and from them, inevitably, to adversaries of the United States and to the world public. Starting in January 2013, he contacted several people with offers to leak information to them, including Glenn Greenwald, a commentator previously with *The Guardian* newspaper in London, and Laura Poitras, a documentary filmmaker. The three of them carefully planned how to store and transfer the classified data, assuming NSA’s surveillance capabilities would be trained on them. Julian Assange agreed to pay for Snowden’s travel and lodging outside the country, and provided legal counsel. On May 20, 2013, Snowden fled from Hawaii where he worked at an NSA facility, taking his hard disks to Hong Kong, accompanied by a Wikileaks editor (Wilentz, 2014).

Snowden publicly announced his actions on July 9 in an interview with Greenwald in a video that was published in *The Guardian* (Reitman, 2013). He portrayed himself as a whistle blower bent on warning the American public about the government’s surreptitious theft of their civil liberties granted in the Fourth Amendment to the Constitution, which guarantees the right to be secure from against unreasonable searches and seizures, and includes the right to privacy. He claimed he leaked classified information so the public could know about and insist on reform of the intelligence surveillance programs being carried on out of its sight. He was quoted as explaining that

My sole motive is to inform the public as to that which is done in their name and that which is done against them... I'm willing to sacrifice all of that [his previous life] because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties

---

<sup>46</sup> This article provides an instructive comparison of Bradley Manning and Edward Snowden (Miller, 2013).

<sup>47</sup> Snowden disputes the claim by journalists that he tricked co-workers into using their passwords and PKI certificates, but the co-workers support the claim.

## LEAKS AS A TYPE OF ESPIONAGE

for people around the world with this massive surveillance machine they're secretly building (Greenwald, MacAskill & Poitras, 2013).

For the next 6 weeks, Snowden lurked in hotels, avoiding authorities and the press, seeking asylum in any of several South American countries. From Hong Kong he flew to Moscow on June 23, but was stalled in the Sheremetyevo International airport transit zone when the United States withdrew his passport (Osborn & Anishchuk, 2013). On August 1, 2013, Russia offered Snowden 1 year of temporary political asylum, and he left the airport for living quarters provided for him. His asylum extended to 3 years and was then renewed. He has continued to live outside Moscow, a propaganda plum for the government of Vladimir Putin and a vexation for the United States, where he gives occasional interviews, writes opinion pieces for newspapers, lives with his girlfriend, and appears to be negotiating over his next steps (Myers, 2013).

Working from his archive secreted outside Russia through his supporters who are less constrained than he is since he lives in Moscow, for 2 years Snowden leaked bombshell after bombshell in stories published by various press and Internet sites. His stolen documents show wide-ranging programs that the NSA secretly put in place after 9/11 in the name of tracking potential terrorists. The NSA had been collecting and storing the bulk domestic phone records of American citizens, cooperating with Internet providers to collect in bulk customers' email records, and surveilling the communications of foreign governments. For years the Foreign Intelligence Surveillance Act (FISA) court had been serially approving these activities in secret, following the legal procedure set up to handle classified requests for authorization. Other documents from Australian and British sources reveal the extent of allied cooperation in NSA's surveillance programs (Bamford, 2014; Shane, 2013b).

Initially, the government reacted to Snowden's leaks with consternation and outrage. He has been charged with theft of government property and two counts of espionage (Shane, 2013b). The audit of what Snowden took with him lasted for months; the intermittent and on-going release of additional documents keeps the leak alive; and it has taken time to work out the ramifications and reactions flowing from their publication (Ignatius, 2014). Three NSA employees had their security clearances suspended and were investigated for security violations for allowing Snowden to use their public key infrastructure certificates; one person resigned from the NSA (Nakashima, 2014).

Critics of Snowden bitterly point out that terrorist groups such as Al Qaeda, and other nations in contention with the United States, quickly changed their communications protocols in response to his leaks, losing an intelligence capability the United States had built over years using millions of dollars (Tsukayama, 2014). One critic blamed a Snowden leak for contributing to the rise of the Islamic State in Syria (ISIS) by warning its leaders off unencrypted email, which they stopped using, thereby losing the NSA's insight into their plans (Harris, 2015). Other information

leaked by Snowden demonstrated that for years Chinese hackers had been deeply penetrating various defense programs such as the Joint Strike Fighter through cyber espionage, but ironically, it also showed that the NSA was detecting and tracking this penetration, and was planning electronic countermeasures—until the leak tipped off the Chinese (Gertz, 2015).

Evaluation of Snowden continues to evolve. He remains a wanted fugitive. His actions suggest he hopes that with hindsight, and as the public reacts to the substance of his revelations, authorities will soften, the political climate will shift, and he will be able to strike a plea bargain and return home (Gertz, 2014). To some extent this shift has begun to happen. There has been vigorous public protest against the secret programs Snowden revealed. In May 2015, a federal appeals court declared that NSA's collection of Americans' bulk telephone records was illegal, and Congress later voted to discontinue the program of government collection and storage, instead proposing to keep these records accessible but in the hands of the telephone companies (Savage, 2015). It is unclear what form a revised program may take.

In response to Snowden's leak, there have been efforts to temper or discontinue other controversial programs, and a campaign has begun to demonstrate more transparency about activities by the Intelligence Community. "The intelligence community is by design focused on keeping secrets rather than disclosing them," the Civil Liberties Protection Officer for the Director of National Intelligence (DNI) is quoted as saying. "We have to figure out how we can work with our very dedicated work force to be transparent while they're keeping secrets" (Gerstein, 2015). An international conference of intelligence officials reported agreement among themselves that "Snowden—love him or hate him—has changed the landscape," and that going forward, there should be no secret laws, there should be stronger external controls over agencies, and those agencies should abjure techniques such as interrupting data flows or hacking into other agencies' internal networks. The officials mused about whether Snowden had provided a necessary counterbalance to the excesses of intelligence collection put in place after 9/11, even though they uniformly considered his disclosures to have been "hugely damaging" (Campbell, 2015).

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

### ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

An agent is someone who is authorized to act on another's behalf, according to the first definition in an online dictionary; the sixth definition narrows that to someone "who acts in an official capacity for a government or private agency, as a guard, detective, or spy" (Dictionary.com, 2015). Federal law has required registration by anyone acting within the United States as an agent of a foreign government since shortly before the Second World War. Congress passed the Foreign Agents Registration Act (FARA, 22 U.S.C. section 611) in 1938 in response to concern about foreign governments surreptitiously spreading propaganda to advance their interests, while the American government and the public could not tell who was really behind it. The immediate provocation for the law came from agents for Nazi Germany, who were arguing in the press that the steps Germany was taking toward rearmament in the late 1930s were a positive development for America because they were the best way to block the "Communist peril" (Koerner, 2003). At first, registrations of foreign agents went to the Department of State, but in 1942 this responsibility was shifted to the Attorney General of the United States, where it remains (Executive Order 9176, 1942).

FARA focuses on political actions by agents of foreign governments, including lobbying, advertising, public relations, and fund raising for "foreign principals"; it excludes specified commercial activities and actions by acknowledged foreign officials and embassy personnel (Department of Justice, "Criminal Resource Manual," 2015). According to the FARA Registration Unit in DoJ that takes in these registrations, FARA requires "periodic public disclosure [by agents] of their relationship with the foreign principal, as well as activities, receipts, and disbursements in support of those activities" (Department of Justice, National Security Division, 2015). The unit tracks all registrations it receives, and reports on them semi-annually to Congress, also making its reports available to the public at its website.<sup>48</sup> The reports are revealing of the scale of influences on the federal government because they are organized by country, from Afghanistan to Vietnam, and they list the names, addresses, and professions of each agent, the foreign government for which they do work, the activities they undertake, the total monies they received for their services in the past 6 months, and a description of any information they disseminated. The entire report is nearly 300 pages long; just the single-spaced list of names and organizations runs to 31 pages, and includes lobbying firms, tourism promoters, public relations companies, legal practices, and policy consultants (Department of Justice, Report of the Attorney General, 2014).

---

<sup>48</sup> The FARA Registration Unit is within the Counterintelligence and Export Control Section of the National Security Division of the Department of Justice. The semi-annual FARA reports to Congress are available at <http://www.fara.gov/annualrpts.html> .

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

While the FARA serves as the foundation for efforts to track agents of foreign governments, it is the related criminal statute, which focuses on the non-political and illegal activities, that concerns students of espionage. This is the Agents of Foreign Governments Act (AGFA) (Title 18, U.S.C. section 951), also enacted in 1938. It specifies the penalties for not complying with the FARA. It is the statute most often used to prosecute intelligence-gathering and other crimes by individuals acting in secret at the behest of or in support of a foreign government or official, although there are other laws that may be used as well.<sup>49</sup> The AGFA is deceptively simple: it requires that anyone acting as an agent of a foreign government who does not register with the Attorney General shall be fined, or imprisoned not more than 10 years, or both. The Act defines an agent of a foreign government as “an individual who agrees to operate within the United States subject to the direction or control of a foreign government or official,” but it specifies several exceptions to its requirements for various acknowledged foreign personnel (Title 18, U.S.C. section 951). Because it is so open-ended, it can be used by itself to prosecute a wide variety of activities that may be undertaken by an agent of a foreign government, or, as circumstances warrant, section 951 can be prosecuted along with other statutes that criminalize conspiracy, aiding and abetting, and a range of substantive crimes, including many that are espionage-related.<sup>50</sup> Although section 951 does not specify

---

<sup>49</sup> See the listing at Department of Justice, National Security Division, Foreign Agents Registration Act, FARA Related Statutes, 2015, at <http://www.fara.gov/rstatutes.html>.

<sup>50</sup> The definitions provided in U.S.C. section 1801 of Chapter 36, Foreign Intelligence Surveillance, of Title 50, War and National Defense, provide more specific legal descriptions for the activities that come under the AFGA and that typically would be associated with espionage. They include: “As used in this subchapter:

(a) “Foreign power” means—

- (1) a foreign government or any component thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
- (4) a group engaged in international terrorism or activities in preparation thereof;
- (5) a foreign-based political organization, not substantially composed of United States persons;
- (6) an entity that is directed and controlled by a foreign government or governments; or
- (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) “Agent of a foreign power” means—

(1) any person other than a United States person, who—

- (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
- (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

the types of acts themselves, they are better described in 50 U.S.C. section 1801, Definitions, under the chapter on Foreign Intelligence Surveillance that are reproduced in footnote 44 on these pages. The elements of such acts include clandestine operation, intelligence gathering, illegality, sabotage, terrorism, false identity, and the international proliferation of weapons of mass destruction.

### Individuals Charged as Agents of a Foreign Government

An analysis of the 30 individuals among the 209 under study in this report who were charged and convicted under the AFGA demonstrates the flexible interpretation available in these prosecutions. Table 16 lists the 30 persons convicted under section 951, sorts them by the cohort in which they began espionage, and provides some related information about them to help sort them into categories.

- 
- (C) engages in international terrorism or activities in preparation thereof;
  - (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation thereof; or
  - (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation thereof for or on behalf of a foreign power; or

(2) any person who—

- (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
- (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
- (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof, for or on behalf of a foreign power;
- (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
- (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C)."

**ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE**

**Table 16  
Individuals Convicted as Agents of a Foreign Government**

<b>Name</b>	<b>Citizen-ship</b>	<b>Level of Clearance</b>	<b>Volunteer or Recruit</b>	<b>Recruit-ed by</b>	<b>Foreign Intelligence Service (FIS) member</b>	<b>Coded as Both Classic Espionage and as a Foreign Agent</b>
<b>Began 1947-1979 12 individuals</b>						
Alvarez, Carlos,	naturalized	none	recruit	FIS		
Boyce, Christopher	native	TS/SCI	volunteer			both
Butenko, John	native	TS	recruit	FIS		both
Chung, Dongfan	naturalized	S	recruit	FIS		
Humphrey, Ronald	native	TS	volunteer			both
Johnson, Robert	native	TS	volunteer			both
Kadish, Ben-Ami	native	S	recruit	FIS		
Lee, Andrew	native	none	volunteer			both
Rees, Norman	naturalized	none	volunteer			suicide
Szabo, Zoltan	naturalized	TS	recruit	FIS	yes	both
Thompson, Robert	native	S	volunteer			both
Whalen, William	native	TS	recruit	FIS		both
<b>Began 1980-1989 5 individuals</b>						
Ali, Amen	naturalized	none	volunteer			
Alvarez, Elsa	naturalized	none	recruit	FIS		
Chiu, Rebecca	naturalized	none	recruit	FIS		
Hall, James	native	TS/SCI	volunteer			both
Mak, Chi	naturalized	S	recruit	FIS	yes	
<b>Began 1990-2015 13 individuals</b>						
Alonso, Alejandro	native	none	volunteer		yes	
Gari, George	native	none	recruit	FIS	yes	
Guerrero, Antonio	native	none	recruit	FIS	yes	both
Hernandez, Linda	native	none	recruit	FIS	yes	
Hernandez, Nilo	naturalized	none	recruit	FIS	yes	
Latchin, Sami	naturalized	none	recruit	FIS	yes	
Nicholson, Harold	native	TS/SCI	volunteer			both

**ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE**

<b>Name</b>	<b>Citizen-ship</b>	<b>Level of Clearance</b>	<b>Volunteer or Recruit</b>	<b>Recruit-ed by</b>	<b>Foreign Intelligence Service (FIS) member</b>	<b>Coded as Both Classic Espionage and as a Foreign Agent</b>
Nicholson, Nathaniel	native	none	recruit	family		
Santos, Joseph	naturalized	none	recruit	FIS	yes	
Shaaban, Shaaban	naturalized	none	volunteer			
Shemami, Najeb	naturalized	none	recruit	FIS		
Soueid, Mohamad	naturalized	none	recruit	FIS	yes	
Yai, John	naturalized	none	recruit	FIS	yes	

An initial look at Table 16 suggests that categorizing espionage-related offenders by whether they were prosecuted and convicted of AFGA, Title 18 U.S.C. section 951 is not a very revealing strategy. Some individuals listed in this table were native-born, some were naturalized citizens. Some held security clearances and had access to classified information, many did not. Many were recruited, but 40% were volunteers. A common thread does run among recruits, however, in that all but one was recruited by a foreign intelligence service. Many of the 30 were convicted both of classic espionage, under the various espionage statutes (and so were already counted in the section on classic espionage earlier in this report), but two-thirds were convicted of being an agent of a foreign government and not for classic espionage, some of those for being a foreign agent alone, others combined with other charges besides classic espionage. This hodgepodge suggests that there are different categories of individuals embedded in this list, and they need to be sorted out before any patterns in prosecutions of agents can be discerned.

Using Table 16 as a starting point, the three tables that follow reorganize the entries in Table 16 by filtering on several of the fields. This filtering allows us to distinguish and sort out three groups that are mixed together in Table 16. Each of the next three tables depicts one of these groups: (1) Table 17 presents the classic spies who were also convicted as foreign agents; (2) Table 18 presents employees of foreign intelligence services who were convicted as foreign agents; and (3) Table 19 presents persons who were not convicted of classic espionage but who were convicted of being agents of foreign governments. For some in this third group, acting as a foreign agent was their only conviction, while for others it was one of several offenses.

**ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE**

**Classic Spies Who Were Also Convicted as Foreign Agents**

Table 17 lists those convicted of both classic espionage and of acting as an agent of a foreign government. Most of them began their espionage in the period before 1979.

**Table 17  
Individuals Convicted Both of Classic Espionage and as Agents of a Foreign Government**

<b>Name</b>	<b>Citizenship</b>	<b>Level of Clearance</b>	<b>Volunteer or Recruit</b>	<b>Recruited by</b>	<b>Foreign Intelligence Service (FIS) member</b>
<b>Began 1947-1979 8 individuals</b>					
Boyce, Christopher	native	TS/SCI	volunteer		
Butenko, John	native	TS	recruit	FIS	
Humphrey, Ronald	native	TS	volunteer		
Johnson, Robert	native	TS	volunteer		
Lee, Andrew	native	none	volunteer		
Szabo, Zoltan	naturalized	TS	recruit	FIS	yes
Thompson, Robert	native	S	volunteer		
Whalen, William	native	TS	recruit	FIS	
<b>Began 1980-1989 1 individual</b>					
Hall, James	native	TS/SCI	volunteer		
<b>Began 1990-2014 2 individuals</b>					
Guerrero, Antonio	native	none	recruit	FIS	yes
Nicholson, Harold	native	TS/SCI	volunteer		

Ten of these eleven individuals committed serious espionage crimes involving classified information and were convicted under the espionage statutes along with being convicted as foreign agents. These include Christopher Boyce, Robert Johnson, and Harold James Nicholson, who is discussed earlier as having lured his son Nathaniel into espionage.

In this table, only Antonio Guerrero had no access to classified information. He was one of a group doing surveillance and intelligence gathering for the Cuban intelligence service operating in south Florida during the 1990s. They were known

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

as the La Red Avispa network (“avispa” means wasp in Spanish). Ten of them were rolled up starting in 1998. Most chose to plead guilty to being foreign agents, and received prison terms of 3 to 7 years, while espionage charges against them were dropped. Guerrero, who had been born in Miami but was taken to Cuba as an infant, chose to go to trial. It was held in Miami, where anti-Castro feeling ran high. In 2001, he was convicted of espionage as well as of being a foreign agent, and was sentenced to life in prison. His sentence was reduced to 21 years and 10 months in 2009 (Weaver, 2009). Recently, he was one of the five Cubans and Cuban-Americans released to Cuba as part of the warming of diplomatic relations between the United States and Cuba (Robles & Davis, 2014; Freeman, 2014).

Except for Guerrero, all those who were convicted of classic espionage and of acting as foreign agents had security clearances and access to classified information, or in the case of Andrew Lee, was the accomplice of someone who did. Ten of the eleven individuals were native-born citizens. Seven of the eleven volunteered to commit espionage. Guerrero was one of the four recruits in this group, all of whom were recruited by a foreign intelligence service. Two actually worked for an intelligence service as employees. Guerrero was one of these, and the second was Zoltan Szabo.

Szabo had served in the U.S. Army during the Vietnam War, and began working for the Hungarian intelligence service in 1967. He recruited Clyde Conrad, a retired American Army sergeant working in at a military archives in Germany, into performing espionage for the Hungarians. Conrad, in his turn, recruited at least five of his Army confederates to be spies in his own espionage ring, first in West Germany and then continuing in the United States. The Conrad ring betrayed damaging intelligence on CIA sources and methods in Germany and nuclear secrets, including American plans in the event nuclear war with the Soviets broke out in the 1980s. Szabo cooperated with investigators against Conrad to receive a light sentence. He was tried in Austria rather than in the United States and received no prison time (Gerth, 1989; Rafalko, n.d.). His conviction codes here are based on descriptions of his espionage activities themselves.

It would appear there is a trend away from the practice of prosecuting persons who commit classic espionage under both the espionage statutes and as foreign agents, since 8 of the 11 instances here date from the earliest cohort that began espionage, before 1979.

The individuals in Table 17 were spies who committed classic espionage, and whom prosecutors chose to also charge with acting as an agent of a foreign government. Given the difficulties that were discussed earlier in successfully bringing espionage charges, it would not be surprising if prosecutors chose to add the foreign agent charge, which carries less prison time but under which it is easier to achieve a conviction, in order to ensure that the offender is convicted of some level of crime—as a sort of back-up or consolation prize for the prosecution if the jury does not find espionage itself.

**ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE**

**Employees of Foreign Intelligence Services**

A second group that can be identified within the hodgepodge in Table 16 is the foreign intelligence service employees. Table 18 lists those who worked directly for an intelligence service and who were convicted of acting as an agent of a foreign government.

**Table 18  
Individuals Working for a Foreign Intelligence Service (FIS) and Convicted as Agents of a Foreign Government**

<b>Name</b>	<b>Citizenship</b>	<b>Level of Clearance</b>	<b>Volunteer or Recruit</b>	<b>Recruited by</b>	<b>Foreign Intelligence Service (FIS) member</b>	<b>Coded as Both Classic Espionage and as a Foreign Agent</b>
<b>Began 1947-1979 1 individual</b>						
Szabo, Zoltan	naturalized	TS	recruit	FIS	yes	both (imputed)
<b>Began 1980-1989 1 individual</b>						
Mak, Chi	naturalized	S	recruit	FIS	yes	
<b>Began 1990-2015 9 individuals</b>						
Alonso, Alejandro	native	none	volunteer		yes	
Gari, George	native	none	recruit	FIS	yes	
Guerrero, Antonio	native	none	recruit	FIS	yes	both
Hernandez, Linda	native	none	recruit	FIS	yes	
Hernandez, Nilo	naturalized	none	recruit	FIS	yes	
Latchin, Sami	naturalized	none	recruit	FIS	yes	
Santos, Joseph	naturalized	none	recruit	FIS	yes	
Soueid, Mohamad	naturalized	none	recruit	FIS	yes	
Yai, John	naturalized	none	recruit	FIS	yes	

The individuals in Table 18 differ from those discussed as classic spies in Table 17 because these all worked for foreign intelligence services. Seven of the eleven were naturalized citizens, and ten of the eleven were recruited by their foreign intelligence service; only one volunteered. The two individuals who began espionage before 1990, one in each of the two earlier cohorts, held security clearances, but the nine who began after 1990 held none. John Yai, who was one of these without access to classified information, worked for the North Korean intelligence service and was discussed earlier. Only one person in this group of eleven persons is coded as both an instance of classic espionage and an agent of a foreign government, and

## **ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE**

that is Zoltan Szabo. If there is a trend in Table 18, it is the reverse of the one noted in Table 17, since here nine of the eleven persons, 82% of them, began their espionage in the latest cohort since 1990, in contrast to the classic spies in Table 17 who most frequently began in the earliest cohort. Since 1990, several things could be happening to cause this trend. Perhaps there are more employees of foreign intelligence services spying in the United States than there have been in the earlier periods. A former head of the House Intelligence Committee, Mike Rogers, suggested this when he publicly claimed in April 2016 that “There are more spies in the United States today from foreign nation states than at any time in our history—including the Cold War, and they’re stealing everything. If it’s not bolted down, it’s gone” (Hattem, 2016). Then again, perhaps more of them are being caught and prosecuted, or more frequently than in the past, they are being convicted on the charge of serving as agents of a foreign government.

### **Persons Not Convicted of Classic Espionage, but Convicted of Acting as Agents of Foreign Governments, Solely or with Other Charges**

The third group extracted here from Table 16 is composed of those who were not convicted of classic espionage but were convicted of acting as agents of a foreign government, some solely for that offense, and others for that offense combined with other charges. Table 19 lists these nineteen individuals.

**ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE**

**Table 19  
Individuals Not Convicted of Classic Espionage but Convicted as Agents of a Foreign Government**

<b>Name</b>	<b>Citizenship</b>	<b>Level of Clearance</b>	<b>Volunteer or Recruit</b>	<b>Recruited by</b>	<b>Foreign Intelligence Service (FIS) member</b>	<b>Convicted Only as Acting as a Foreign Agent (FA)</b>
<b>Began 1947-1979 4 individuals</b>						
Alvarez, Carlos,	naturalized	none	recruit	FIS		Only FA
Chung, Dongfan	naturalized	S	recruit	FIS		
Kadish, Ben-Ami	native	S	recruit	FIS		Only FA
Rees, Norman	naturalized	none	volunteer			Suicide, not tried
<b>Began 1980-1989 4 individuals</b>						
Ali, Amen	naturalized	none	volunteer			
Alvarez, Elsa	naturalized	none	recruit	FIS		Only FA
Chiu, Rebecca	naturalized	none	recruit	FIS		Only FA
Mak, Chi	naturalized	S	recruit	FIS	yes	
<b>Began 1990-2015 11 individuals</b>						
Alonso, Alejandro	native	none	volunteer		yes	Only FA
Gari, George	native	none	recruit	FIS	yes	Only FA
Hernandez, Linda	native	none	recruit	FIS	yes	Only FA
Hernandez, Nilo	naturalized	none	recruit	FIS	yes	Only FA
Latchin, Sami	naturalized	none	recruit	FIS	yes	
Nicholson, Nathaniel	native	none	recruit	family		
Santos, Joseph	naturalized	none	recruit	FIS	yes	Only FA
Shaaban, Shaaban	naturalized	none	volunteer			
Shemami, Najeb	naturalized	none	recruit	FIS		
Soueid, Mohamad	naturalized	none	recruit	FIS	yes	
Yai, John	naturalized	none	recruit	FIS	yes	Only FA

Nine of the eleven employees of foreign intelligence services appear both in Table 18 and in Table 19 because they were nine of the eleven persons who were convicted

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

solely of acting as agents of a foreign government (they are noted as “only FA,” that is, only foreign agent, in Table 19). Persons sent from abroad to become naturalized citizens of the United States, and thereby to become eligible to gain positions with access to classified information, as employees of foreign intelligence services typically are, obviously are acting as agents of the government that sent them.

A trend seems to be strengthening to use the AGFA alone to prosecute American citizens who work for foreign intelligence services; in the recent past, there have been more successful prosecutions using this statute than there were in past cohorts. However, not all the individuals solely charged and convicted of serving as agents of a foreign government fit this pattern. Ben-Ami Kadish, discussed earlier, was a longtime resident who was born in the United States but grew up in Palestine and had close ties to Israel; he cooperated with an Israeli intelligence operative to provide classified documents and yet was only charged as a foreign agent.

Also, not all of the known employees of foreign intelligence services who committed espionage, and that are included in this study, were charged with acting as a foreign agent, although obviously they did so. At least three such employees were charged and convicted only of classic espionage. This underlines the discretion prosecutors must exercise and the impact of circumstances and context in each case of espionage, which results in various approaches. The three foreign intelligence service employees charged only with classic espionage include the following:

- Larry Wu-tai Chin, who joined the intelligence service in China in the 1940s and came to the United States tasked with collecting intelligence. He became an American citizen, an analyst, and a translator for the CIA, all the while spying for China for the next 30 years. He earned a salary from China that may have approached \$1 million, and grew wealthier still by buying investment properties around Washington, DC. He supported a gambling habit that was so flagrant that several Las Vegas casinos cut off his access to their tables. Chin transmitted closely held secrets on American Far Eastern policy for decades, starting with reports on American interrogations of Chinese prisoners during the Korean War. After his conviction in February 1986 on all seventeen counts of espionage with which he had been charged, he was reported to have committed suicide in his cell<sup>51</sup> (Engelberg, 1986).
- Karl Koecher, who joined the Czechoslovak foreign intelligence service in 1963 and spent 2 years in intelligence training, was sent to the United States with his wife and fellow agent, Hana Koecher<sup>52</sup>. They became naturalized citizens, and Karl taught philosophy at a Staten Island college for 4 years. In 1973, he

---

<sup>51</sup> Reports on Chin’s death stated that he committed suicide by putting a plastic bag over his head and tying it with his shoelaces (Engelberg, 1986).

<sup>52</sup> Hana Koecher was not charged with espionage or being a foreign agent, but of misprision, that is, concealment, of a felony committed by her husband. She is not included as one of the individuals coded in this study.

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

obtained a security clearance and took a job as a contract translator for the CIA. From 1975 to 1977, he worked as an employee at the CIA while he continued to spy for the Czechs, but in 1977 he lost his CIA job and had to revert to teaching. Hana got a job in the diamond trade in New York City, and she continued working as a courier, moving information to the Czechs until, in November 1984, the Koechers were arrested. Two years later, they were exchanged for Anatoly Shcharansky, a famous Russian dissident. They returned to Czechoslovakia, where the government welcomed them as heroes and granted them use of a villa outside Prague and a new Volvo (Raab, 1984; Stein, 2010).

- Ali Mohamed, a former Egyptian military officer, was an enigmatic figure. He enlisted in the U.S. Army in 1986, became an American citizen by marrying an American woman, and served as a cultural and military advisor for the Army during the late 1980s and then for the FBI during in the 1990s. It was a period in when American officials needed urgently to better understand evolving transnational terrorist groups like Al Qaeda, and Mohamed credibly filled that need. He became a unique combination of terrorist and spy.

While playing the role of cultural asset for the United States, however, Ali was actually a committed Islamic extremist working for Ayman al-Zawahiri. During his enlistment in the U.S. Army, he took leave in 1988 and spent several weeks fighting with the Mujahedeen in Afghanistan. Despite reports from his superior officers criticizing this, there was no response to this glaring infraction from the Army or the Intelligence Community. In 1989, Mohamed began traveling from his Army base to New York City where he advised Islamic radicals meeting in mosques there, including the group that would bomb the World Trade Center the first time in 1993. He also used Army manuals that were classified Secret to produce a textbook for Al Qaeda trainees on collecting intelligence, doing surveillance, and planning terror attacks.

Mohamed resigned from the Army in 1989 with an honorable discharge in 1991. Zawahiri then asked him to coordinate the move of the Bin Laden family and its supporters from Afghanistan to Sudan and during these months he developed close ties with Osama bin Laden. During the late 1990s, Mohamed worked directly for Bin Laden and Al Qaeda. His tasks included providing military training—learned from the U.S. Army—to Al Qaeda recruits, and scouting the U.S. Embassy in Nairobi, which was one of the two American embassies in East Africa that Al Qaeda bombed.

Mohamed was an audacious double agent working simultaneously for Islamic extremists and either the Army or the FBI. He was arrested in September 1998, after the East Africa bombings, and pled guilty to five charges of terrorism and falsification. The seriousness of his espionage pales in comparison with his other activities. He then remained in prison for months without being sentenced, and eventually he dropped out of public view and disappeared,

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

putting the final touch to his chimerical career (Weiser & Risen, 1998; Williams & McCormick, 2001; Poole, 2010).

There are some commonalities among the persons listed in Table 19. Fourteen of the nineteen were naturalized citizens. Of the eleven persons who began activities in the recent cohort since 1990, none held a security clearance, and in the previous two cohorts only three had clearances. Fourteen were recruited, while only four were volunteers. Of the recruits, only Nathaniel Nicholson was not recruited by a foreign intelligence service, since it was his father who convinced him to contact the Russians.

Norman Rees,<sup>53</sup> listed in Table 19 as having committed suicide before he could be convicted, was unusual in the longevity of his espionage case. He began sharing unclassified information with the Soviets in 1942 about the oil industry where he worked as a petroleum engineer, while the United States and the Soviet Union were allies. Sympathetic toward Communism, as World War II ended and the Cold War began and intensified, Rees continued to collect and pass on American industrial information and techniques to the Soviets until 1971, when the FBI interviewed him. At that time Rees agreed to work for them as a double agent. In 1976, he learned that a Dallas newspaper was about to publish his story and name him, and Rees promptly committed suicide (Blau, 1976). His information had been so valuable to the Soviets that they paid him \$30,000 and a \$5000 annual pension. He received a medal for the valuable catalytic cracking converter equipment he passed to the Soviets in 1950, which set the subsequent course of Soviet oil industry development (Associated Press, 1976). Since his death prevented his being tried or convicted, what he apparently would have been charged with has been imputed here.

Of the ten persons in Table 19 who were convicted solely of being foreign agents, seven of them were working with the Cuban Intelligence Service, all in south Florida. Carlos and Elsa Alvarez, both naturalized American citizens, had been working separately for the Cubans when they met and married in the early 1980s and began to work together. Carlos Alvarez taught psychology as a professor at Florida International University (FIU). He began passing information to the Cubans in 1977 and continued until 2005; Elsa Alvarez also worked at the University as a counselor and began spying in 1982. They were arrested in 2006 and convicted in a plea bargain in March 2007 of conspiracy to act as agents of a foreign government—the conspiracy statute, Title 18 U.S.C section 371, carries lesser prison sentences than does section 951 itself (United States District Court Southern District of Florida, 2007; Weaver, 2007).

---

<sup>53</sup> Norman Rees is included in the coded data of this study despite his having begun espionage in 1942, 5 years before 1947, which is the year that defines the start for the first cohort of individuals in this report. Rees continued his surveillance for the Soviets and passed along unclassified industrial information to them for decades until the early 1970s, when he briefly became a double agent for the FBI then, threatened with public exposure, committed suicide.

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

The Alvarezes wrote reports that they encrypted onto computer disks and sent to post office boxes in New York City to the Cuban intelligence service. They used code names, a short wave radio, messages on water-soluble paper, coded pager messages, and personal meetings in Cuba to receive instructions for their surveillance and collection. Cuban intelligence wanted information on any prominent people the Alvarezes knew or could find out about, attitudes in the south Florida community, political developments as they might affect Cuba, and current events of concern to the Cuban government. Carlos was sentenced to 5 years in prison, while Elsa received 21 months (1 year and 9 months) in prison for her role in supporting and contributing to her husband's activities. Professor Alvarez had made repeated trips to Cuba with his FIU students to introduce them to the island and to foster friendly attitudes between the two countries (United States District Court Southern District of Florida, 2007).

The other five individuals who were convicted solely of being foreign agents for Cuba were part of the La Red Avispa network in southern Florida, and worked alongside Antonio Guerrero, who was discussed earlier. Alejandro Alonso, George Gari, Linda and Nilo Hernandez, and Joseph Santos all pleaded guilty in 1999 and 2000 to acting as agents of a foreign government and served various prison terms of between 4 and 7 years. Others in the network who were not American citizens are not included here. The network's agents infiltrated anti-Castro immigrant groups to report on their plans, and took jobs at military bases in south Florida where they surveilled and reported on activities there and hoped to gain access to classified information, but did not (Pressley, 1998; "Miami Spy-hunting, 2000).

Five of the persons listed in Table 19 were supplying information or equipment to Middle Eastern countries. Two were volunteers: Amen Ali and Shabaan Shabaan. The other three were recruits by foreign intelligence services: Sami Latchin and Najib Shemami were recruited to work for Iraq, and Mohamad Anas Haitham Soueid was a recruit for Syria. All five were convicted of export control or trade embargo offenses along with convictions for serving as an agent of a foreign power. Ali tried to ship dual use military equipment to Yemen (Kotowski, 2011). Shabaan worked with the Iraqi intelligence service collecting intelligence from open sources on American intentions during the run-up to the Iraq War (Corcoran, 2006). Latchin came to the United States in 1993 on orders from Saddam Hussein to fit in, become a citizen, and collect information on Iraqi opposition groups. While he "slept," until he could emerge as an agent, Latchin slowly spent his way into bankruptcy and was working as a gate agent at O'Hare airport when he was arrested. Identified in 2004 in documents captured in Iraq, Latchin was convicted in 2007 of being a foreign agent, violating the trade embargo against Iraq, and various falsifications (Coen, 2007).

Like Latchin, Shemami and Soueid are examples of foreign agents who had no access to classified or restricted information, but who instead focused on surveilling immigrant communities and sending reports to foreign governments that were worried about the threat these communities could pose to their regimes.

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

Najib Shemami was a naturalized citizen who had lived in the Detroit, Michigan area for some 40 years when he was arrested in 2007 and initially charged with four espionage-related offenses, including acting as a foreign agent. His indictment was based on Iraqi intelligence records captured during the Iraq War in 2003 (“Community members spied for Iraq,” 2007).

Starting in September 2002, and continuing through January 2003, Shemami worked for the Iraqi Intelligence Service (IIS) collecting and reporting observations and information he gathered from his community in Detroit and during three trips he made to Iraq and Turkey. As a merchant and importer of delicacies from the Middle East, Shemami had traveled there frequently since 1996 for his work. While the United States prepared for a likely invasion of Iraq in 2002, the IIS recruited him as their agent by making him a deal: he could continue importing foodstuffs—some observers describe what he was doing as smuggling goods and medicine back into Iraq as well—to the United States unhindered by the Iraqi authorities, in exchange for information the IIS requested (Associated Press, 2009).

The captured IIS records documented Shemami’s contributions to Saddam Hussein’s regime, including naming Iraqi natives living in the United States whom Shemami judged would be asked to guide American troops during an invasion of Iraq, names of expatriates who could become potential political candidates in Iraq, observations he made of military preparations in Turkey such as the locations of 200 tanks and of tents made ready for refugees, and the name of an Iraqi expatriate interviewed by, and possibly cooperating with, the FBI (United States District Court Eastern District of Michigan, 2007; Ashenfelter, 2007).

Shemami would be among the first of a dozen Iraqis in the United States, some naturalized citizens, some permanent residents, prosecuted in the late 2000s for acting as agents of Saddam Hussein’s government based on captured records. Hussein had maintained an extensive operation watching for threats to his regime in the United States and gathering intelligence among Iraqis here, including sending in “sleeper” agents who were directed to live quietly and blend into American society until instructed by the IIS to collect specific information (Leinwand, 2008).

Shemami was charged with conspiracy to act as an unregistered agent of a foreign government, acting as such an agent, providing services to Iraq—an act which violated the International Emergency Economic Powers Act (IEEPA), violating the Executive Orders that had declared Iraq a threat to the national security of the United States since 1990 and established a trade embargo, and lying to the FBI (United States District Court Eastern District of Michigan, 2007). His defense argued at trial that the IIS had coerced him into becoming their agent by threatening him with torture. One Detroit FBI agent commenting on that claim is quoted as saying that help was available to Americans to resist such pressure. “We’re here to help them... There are ways we can help them. They also have to say ‘Hey, we need help’” (Egan, 2009). Shemami pled guilty early in 2009 and was

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

sentenced to 46 months (3 years and 10 months) in prison, leaving behind a wife and nine children (Schmitt, 2009).

The regime of Bashar al-Assad, President of Syria, was also declared a threat to the national security of the United States under IEEPA based on its state support for terrorism. Similar to the practice of Saddam Hussein, Assad has been running American agents to serve as observers and reporters of the names and threatening activities among disaffected Syrian expatriates in the United States. Mohamad Anas Haitham Soueid, a Syrian-born naturalized American citizen living in Leesburg, Virginia, was arrested on October 11, 2011, and charged with conspiring to and actually acting as an agent of a foreign government (Syria) and with four counts of lying on firearms forms and to federal agents (United States Department of Justice, 2011). As the protest movement in Syria against Assad escalated in 2011, Soueid helped him monitor protestors among the Syrian immigrant communities in the United States.

Soueid recruited others to record audio and video at anti-Assad public protests and to make recordings of conversations with participants that could be used later by the Syrian intelligence service to identify them. He passed along phone numbers and email addresses of protest leaders, details about individuals who were financing the protests, logistics of meetings, internal conflicts developing within the movement, and its future plans, along with dozens of the audio and video recordings. He traveled to Syria several times between March and October 2011 where he met personally with Assad (United States Department of Justice, 2012; United States Department of Justice, 2011; Goodman, 2011). He used a laptop computer provided by Syrian intelligence to communicate securely with his contacts in the Syrian embassy in New York and in Syria. He destroyed the laptop and burned documents in his backyard after an interview with the FBI implied his imminent arrest.

Soueid was convicted in March 2012 of acting as an unregistered government agent of Syria and of falsification, and was sentenced the following July to 18 months in prison and 3 years of probation. Prophetically, he claimed at his trial that he was acting to prevent Islamic extremists from taking over in Syria and creating a larger national security threat to the United States than Assad ever had (Associated Press, 2012). “By illegally acting as an agent of Syria, Mr. Soueid deceived his adopted country of the United States in support of a violent and repressive despotic regime,” the FBI Assistant Director said at his sentencing. “Through today’s sentencing, he will now be held accountable for his actions” (United States Department of Justice, 2012).

Acting as an agent of a foreign government is, in a large sense, the essence of espionage. Applying the categories from the discussion of classic espionage earlier to the example of Mohamad Soueid’s actions helps to demonstrate how being a foreign agent is like, but not completely like, the classic pattern:

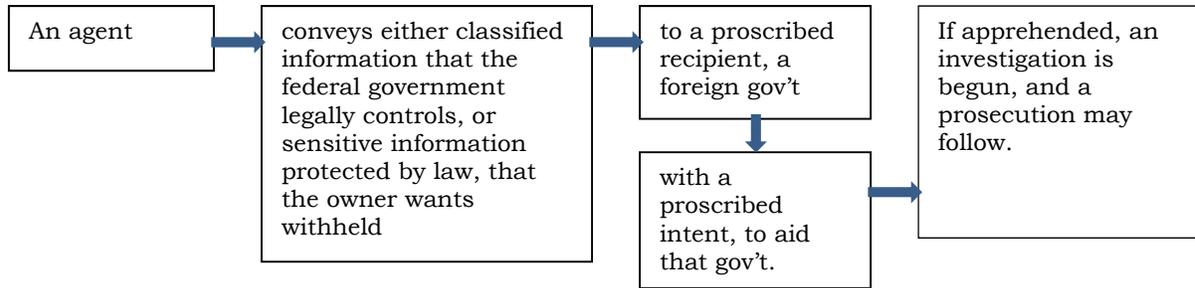
## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

- A context of competition. Syria has been designated a state sponsor of international terrorism by the Department of State since 1979, and various punitive economic, financial, and trade sanctions have been imposed on Syria by the United States based on that designation (sources for these entries follow entry 8).
- Secret means. Soueid and his co-conspirators secretly made audio and video recordings of opponents of the Assad government in the United States and emailed the recordings to the Syrian intelligence service so its agents could identify and take punitive action against them in defense of the regime.
- Goal is secrets. No classified or restricted information was involved in Soueid's case. Instead, he collected the identities, (information such as names, addresses, and email addresses) of Syrian opponents of Assad, and documented their political expressions in recordings to pass along to Syrian intelligence. The information was sensitive to the individuals being spied on, and perhaps it was even life-threatening information to those betrayed to the brutal regime, which is known for harassing, intimidating, and murdering its opponents in Syria and the relatives.
- Political, military, economic secrets. The secrets that Soueid collected were the political opinions of individual protesters and the political plans that groups made to protest and act against the regime. Soueid was sued in a civil action by several people, whose lives had been damaged as a result of his surveillance, including one woman whose father had been murdered in Syria and whose daughter had been kidnapped.
- Theft. The theft done by Soueid and his co-conspirators was theft of the privacy and security of the Syrian legal residents in the United States who were lawfully assembling and expressing their views in peaceful protest.
- Subterfuge and surveillance. Soueid and his co-conspirators clandestinely attended protest rallies and planning meetings of groups opposed to Assad, secretly made recordings there, and lied to the FBI about their actions.
- Illegality. Soueid was charged with Title 18 U.S.C. section 371, conspiracy to act as an agent of a foreign government, Title 18 U.S.C. section 951, acting as an agent of a foreign government, Title 18 U.S.C. section 922(a)(6), material false statement on a firearms purchase application, Title 18 U.S.C. section 924(a)(1)(A), false statement on a firearms application, and Title 18 U.S.C. section 1001, false statements to the FBI. He was convicted of conspiracy to act and of actually acting as an agent of a foreign government and of various falsifications.
- Psychological toll. After the FBI interviewed him but before he was arrested, Soueid burned some of his documents in his backyard and destroyed the laptop computer given to him by Syrian intelligence, suggesting that he was anxious about the legal consequences of being caught in his surveillance for Syria, but during his trial he continued to be defiant in his support for the Assad regime

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

(United States Department of State, 2015; United States District Court for the Eastern District of Virginia, Alexandria Division, Indictment, 2011; Department of Justice, Office of Public Affairs, 2012).

As the examples of Soueid and the others discussed in this section illustrate, the statutes that define acting as an agent of a foreign government are general and do not name espionage itself, yet the acts of such agents, even when they do not have access to classified or controlled information, play out an espionage scenario.



**Figure 6 Acting as an Agent of a Foreign Government in a Model of Espionage Elements**

In the United States, such agents collect information and clandestinely pass the information to a foreign government, thereby causing damage to the United States—in some instances, damage to the interests or people of expatriate communities, in others by meddling in American foreign policies, economic developments, or international military actions (Koerner, 2003). In the cases of Shemami and Soueid, they brought the divisions and dangers of the wars in Iraq and in Syria directly into their immigrant communities at home. They served as agents for foreign governments, but they were also American citizens who owed their first allegiance to the United States and betrayed that trust.

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

### **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

The United States considers the sale, export, or re-transfer of various American defense articles and knowledge to be potential threats to its national security, its economic security, and its foreign policy goals. These defense articles include military technology, dual use technologies and software, defense services, conventional weapons, missile technology, satellites, nuclear, chemical, or biological materials or weapons. They constitute millions of items (United States Department of State, Directorate of Defense Trade Controls, 2015a).

Legislation to meet these threats to national security by controlling exports of these sensitive items originated in times when the United States was facing war, in laws such as the Trading with the Enemy Act of 1917 and the Neutrality Act of 1935. Congress considered these laws necessary to prevent “giving aid and comfort to the nation’s enemies” when, as war approached, it was clear who those enemies would be (Fergusson, 2009). In the late 1940s, as the Cold War with the Soviet Union took hold, controlling defense exports shifted from its initial wartime focus to one of preventing the Soviets and their allies from procuring articles, knowledge, or materials that would help them if an actual war with the West broke out. Export control grew to become an extensive and complex federal enterprise, designed to be carried on indefinitely (Fergusson, 2009; Fergusson & Kerr, 2014).

The mechanisms of export control available to regulators in the 1950s, i.e., lists of proscribed items and procedures to license approved exports and deny licenses to those that are disapproved, shaped the export control system that persists today. The assumptions from the context of the 1950s—that of a bi-polar face-off between two super powers—also shaped the system. Yet since then, the world has become a different place, one that is more globalized, more internationally interconnected in transportation, communications, and economic cooperation, and one in which the United States faces multiple competitors and potential adversaries.

For years, people have argued that the export control system needs large-scale revision to bring it into line with these changes. Critics do not agree, however, on how it should be revised. Some argue for loosening controls to boost trade and economic profit and thereby benefit the American economy; others argue for tightening export controls to hold on to the technological advantages the United States has in the face of accelerating international competition.

Two main federal agencies handle licensing of controlled exports: the DoS and the Department of Commerce (DoC)<sup>54</sup>. Due to inadequate coordination between them,

---

<sup>54</sup> This discussion simplifies what is a complicated regulatory landscape on exports; it seems unnecessary to ask the reader to master the specialized and often arcane fields of trade policy and export control to see the relationship of these fields to espionage. Numerous federal agencies take roles in regulating specific exports, including the Department of Energy and the Nuclear Regulatory Commission that deal with various aspects of nuclear weaponry and materials. The

## VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

disputes over their respective jurisdictions, and vexing delays for applicants, in 2007 the GAO declared export control to be a high risk area that required strategic reexamination. The Obama administration began a major revision of the system in 2009, working to simplify and unite it under goals that include designating one licensing agency (instead of the two main and many subsidiary agencies that currently manage parts of it); one list of items that require an export license (instead of the two overlapping lists now in place); one enforcement structure; and one information technology system that all users could access (Levine, 2012; Fergusson & Kerr, 2014). As of 2015, reformers were making slow but appreciable progress, starting with steps to cross-reference and reconcile the two lists.

### Three Export Control Statutes

The three main statutes governing export control all date from the late 1970s. Their authors made use of the procedures then available to them that had built up since the First World War. These three statutes now define the current export control system, with some later revisions.

The Export Administration Act (EAA) of 1979<sup>55</sup> controls dual use technologies, that is, technologies that may have both commercial and military uses. It is implemented by the Department of Commerce (DoC) through the Export Administration Regulations (EAR)<sup>56</sup>. The list of specific items tracked under the EAR, which require export licenses from the DoC, is called the Commerce Control List (CCL). There are ten broad categories on the CCL:

- Nuclear materials, facilities, and equipment;
- Materials, chemicals, microorganisms, and toxins;
- Materials processing;
- Electronics design development and production;
- Computers;
- Telecommunications and information security;
- Lasers and sensors;
- Navigation and avionics;
- Marine; and

---

Department of Defense plays an important role in defining military weapons, articles, and technology of all types and overseeing their global availability. The Bureau of Industry and Security, which administers export control in the Department of Commerce, lists sections of nine federal agencies that have responsibilities for export control. In addition to those already mentioned here, they also include the Department of the Interior, the Drug Enforcement Administration, the Food and Drug Administration, the Patent and Trademark Office, and the Environmental Protection Agency. (See <http://www.bis.doc.gov/index/php/about-bis/resource-links>)

<sup>55</sup>Title 2 of P.L. 96-72

<sup>56</sup>15 C.F.R. 730 et seq.

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

- Aerospace, propulsion systems, space vehicles, and related equipment (Fergusson, 2014).

According to a Congressional Research Service (CRS) report of 2014, “Each of these categories [that are listed on the CCL] is further divided into functional groups: equipment, assemblies, and components; test, inspection, and production equipment; materials; software; and technology. Each controlled item has an export control classification number (ECCN) based on the earlier categories and functional groups. Each ECCN is accompanied by a description of the item and the reason for control. In addition to discrete items on the CCL, nearly all U.S.-origin items are “subject to the EAR.” This means that any item “subject to the EAR” may be restricted to a destination based on the end-use or end-user of the product. For example, a commodity that is not on the CCL may be denied [a license to export] if the good is destined for a military end-use or an entity known to be engaged in weapons proliferation” (Fergusson, 2014).

An oddity about the 1979 EAA is that Congress has repeatedly allowed it to expire, and then turned around and renewed it for a further specified period of time. During periods when it is expired (as it was in 2015), successive Presidents have declared that all of its powers and requirements will continue under the authority granted to the President under the International Emergency Economic Powers Act, discussed further.

The second major statute is the Arms Export Control Act (AECA) of 1976,<sup>57</sup> which regulates military technology. It requires the President to control the import and export of defense articles and defense services, which include consulting, advising, and sharing information. This sharing is one of the activities that can lead to charges of espionage. The AECA requires that governments that receive or buy weapons and other military items from the United States use them for internal security and legitimate self-defense, and not for aggression or escalation of a conflict. Elements that are considered in determining the legitimacy of an export include whether the exports contribute to an arms race, if they aid in the development of weapons of mass destruction, or if they support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements (Fergusson & Kerr, 2014).

The Act is implemented by the DoS through the International Traffic in Arms Regulations (ITAR).<sup>58</sup> The list of specific items tracked under the ITAR, which requires export licenses from the DoS, is called the United States Munitions List (USML). There are 21 broad categories on the USML, including:

---

<sup>57</sup>Title 2 of P.L. 94-329, 90 Stat. 729, enacted June 30, 1976, codified at 22 U.S.C. chap. 39.

<sup>58</sup>C.F.R. 120-130.

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

- Firearms, Close Assault Weapons and Combat Shotguns
- Guns and Armament
- Ammunition/Ordnance
- Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
- Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
- Surface Vessels of War and Special Naval Equipment
- Ground Vehicles
- Aircraft and Related Articles
- Military Training Equipment and Training
- Personal Protective Equipment
- Military Electronics
- Fire Control, Range Finder, Optical and Guidance and Control Equipment
- Materials and Miscellaneous Articles
- Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
- Spacecraft and Related Articles
- Nuclear Weapons Related Articles
- Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
- Directed Energy Weapons
- Gas Turbine Engines and Associated Equipment
- Submersible Vessels and Related Articles
- Articles, Technical Data, and Defense Services Not Otherwise Enumerated (Department of State, Directorate of Defense Trade Controls, 2015b).

A glance through the categories on the DoC's list, the CCL, followed by DoS's list, the USML, each reproduced earlier, will suggest the potential for disagreement between the two agencies, and the likely confusion for those applicants dealing with the DoC who might also be dealing with the DoS. The lists overlap, they use different terms for the same or similar items, and their categories do not match one another. This is why the export control reform effort decided that the first project it would take on was trying to reconcile the categories on the two lists.

The third major export control statute is the International Emergency Economic Powers Act (IEEPA) of 1977.<sup>59</sup> It grants the President the ability to declare an

---

<sup>59</sup> Title 2 of P.L. 95-223.

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

emergency when the United States is under unusual and extraordinary threat from abroad, short of war. Under such an emergency, the President may block financial transactions or freeze assets of belligerent foreign governments or specific foreign nationals. President Carter first declared an IEEPA emergency in 1979 in response to the Iran hostage crisis, and Iranian assets continued to be frozen by sanctions until early in 2016 when a nuclear deal was reached (Pearce, 2016). When the DoS declared Syria to be a state sponsor of terrorism in 2004, the United States froze its assets under IEEPA. Emergencies such as the attacks on 9/11 caused a similar blocking of Al Qaeda's assets and freezing of its finances in the United States (Fergusson & Kerr, 2014).

Americans who have tried to illegally trade with countries or transnational groups that are designated under IEEPA, EAA, or the AECA, or who have provided information, which is considered an export, to such governments, break the export control laws and arguably, commit a type of espionage (Michigan Technological University, 2015).

These statutes from the 1970s are sometimes insufficient for the changed demands of national and economic security in the context of the 21<sup>st</sup> century. Among these changes are the facts that: (1) a larger proportion of sensitive technology is now dual use, and thus it requires a difficult assessment by export control regulators of the risk that what is bought as a commercial application might be diverted to a military end use; (2) more countries, alongside the United States and Russia, are exporting sensitive dual-use technologies, including newer arms suppliers like China, Israel, Turkey, and Ukraine; (3) globalized methods of manufacturing now result in sensitive dual-use technologies becoming international—e.g., a defense article can be financed in one country, designed in a second, and assembled in a third [anyone using an Apple device is familiar with this sort of international collaboration]; (4) sensitive technologies have spread around the globe and are no longer the special province of just a few advanced countries, so it becomes complicated to track and “maintain sovereignty” over those technologies; (5) with more competition between international arms suppliers, it becomes difficult to exert discipline on exporters to deny them business, since if an international customer is blocked from buying what it wants from the United States, it can turn around and buy it from another country instead; and (6) the health of the economy may now be more intertwined with national security than it ever has been, making access to international markets not simply a commercial goal, but one that has direct implications for the security of the United States (Beck, 2000).

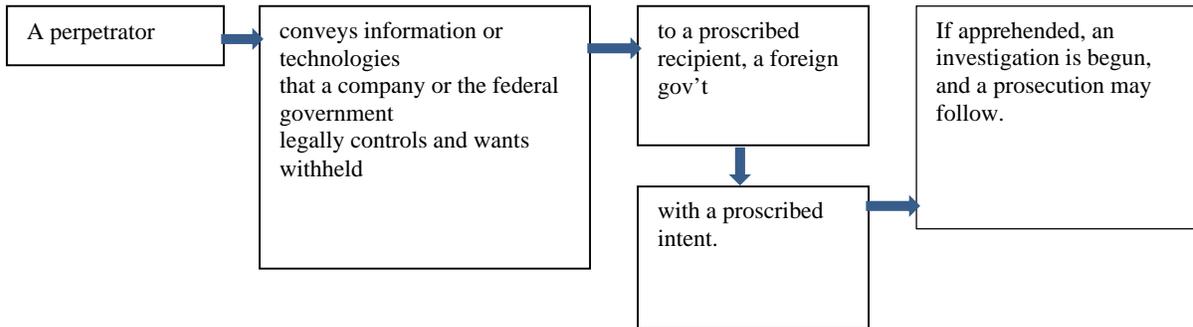
### **Enforcement of Export Control**

Enforcement of export control statutes is in large part the responsibility of the Counterintelligence and Export Control Section (CES) in the Department of Justice's National Security Division (NSD). This is the same legal section that handles enforcement of the FARA, which was discussed earlier in the Acting as a Foreign Agent chapter. According to its website,

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

the CES supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology. The Section has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy (United States Department of Justice, “Counterproliferation overview,” 2015).

Putting the response to export control violations in the counterintelligence section of DoJ’s National Security Division demonstrates the federal government’s appreciation that these violations endanger the national security as well as the economic advantages of the United States. When a person illegally exports a military technology, a dual use article, or information that falls under export control, in effect they commit espionage, in impact if not currently in name. The model that illustrated classic espionage earlier in this report also can illustrate the basic elements of export control violations.



**Figure 7 Export Control Violations in a Model of Elements of Espionage**

In Figure 7, proscribed recipients of controlled exports would include countries specified by name under declared IEEPA emergencies since 1979 that continue in place, including Syria, North Korea, and Lebanon. Other proscribed countries are listed by the various regulatory agencies that publish lists of specific denied exports or that fall under general trade sanctions. Lists include the DoS’s “U.S Embargo Reference Chart” and the DoC’s “Denied Persons List” and “Entity List.” China, Iraq, Libya, Syria, Sudan, and many others are found on these lists. Some defense items are proscribed for export to virtually any foreign government. Proscribed intent is specified in the three statutes governing export control under discussion here, which criminalize transferring controlled items or information without the evaluation of regulators and their grant of authorization with an export license (United States Department of State, 2015; United States Department of Commerce, 2015a; Department of Commerce, 2015b).

The DoD agency tasked with documenting the foreign collection threat to American industries also considers export control violations to be a type of espionage. To pursue its mission to “secure the nation’s technological base,” the Defense Security Service (DSS) oversees and monitors the thousands of contractor companies that

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

have been granted facilities clearances by the federal government to handle classified or sensitive information. DSS collects reports from these cleared contractors on attempts by foreign individuals or governments to acquire controlled information or technologies. DSS analyzes and compiles these reports in an annual publication that documents trends in foreign collection efforts, in order to raise awareness of this threat and improve countermeasures. The 2014 version of this report, titled “Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting,” notes that “Cleared contractor reporting provides information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversion activities,” and where warranted, DSS refers such reports to counterintelligence and law enforcement authorities for prosecution (United States Department of Defense, Defense Security Service, 2013).

DSS sponsors the Center for Development of Security Excellence (CDSE), a security education and training organization, which provides courses for professional advancement and certification of security personnel and the larger security community. One of CDSE’s website pages, titled “Understanding Espionage and National Security Crimes,” explains that

U.S. defense information comprises more than just classified information. Targeting of defense information has included dual-use technology, military critical technology, sensitive company documents, proprietary information, and Export Administration Regulation (EAR) or International Traffic in Arms Regulation (ITAR) controlled technology....ITAR and EAR are export control laws whose broad scope extends to products, software, technical details, and services, and includes both military and commercial items (United States Department of Defense, Defense Security Service, Center for Development of Security Excellence, 2015).

The Center goes on to explain that “along with traditional espionage and economic or trade secret espionage, ITAR and EAR violations must be reported to DSS by DOD security personnel for follow-up actions” (Department of Defense, Defense Security Service, Center for Development of Security Excellence, 2015).

Nine persons among the 209 individuals under study in this report violated export control laws because they transmitted restricted defense technologies or information. Table 20 lists them by cohort, shows the information they compromised or attempted to compromise, their citizenship and level of clearance, and lists the countries that benefitted from their espionage.

VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

**Table 20**  
**Individuals Convicted of Export Control Violations**

<b>Name/Yr Began Espionage</b>	<b>Citizen-ship</b>	<b>Clearance</b>	<b>Recipient</b>	<b>Type of Information Passed</b>
<b>Began 1947-1979 0 individuals</b>				
<b>Began 1980-1989 4 individuals</b>				
Ali, A. 1987	natural -ized	none	Yemen	Night vision goggles, chemical weapons suits, body armor, plus classified documents
Hoffman, R. 1986	native	TS	Japan	Software used to track missiles or rockets using exhaust plumes.
Kota, S. 1985	natural -ized	none	Soviet Union	Mercury cadmium telluride missile detectors; radar absorbing paint for stealth technology; biotechnology used to produce a synthetic hormone.
Mak, C. 1983	natural -ized	S	China	Electric-powered propulsion system; solid-state power switch for warships and submarines.
<b>Began 1990-2015 5 individuals</b>				
Gowadia, N. 1999	natural -ized	TS/SCI	China, Israel, Germany, Switzerland; attempted to Austria, Lichtenstein, 2 others unidentified	Exhaust systems for B-2 bomber; stealth avoidance using infrared sensors; radar-evading stealth exhaust nozzle for cruise missiles.
Knapp, M. 2009	native	none	Attempted to Iran, Russia	Anti-gravity flight suits; survival radios; F-14 fighter pilot ejection seats; an F-5B Tiger II fighter jet airplane
Roth, J. 2004	native	none	China	Plasma actuators for flight controls in automated weapons systems (drones).
Sherman, D. 2004	native	none	China	Plasma actuators for flight controls in automated weapons systems (drones).
Shu, Q. 2003	natural -ized	none	China	Cryogenic fueling system for space launch vehicles used in launch of satellites or space stations.

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

Eight of the nine individuals listed in Table 20 were convicted of violating, attempting, or conspiring to violate the AECA, the EAA, or the IEEPA. Further convictions for money laundering, income tax evasion, filing false tax returns, falsification, wire fraud, lying, and bribery of foreign officials piled up against them. Two were also charged as agents of a foreign government, Amen Ali and Chi Mak. One was convicted of classic espionage as well as of export control violations, Noshir Gowadia, and another, Subrahmanyam Kota, was initially charged with classic espionage but later saw his charges reduced.

Kota had founded a software development company in Boston. Starting in 1985, he also developed a network of friends that worked in defense industries and were willing to collect information for him. Since he had no access himself, these friends could access for him sensitive or classified defense technologies, which he in turn sold to the Soviets. He sold missile detection technology and stealth radar coatings for thousands of dollars.

Kota was caught in an FBI sting in 1994 while he was attempting to sell an international biotechnological breakthrough consisting of specialized cells from bioengineered hamster ovaries used to make an expensive drug that would stimulate human red blood cell production. In exchange for Kota's cooperation against an accomplice, prosecutors dropped the two espionage charges against him, and allowed him to plead guilty only to selling stolen biotechnology and income tax evasion (Still, a jury later acquitted the accomplice, while the KGB agent whom the FBI had identified as the waiting buyer, returned unhindered to the Soviet Union). While many of the technologies Kota compromised were clearly sensitive or classified and defense-related, through these maneuverings he avoided prosecution on espionage or export control charges (Apodaca, 1995; Rakowsky, 1995).

The nine individuals listed in Table 20 were similar in some ways but not in others. Citizenship did not define them: four were native-born, five were naturalized citizens. Their levels of security clearance varied: three held clearances (Hoffman a Top Secret, Mak a Secret, and Gowadia a TS/SCI at various stages of his career), but the other six had no security clearances. Information and technologies can be designated "restricted" on the CCL or the USML and thus require an export license, yet not be classified. With dual use technologies, a designation could depend on whether a commercial or military source was sponsoring and funding the research and development, as well as on the stage of the item's development when it was compromised. Recipient countries from these nine persons included several avid collectors of American military technologies, such as China (recipient in five of the nine cases), the Soviet Union or Russia in two cases, and Iran in one. However, other recipients were neutral or allied with the United States, including Israel, Yemen, Japan, and various close allies of the United States that Gowadia approached.

Seven of the nine individuals were contractors to the federal government; only Ali, who ran a cigarette store and Knapp, who was unemployed after losing a job in

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

human resources, were not. All seven of the contractors were scientists or other highly trained professionals: Hoffman was a proverbial rocket scientist and a physicist who worked on propulsion; Kota was a computer software engineer; Mak was an electrical engineer; Gowadia was an aeronautical design engineer; Roth, and his former student and protégé Sherman, were electrical engineers and plasma scientists; and Shu was an internationally recognized physicist working with cryogenics. All nine individuals acted primarily for money. In addition, two were motivated by divided loyalties (Ali and Mak—both of whom worked directly for the intelligence services of their foreign government sponsors); two were motivated by disgruntlement (Hoffman and Knapp); and four of the scientists sought recognition and career advancement as well as money (Gowadia, Roth, Sherman, and Shu).

Marc Knapp was discussed earlier as an example of someone who held no security clearance and who attempted to transmit restricted but unclassified information and equipment. He was also an example of someone who was prosecuted for violating export control statutes. Working with an FBI undercover agent whom Knapp thought was an arms broker, for 8 months in 2009 and 2010 Knapp procured restricted military hardware and evaded export control regulations, trying to make money by selling it to Iran or Russia. Among other gear, he offered pilot ejector seats, emergency survival locator radios, anti-gravity flight suits, and an F-5B Tiger II fighter jet. He pled guilty to violating the IEEPA,<sup>60</sup> Executive Order 13222 that continues the EAA in force, and the AECA. Convicted, he was sentenced to 46 months (3 years and 10 months) in prison (Department of Justice, 2011; United States Immigration and Customs Enforcement, 2011).

Noshir Gowadia committed both export control violations and classic espionage at the end of what had been a productive and successful career in aeronautical engineering. Born in India, Gowadia came to the United States in the 1960s for postgraduate studies having already, he claimed, earned a Ph.D. at the age of fifteen. He began working for Northrop Corporation in 1968 and became a naturalized American citizen a few years later. Northrop was then developing the highly classified B-2 Spirit “stealth” bomber that combined various technologies to make it virtually undetectable to an adversary’s radar and heat sensors. Gowadia focused on what became his area of specialization, the problem of hiding the infra-red signature from the B-2 bomber’s jet propulsion. As the company merged to become Northrop Grumman, he continued on there, staying for 18 years and becoming the acknowledged expert on nozzle design until he left in 1986 (United States District Court for the District of Hawaii, 2007).

For the 16 years following his retirement from Northrop Grumman, Gowadia joined the ranks of professionals hustling to piece together an income. His consulting

---

<sup>60</sup> IEEPA is at Title 50, U.S.C. sections 1702 and 1705c; the E.O 13222 is at Title 31, C.F.R. sections 560.204-560.205; the AECA is at Title 22, U.S.C. sections 2778(b)(2) and section 2778(C), and Title 22, C.F.R. sections 121.1, 123.1, and 127.1.

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

company served as the base from which he marketed his expertise in aeronautics and stealth design. His past experience allowed him to win contracts with DARPA and several other government agencies and military services, work a stint at Los Alamos National Laboratory in New Mexico, serve as an adjunct professor at three different universities, and persistently seek and sometimes win international contacts (United States District Court for the District of Hawaii, 2007).

In the 1990s, Gowadia deepened his international presence by setting up two overseas companies, one in Lichtenstein, a tax-friendly place from which to solicit contracts in Europe and to stash the earnings from them, and one in Canberra, which he opened with a former Australian Navy lieutenant-commander. The Australian venture began from an initial nibble, an invitation from the Australian Defence Force (ADF) to Gowadia to give a two-day seminar on stealth design. Pleased with his talk, officials encouraged Gowadia to set up a local company, and then took a large bite by paying him \$1M (Australian) between 1999 and 2003 for his services, which included studies, training, and consulting on tests that applied his designs to the Australian C-130 transport plane. In 2003, however, negotiations over expanding Gowadia's work to other Australian aircraft failed because he demanded 100% ownership of any intellectual property that would be developed from such a venture (McKenna, 2010).

In 1999, as he had begun to spend more time in Australia, Gowadia bought oceanfront land on Maui. In 2002, he finished building a lavish home there that sported a roofline shaped like a B-2. Months later, when the contract with the ADF collapsed, he faced a nearly \$15,000 monthly mortgage on his new house without commanding some of the income he had expected would pay for it. As he had been doing for decades, he fell back on selling his expertise, but this time he focused on the Chinese (McKenna, 2010; Boylan, 2005).

His initial tentative contacts with them had already begun in January 2002 through a "Chinese access agent" named Henry Nyoo; these led to conversations with an official from the Chinese State Bureau of Foreign Exports, Tommy Wong. Wong and Nyoo worked the aeronautical research centers in the PRC to market Gowadia's offer to provide the Chinese with information and consulting services on how to develop their stealth capability for the Chinese air force. On July 29, 2003, Gowadia, Nyoo, and Wong flew to Hong Kong and then to Chengdu, the center of research and development in China for fighter aircraft and cruise missiles. Gowadia spoke and made a PowerPoint presentation proposing to work with them on "low observable" propulsion systems—a presentation that included U.S. national defense information restricted from export and classified at the Secret level (McKenna, 2010; United States District Court for the District of Hawaii, 2007).

Over the next 2 years, he made at least five more trips to the People's Republic of China (PRC). Between trips, he emailed classified data to the Chinese engineers he worked with, evaluated and corrected their test results, advised them on how to improve their testing and measurement facilities, oversaw the design of a nozzle for

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

a cruise missile that would make it difficult to detect by radar, and provided the Chinese with classified flight test data that helped them modify their cruise missiles by showing them what “the exact ‘lock on range’ of a new Chinese missile would look like ‘from a pursuing U.S. air-to-air missile’” (Gordon, 2005). According to Dean Wilkening, director of a science program at Stanford University’s Center for International Security and Cooperation, “The reason foreign governments would like this [stealth] technology is if they reverse engineer it, they can apply this to their fighter aircraft [and] if you do that, our air-to-air missiles don’t work very well. They can’t find the target.” (United States Department of Justice, United States Attorney Edward H. Kubo, 2006; Gertz, 2006; Gordon, 2005).

Gowadia was arrested on October 26, 2005 after spending 10 days in voluntary interviews with the FBI. His house was searched, where many classified documents and reports were found (Macavoy, 2008). He signed statements admitting to having willfully conveyed national defense information to a person not entitled to receive it (Boylan & Perez, 2005; Dooley, 2009b). From the initial sole charge, the investigation into Gowadia’s activities mushroomed over the next 5 years, generating thousands of pages of classified evidence, during which time he remained in jail without bail as a flight risk. After the first charge was filed, increasingly more serious indictments were handed down later in 2005, in 2006, and again in 2007 as the investigations expanded around the world (United States Department of Justice District of Hawaii, 2010). While he remained in jail, his defense lawyers requested an evaluation for mental problems that could have made him incompetent to stand trial. The report on his psychological evaluation determined that he did suffer from a “narcissistic personality disorder,” but a judge ruled in February 2010 that his grandiosity would not make him incompetent to stand trial, and it began on April 13, 2010 (Sample, 2009; Associated Press, 2010).

Prosecutors announced during Gowadia’s trial that the Chinese government had paid him \$15,000 on his first trip there, and later sent payments that brought the total to \$110,000 to his secret Swiss bank accounts. These he had set up from Lichtenstein in the name of his fake charitable foundation for children. Gowadia distributed no money from his charity to any actual children. While he was working for the Chinese in 2002 and 2004, he had also sent classified information to the Swiss government and to businessmen in Israel and Germany with marketing offers suggesting he could apply stealth technology to various aircraft in those countries. He made other offers and disclosures to additional unspecified countries—Gowadia had approached eight countries in all (United States District Court for the District of Hawaii, 2007; Department of Justice, 2011).

Although his defense attempted to prove that the information and services he had admittedly shared with the PRC had not been classified but were instead publically available, Gowadia’s initial confession was difficult to overcome in court (Dooley, 2010; “Accused spy sold nothing secret,” 2010). He had signed a statement admitting that he had

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

disclosed classified information and material both verbally and in papers, computer presentations, letters, and other methods to individuals in foreign countries with the knowledge that information was classified... The reason I disclosed this classified information was to establish the technological credibility with the potential customers for future business. I wanted to help these countries to further their self aircraft systems. My personal gain would be business (Gertz, 2006).

He was convicted on fourteen counts, including two counts of willfully communicating classified national defense information to the PRC with the intent that it be used to the advantage of the PRC or to the injury of the United States; three counts of willfully communicating classified national defense information to persons not entitled to receive it in the PRC and elsewhere; one count of illegally retaining defense systems information at his Maui residence; four counts of exporting technical data related to a defense article without an export license in violation of the AECA; one count of conspiracy to violate the AECA; one count of money laundering based on proceeds from the AECA violations; and two counts of filing false tax returns for the years 2001 and 2002. Testimony revealed that he had not paid any federal income tax in the years between 1997 and 2005, and although it was difficult to sort out the laundered money, his private consulting firm had earned at least \$750,000 between 1999 and 2003 (Department of Justice, 2011; Boylan, 2005).

On January 24, 2011, Gowadia was sentenced to 384 months (32 years) in prison and was initially sent to the supermax penitentiary in Florence, CO. In that same month, the existence of a new Chengdu J-20 Chinese stealth fighter plane was announced to the public (Dsouza, 2012). At Gowadia's sentencing hearing the prosecutor, Assistant U.S. Attorney Ken Sorenson, said

This case was unique in that we litigated know-how, the very concept of exporting your knowledge base that you derive, in whole or in part, from your activities working in United States classified programs. If you can take that and go sell it or market yourself on an international stage in secrecy to other governments and not suffer criminal sanctions for it, then we're in trouble (Niese, 2010).

Gowadia was an example of someone who both illegally exported defense information and services and, at the same time, knowingly transmitted classified national defense information to a foreign government for its advantage. Thus he is coded as both a case of classic espionage and a case of export control violations. He also provides an example of someone who worked on important government technologies and sought to sell his expertise through espionage. He saw what he was doing as helping the Chinese. "On reflection," he wrote in a statement written after his arrest, "what I did was wrong to help [the] PRC make a cruise missile. What I did was espionage and treason" (Dooley, 2009a).

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

Quan-sheng Shu, on the other hand, also was trying to help the Chinese and enrich himself in the process, but the information he transmitted was not classified national defense information, rather it was only restricted from export by the export control laws. Between January 2003 and October 2007, Shu attempted to broker a three-way deal worth \$4 million between the Beijing Special Engineering Design Research Institute (BSEDRI) in the PRC, an unnamed French company in Paris, and Shu's sole-proprietor company, AMAC International, Inc., in Newport News, Virginia. He did not realize that for most of that time he was being watched, tracked, and listened in on by the FBI, Immigration and Customs Enforcement (ICE), and DoC's Office of Export Enforcement (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

Shu was born in Shanghai, attended college in Beijing, and earned a Ph.D. in physics in 1970 at the Institute of Low Temperature in Hangzhou, China. He launched his professional career in cryogenics (i.e., low temperature physics) in China, working at the Institute itself for 7 years, then becoming an Assistant Professor and in 1985, a full Professor of Physics at Zhejiang University in Hangzhou. Starting in 1983, he began to divide his time between his academic duties in Hangzhou and various research positions in the United States, first at the University of Washington in Seattle, then at the Fermi National Accelerator Laboratory near Chicago. In 1998, Shu became a naturalized American citizen and in that same year he incorporated his company in Virginia. AMAC competed for small business research grants to do specialized research in cryogenics for government agencies including the Department of Energy and the National Aeronautics and Space Administration. AMAC maintained a second office in Beijing (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

One research grant allowed Shu to hone his company's expertise in the cryogenic transfer and storage technology of liquid propellants that were used in aerospace applications. AMAC developed an energy-efficient cryogenic transfer line with magnetic suspension for National Aeronautics and Space Administration's (NASA) Kennedy Space Center that promised to extend space missions, save cryogenic fuel, and reduce overall launch mass. Projects like this enhanced AMAC's international reputation (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

As part of its extensive modernization effort, in the early 2000s the PRC began to plan its fourth and newest space launch facility on the island of Hainan. This would house heavy payload launch vehicles designed to send space stations and satellites into orbit. The facility would also provide support for manned space flight and future lunar missions. When Chinese astronauts walk on the moon, they will be launched from Hainan (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

Such space vehicles use a combination of liquid hydrogen and liquid oxygen as their fuel, and these require very low temperatures to produce, store, and use them. Shu offered to assist in China's systematic expansion of their space program at Hainan by providing his technical expertise in cryogenics and his knowledge of where and how to acquire foreign technology for cryogenic pumps, valves, transfer lines, and refrigeration equipment—all of the components that would be necessary to produce liquefied hydrogen and oxygen at the launch facility. Shu relied on emails and phone calls to court high-ranking BSEDRI officials and officers of the 101 Institute, which was tasked with implementing the project, from his offices in Beijing and Newport News. He also helped to arrange for PRC officials to visit various European space launch facilities and hydrogen production and storage facilities, so they could see the best examples of such facilities for themselves (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

Starting in January 2003, every few months Shu began shuttling between the PRC, the AMAC office in Newport News, and Paris. By August, he had Chinese approval to provide technical design work, and by November he had entered the bidding on the project, proposing that AMAC would be the broker between the Chinese and the unnamed French company that would actually provide the equipment and test it. He would provide the expertise in cryogenics along with the Chinese language and cultural awareness needed in the role of international broker. Through 2004 and 2005, Shu followed the evolving project and kept the French apprised of changes and new opportunities. Between December 2005 and January 2007, he actively negotiated a deal in which the PRC would buy liquid hydrogen tanks and associated equipment from the French company, and for its services AMAC would receive a commission from the French. On January 15, 2007, the contract was finalized, and soon thereafter Shu received the first two wire transfers from Paris totaling \$253,962. Eventually he would receive \$386,740 (United States Department of Justice, Federal Bureau of Investigation, "Redacted affidavit," 2008; United States Department of Justice Eastern District of Virginia, Press release, 2008).

The negotiations had been delicate. Shu directed his employees to make up the names of end-users to be entered on export paperwork, rather than admitting that the Chinese military would be using the technology, because there was a U.S. embargo on exporting such data and articles to the PRC. To one of his employees in Beijing, he explained that the Chinese would not be telling the French company everything, because the actual use for the product would "involve the military aspect," and this fact would not be released to outsiders. He warned the French not to include too much detail in their specifications, lest the Chinese be able to reverse engineer the equipment and manufacture it for themselves, cutting AMAC and the French out of the deal.

Kickbacks were an expected part of the transaction. Shu offered to three key PRC officials 3% of the estimated \$4 million the deal would represent, but there was

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

haggling: Chinese officials suggested that German and Russian bidders were offering 5%, while the senior Chinese official passed the word that he would require an additional 2%, along with Shu's assurances to him that no other Chinese officials would know about this additional 2% sweetener—a suggestion having been passed along to Shu from the very Chinese officials that were not supposed to know about it (United States Department of Justice , Federal Bureau of Investigation, Redacted affidavit, 2008)<sup>61</sup>.

As Shu was pulling these threads together into a deal, on July 21, 2006, two Special Agents from the DoC's Office of Export Enforcement walked into the AMAC offices in Newport News and announced that they were there to give Shu an "outreach briefing." They explained to Shu that brokering an export deal between an embargoed country (China) and a foreign nation (France) itself counted as an American export. This briefing was to serve as a refresher on the export control regulations and, one would assume, also as a warning that the potential exporter was being watched. Shu responded by simply trying to be a more careful dissembler. He told an employee to make up end-users and uses entries on reports because

...if we said that was for launching satellites, we wouldn't be able to get that 101 [Institute] deal that's worth three million...Everyone hides it...In the end, the manufacturers also help to hide it. The French, also. If you said you wanted to launch, eh, rockets or something, then France won't be able to sell to you...France belongs to NATO....Let me tell you, that's how the military industry buys things. Right, we've done military industry business (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

Shu was arrested on September 24, 2008, and charged with (1) unlawfully and willfully exporting a defense service [cryogenics expertise, advice, and brokering services] to the People's Republic of China without a license, in violation of the AECA (22 U.S.C. § 2778), as implemented by the ITAR, (22 C.F.R. Chapter 1, Subchapter M, Parts 120-130); (2) unlawfully and willfully exporting a defense article [technical data in a document he sent to the Chinese] in violation of the AECA (22 U.S.C. § 2778), as implemented by the ITAR, (22 C.F.R. Chapter 1, Subchapter M, Parts 120-130); and (3) willfully bribing, offering a bribe, and attempting to bribe, a foreign government official, in violation of the Foreign Corrupt Practices Act (15 U.S.C. §§ 78dd-1 and 78dd-2). (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

---

<sup>61</sup> The FBI's "Redacted Affidavit of Criminal Complaint and Arrest Warrant for Shu Quan-Sheng" dated September 19, 2008, reproduces verbatim many of Shu's verbal interactions with his employees, the Chinese, and the French based on telephone and email monitoring by the investigators. The affidavit is widely available online.

## **VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE**

After 2 months, he pled guilty to all three charges, and on April 2, 2009, he was sentenced to 51 months (4 years and 3 months) on each count, to be served concurrently. He also paid back some \$387,000 in restitution to the federal government. “America has provided me with such a wonderful working environment and opportunity,” Shu said at his sentencing hearing, “I would never deliberately harm the country I love” (Potter, 2008).

What Shu did was a type of espionage; his offenses can be described in terms of the classic espionage categories that previously have been applied in this report to other types of espionage, and were discussed earlier. These are:

- A context of competition. The United States and the PRC are engaged in economic, military, and ideological competition for international advantage. Counterintelligence officials and China experts point to the PRC as one of the most effective and persistent collectors of American economic and technological information and a growing threat (Hannas, Mulvenon, & Puglisi, 2013).
- Secret means. Shu tailored the information he shared with each player in his deal, keeping some aspects secret from the other and warning them not to be too transparent with each other. However, he used typical electronic means of communication—email, fax, and phone calls—to make and keep in contact with his clients (United States Department of Justice, Federal Bureau of Investigation, “Redacted Affidavit,” 2008).
- Goal is secrets. The data and the expertise Shu gave to the Chinese were not classified national defense information, but were restricted on the USML. In addition, the United States has had a trade embargo against the PRC since 1989 because of the Tiananmen Square massacre, making brokering any trade deal with the PRC another clandestine activity (McGlone, 2008b).
- Political, military, economic secrets. The data and expertise Shu offered related to essential elements of a technology needed to launch heavy payload space vehicles such as satellites, space stations, and rockets heading for the moon or distant planets. The Chinese are developing their capabilities in space technologies and thereby challenging the United States’ supremacy in space, which has political, military, and economic implications for the American programs (United States Department of Justice, The Eastern District of Virginia, 2008).
- Theft. Shu is not reported to have committed theft in the course of his other crimes.
- Subterfuge. Shu repeatedly advised each of his two clients to withhold information from the other. He asked his employees in Beijing to use only fax to communicate with him because he did not want to let his American employees know all the details of his deals. He asked to communicate directly with Chinese officials rather than go through his employees in Beijing because he did not want them know all the details. He directed his employees to falsify export control forms with fake end-user names and uses for articles in order to evade

## VIOLETIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

export control regulations. When AMAC drafted a letter of invitation to go from the French company to officials at Institute 101, to facilitate the PRC officials getting a visa to visit France, AMAC explained that since this was confidential, the Institute 101 (a military agency) would not be named on the application, and the fictitious name of “China Great Wall Industry Corporation” would be issuing the invitation instead. In a phone conversation with an AMAC employee, Shu explained that “Everyone hides it [the military end use]” (United States Department of Justice, Federal Bureau of Investigation, Redacted Affidavit, 2008).

- Surveillance. Shu is not reported to have gathered information through surveillance, although he did engineer visits to similar space installations for his clients.
- Psychological toll. Shu appeared shocked when he was arrested and charged with serious export control violations. He seems to have regarded his activities as typical business dealings and, despite receiving explicit warnings in person, did not recognize that American authorities would see what he was doing as a crime. Observers reported that he appeared “shaking and bewildered” at his initial court appearance. (McGlone, 2008a).
- Illegal. Shu was convicted of two counts of export control violations and one count of attempting and actually bribing foreign officials, and was sentenced to prison and required to pay restitution (Potter, 2008).

## ECONOMIC ESPIONAGE

### ECONOMIC ESPIONAGE

Given its name, it would seem obvious that economic espionage is indeed espionage. It may be necessary, however, to explain how economic espionage can be committed against the United States by Americans. Economic espionage shares the basic categories and is intertwined with other types of espionage, yet there are unique elements in economic espionage that make it a fifth type and distinct from the four other types previously discussed in this report, which were classic espionage, leaks, foreign agent activities, and violations of export controls.

The phrase “economic espionage” is often not exact. One may see it used interchangeably with “industrial” or “corporate” espionage. Most often, economic espionage refers to theft of information by or for a foreign government, a loss which could have implications for the whole economy of a nation, while “industrial” or “corporate” espionage typically refers to theft from one company by another. Although domestic, such thefts may also have far-reaching impacts on the economy.

#### Trade Secrets

One of its unique elements is that the target of economic espionage is a trade secret and not, as in classic espionage, controlled government or military secrets about intentions, capabilities, plans, or technologies. Usually the secrets in classic espionage are controlled by classification. A trade secret, on the other hand, is intellectual property that was created by a business, which takes steps to keep it a secret, and from which the business derives value because it is not publicly known. A trade secret is not classified by the government, because the government does not own it.

The varieties of trade secrets are vast. They include

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public (Economic Espionage Act, 1996).

Any enterprise can create, declare, and control its own trade secrets. It defines the secret, and determines the value to itself of the intellectual property it has created. A government agency does not determine its value or its legitimacy, as is the case with patents or licenses to export. So, why does the government get involved in helping to secure the secrets of businesses, which typically have their own corporate security programs? As democratic capitalism has evolved in the United States, the government assumed the role of the neutral arbiter to foster a fair and open marketplace, subject to the rule of law. To that end, it provides rules—through laws and regulation—for the conduct of business, and it provides sanctions for not following the rules (Heskett, 2009).

Until 1996, the only choice for prosecuting unlawful misappropriation of trade secrets was under state laws, and because state laws varied, inconsistencies developed. Gradually, starting in the 1980s, all but four states adopted the Uniform Trade Secrets Act (UTSA), in which Congress provided a model law with uniform definitions and approaches that could apply across states, and these inconsistencies were reduced (United States House of Representatives, Committee on the Judiciary, “Trade Secrets” 1996).

By the mid-1990s, however, as (1) more and more intellectual products came to be created and stored electronically on information technology, and (2) globalization knit together the markets of the world and made competition global, alarm over the increasing theft of trade secrets led Congress to focus on this issue, and consider the Economic Espionage Act of 1996. It was the first federal statute to address economic espionage.

The legislation acknowledged an emerging reality: the success of private enterprise in the United States was becoming so important to national security that the federal government needed to protect it. If competitors, and especially if foreign governments, could steal American trade secrets with impunity, the advantages for national security that economic strength conferred could be lost (United States House of Representatives, Committee on the Judiciary, “Trade Secrets” 1996). This is a second element of economic espionage that makes it unique among the various types of espionage: the federal government takes some responsibility for protecting secrets that were created and are owned by private companies.

The United State House of Representatives Committee on the Judiciary debated the legislation that became the Economic Espionage Act (EEA). In its report to the House in September 1996, it recommended quick passage of the proposed law and explained in urgent terms the concerns that had prompted them to act:

As the nation moves into the high-technology, information age, the value of these intangible assets [i.e., trade secrets] will only continue to grow. Ironically, the very conditions that make this proprietary information so much more valuable make it easier to steal. Computer technology enables rapid and surreptitious duplications of the

## ECONOMIC ESPIONAGE

information. Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner.

This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft. The information is pilfered by a variety of people and organizations for a variety of reasons. A great deal of the theft is committed by disgruntled individuals or employees who hope to harm their former companies or line their own pockets. In other instances, outsiders target a company, systematically infiltrate it, and then steal its vital information. More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies.

The term economic or industrial espionage [the terms are used interchangeably here] is appropriate in these circumstances. Espionage is typically an organized effort by one country's government to obtain the vital national security secrets of another country. Typically, espionage has focused on military secrets. But as the cold war has drawn to a close, this classic form of espionage has evolved. Economic superiority is increasingly as important as military superiority. And the espionage industry is being retooled with this in mind.

It is important, however, to remember that the nature and purpose of industrial espionage are sharply different from those of classic political or military espionage. The phrase industrial espionage includes a variety of behavior--from the foreign government that uses its classic espionage apparatus to spy on a company [This concern would be addressed in Section 1831 of the Act], to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics [These concerns would be the focus of Section 1832 of the Act]. All of these forms of industrial espionage are problems. Each will be punished under this bill.

Other countries treat the relationship between their national governments and their national economies differently than does the United States, and this difference fuels some of the most aggressive economic espionage against the United States. There is a spectrum across nations of how closely states' economies and governments are aligned. In the former Soviet Union and the early People's Republic of China, with their Communist ideologies, the economy and the state were essentially the same. Both of those nations have moved away from their strict Communist polities, and they have incorporated versions of capitalism, but they continue to operate under economic nationalism, in which the central Party tries to control and direct the private enterprise that it does allow. American allies also fall in various places along

this spectrum, and not all of them resemble the United States. For example, the French government controls over half of the industrial base in France, and it can be an assertive collector of economic intelligence. Such nations may gather intelligence from foreign companies to convey advantages to their own nation's companies, and they see this as a legitimate role for their governments (Lotrionte, 2015).

On the other hand, the United States espouses a position at the other end of the spectrum, which emphasizes a separation from and minimal interference with private enterprise by government. This has led the United States to declare that it will not use the intelligence apparatus of the federal government to conduct economic espionage against other nations for the benefit of American companies. In 2013, then Secretary of Defense Robert Gates reaffirmed this approach, saying that he refused to slide into what he called “the moral and legal swamp” of economic espionage (Lotrionte, 2015)<sup>62</sup>. The EEA was intended, in part, to protect American trade secrets from the ever more sophisticated theft of trade secrets by the intelligence-gathering operations of other nations (Foreign Press Center Briefing Transcript, Woolsey, 2000)<sup>63</sup>.

### **The Economic Espionage Act of 1996**

The EEA criminalizes two related activities: economic espionage in Title 18 section 1831, and the theft of trade secrets in Title 18 section 1832. Section 1831, economic espionage, is the statute most directly relevant for this study since it implies foreign involvement, although in practice, the two sections are sometimes related to one another<sup>64</sup>.

Section 1831 provides:

---

<sup>62</sup> Catherine Lotrionte's discussion of the relationship between classic and economic espionage is subtle and comprehensive, and it considers the ways in which the United States does collect economic intelligence against other countries (as opposed to engaging in economic espionage against them) and how it does seek to help American companies in activities such as trade negotiations. One of the vexing aspects cited by Gates of the government doing economic espionage on behalf of American companies would be deciding which companies to advantage. See Catherine Lotrionte, “Conquering state-sponsored cyber-economic espionage under international law,” *North Carolina Journal of International Law*, 40(2), Winter 2015, 443-541.

<sup>63</sup> James Woolsey's statement to the foreign press in 2000 gives the American position that the government does not engage in economic espionage, except in three instances: potential nuclear proliferation, monitoring sanctioned nations that hide their activities, and uncovering bribery that distorts competition unfairly. See Foreign Press Center Briefing Transcript, “Intelligence gathering and democracies: The issue of economic and industrial espionage,” briefing by James Woolsey, March 7, 2000.

This paragraph only skates across the surface of the broad topics of economic and political change before and since the fall of the Soviet Union, and the impact of increasing globalization since then. It is intended only to mention some relevant topics as starting points for understanding the context of economic espionage. The discussion in Robert Gilpin with Jean Millis Gilpin, *The challenge of global capitalism*, (Princeton, NJ: Princeton University Press, 2000), discusses that context.

<sup>64</sup> Here the elements in the federal law on economic espionage are taken as the definition and scope of economic espionage. However, other authors define the term economic espionage differently or more broadly.

## ECONOMIC ESPIONAGE

“(a) IN GENERAL.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; [or]

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; [or]

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; [or]

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than \$5,000,000 or imprisoned not more than 15 years, or both.

(b) ORGANIZATIONS.—Any organization that commits any offense described in subsection (a) shall be fined the greater of \$10,000,000 or three times the value of the trade secret to the organization” (Economic Espionage Act, as amended, 1996; White & Case Technology Newsflash, 2013).

The designation of a “foreign instrumentality” as one of the proscribed recipients of economic espionage, in addition to a foreign government or a foreign agent, is meant to cover entities that are directed by a foreign government but may not be publicly linked to it. As defined in the Act, a foreign instrumentality would include “any agency, bureau, ...component, institution, association, or any legal commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government (Economic Espionage Act, 1996; Reilly, 2009). For example, a careful description of the many types of “instrumentalities” that operate in the PRC in shades and mixtures of academic, research, corporate, military, and government auspices is found in a collection of essays titled *Chinese Industrial Espionage*, which demonstrates why it was necessary to include this category of recipient that may be deliberately obscuring its affiliations (Hannas, Mulvenon, and Puglisi, 2013).

Section 1832, on the other hand, deals with domestic trade secret theft. It resembles Section 1831 in that it criminalizes the misappropriation of trade secrets, but in 1832 there is no nexus required to a foreign government, and instead there are several additional provisions. Section 1832 deals with corporate or industrial

espionage, carried on between American companies. It is the theft of trade secrets from one company by another company, or by employees of that company. A complication not addressed by the EEA in either of these two main sections is that of the American company which maintains offices overseas. Unless an overseas theft was committed by an American citizen, it is not protected under the Act (Simon, 1998).

Section 1832 provides that:

“(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than \$5,000,000” (Economic Espionage Act, 1996).

While the two sections share a focus on protecting trade secrets, they differ in several important ways. One difference is in how they specify what the intent of the perpetrator must be. Section 1831 requires only that a person “intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly steals...” while Section 1832 requires two different intentions: (1) a person must have an “intent to convert a trade secret...to the economic benefit of anyone other than the owner thereof,” and (2) he or she must be “intending or knowing that the offense will injure any owner of that trade secret.” The thief may be but does not have to be the one who benefits from the theft, and while the beneficiary does not need to be a foreign government as in

## ECONOMIC ESPIONAGE

1831, in 1832 the beneficiary also could be a foreign government—for example, one to whom an American thief planned to convey a stolen secret as a part of expatriating to that country, even if that country’s government had not initiated the theft (“Spotlight on the Economic Espionage Act,” 2012).

A second difference between Sections 1831 and 1832 is in how the potential benefit is specified. According to the report of the House committee that drafted the legislation, in Section 1831 the benefit to a foreign government should be broadly framed. It “means not only economic benefit but also reputational, strategic, or tactical benefit (United States House of Representatives Committee on the Judiciary, “Report,” 1996). In Section 1832, however, the benefit is specifically economic.

A third difference is that since the emphasis in Section 1832 is on domestic crimes, in order to come under federal jurisdiction it must be about interstate commerce. Therefore, Section 1832 specifies that the trade secret must be “related to or a product or service used in or intended for use in interstate or foreign commerce” (“Spotlight on the Economic Espionage Act,” 2012; Simon, 1998).

A potential confusion lurks because a person convicted of offenses under Section 1832 is accurately said to be convicted under the Economic Espionage Act, yet it is actually only Section 1831, with its requirement of a foreign nexus, that is labeled “foreign economic espionage.” Section 1832, as described earlier, punishes the theft of trade secrets. It would have been clearer if Congress had named its law “Economic Espionage and the Theft of Trade Secrets,” which while closely related, yet in the terms of the Act, are not both economic espionage.

Since 1996, federal authorities have investigated and prosecuted cases under the EEA, and so have built up experience and case law. By 2009, over 100 cases of trade secret misappropriation (Section 1832) had been prosecuted, but only six cases of economic espionage (Section 1831) (Krotoski, 2009). As a guide for his fellow prosecutors, one federal prosecutor listed some common case scenarios that had emerged by that time, including the following:

- State-sponsored targeting of trade secrets and technology misappropriated with the intent to benefit a foreign government or an instrumentality of a foreign government.
- A trusted employee with access to valuable company information who, after becoming disgruntled, downloads and transmits the information to others outside the company who offer it to the “highest bidder.”
- An employee, who after learning how a new prototype is made, decides to form his own company and use the trade secret and other proprietary information to launch his own competing product.
- A competitor who devises a scheme to gain access to company information for use in fulfilling an international contract.

- Employees who execute a plan to steal proprietary information and take it to another country and are stopped at the airport.
- After being offered a senior position with a direct competitor, and before tendering his resignation, an employee uses his supervisory position to request and obtain proprietary information he would not normally be entitled to access. After taking as much proprietary information as he can, he submits his resignation and takes the materials of his former employer to his new position and employer (Krotoski, 2009).

One can discern in these scenarios the legal task of sorting out which section of the Act would best apply, economic espionage or theft of trade secrets. It may depend on the evidence that is available. One legal authority suggests that deciding whether what a company claims to be a trade secret is actually a trade secret may also be a job for the jury. He explains that “among the factors in assessing whether certain subject matter is a trade secret are the:

- extent to which the information is known outside of the company;
- extent to which it is known by employees and others involved in the company;
- extent of measures taken by the company to guard the secrecy of the information;
- value of the information to the company and to its competitors;
- amount of effort or money expended by the company in developing the information; and
- ease or difficulty with which the information could be properly acquired or duplicated by others” (Restatement (Third) of Unfair Competition §40 (1994), quoted in Thomas, 2014).

Sometimes investigators of trade secret theft have had the luxury of investigating an ongoing crime, developing their case by running an undercover agent, and collecting evidence over a period of time before arresting the suspect. But often, such cases are recognized as a theft at the last minute, and reaction by law enforcement becomes an urgent scramble to reach the airport in time to prevent the thief from getting on a plane for a foreign conference or a foreign country, where he or she plans to sell or convey the trade secret, thereby ruining its value for the owner. A trade secret has no expiration time limit, but once it is made public, its status as a trade secret is gone and that status cannot be recovered (Krotoski, 2009).

The paucity of economic espionage cases prosecuted since 1996, despite the urgency Congress expressed then and subsequently about how the draining away of American innovations needs to be staunch, has prompted critics to argue that the economic espionage section of the Act needs to be redrafted. Critics of the EEA argue that based on the Congressional debates held during consideration of the legislation, the courts have so far interpreted Section 1831 more narrowly than

## ECONOMIC ESPIONAGE

Congress intended, and this has made convictions harder to get and discouraged DoJ from bringing more cases (Kuntz, 2013).

Others explain the small number of cases by arguing that economic espionage cases are especially complex; that DoJ chooses to focus its resources on cases it is most likely to win and economic espionage does not have that track record; that there are potential diplomatic repercussions in economic espionage cases that make prosecutors cautious; and that even though the Act authorizes a trial court to issue protective orders to prevent a trade secret from being revealed during a trial, plaintiffs are still leery of a public trial where, with one slip of the tongue, their secrets could be lost (Thomas, 2014; Doyle, 2014; “Recent cases,” 2012). However, starting in 2010, DoJ shifted its priorities and has started prosecuting more economic espionage cases, while the FBI recently created an Economic Espionage Unit in its Counterintelligence Section to focus on such investigations (Coleman, 2014)

The increasing attention paid by federal authorities to protecting trade secrets reflects the ongoing evolution of the United States from its 20<sup>th</sup> century manufacturing base to a “knowledge-and-service” based economy. This shift was already recognized in 1996 and could be seen in the Congressional debate on the Act quoted earlier. Efforts by the government, and American companies themselves, to keep control over their intellectual property (IP), their innovations, their investments in new processes, their creative insights, their “intangible assets,” are not just advisable; control over them is essential for them to stay in business. One author notes that “In 1975, 16.8% of the total value of the S&P 500 reportedly consisted of intangible assets. In 2005, intangible assets reportedly constituted 79.7% of the total value of these firms” (Thomas, 2014). Economic espionage conducted by and benefitting foreign countries is not just about whether particular companies succeed or fail; it is about how the nation fares in international economic competition. When other nations steal American trade secrets to advantage their own domestic companies, in the process they disadvantage American companies and the United States itself. A student of espionage explains that

IP theft results in the loss of revenue for those who made the invention as well as the jobs associated with those losses. It also undermines the means and the incentive to innovate, slowing the development of new inventions and industries that would otherwise expand the economy and raise the prosperity and quality of life for everyone. The negative impact from IP theft on core values is global and staggering (Lotrionte, 2015).

Since 1996, when Congress thought in terms of spies pocketing “diskettes,” our widespread reliance on enhanced technologies has only grown: on computers, smart cell phones with cameras and computers, email and the Internet, flash drives and other electronic storage devices—all the appurtenances of the digital culture

and modern communications—and the ease of capture, storage, and movement of data has made controlling those valuable intangible assets ever more difficult. Thus, discussions of economic espionage usually raise two other related topics: cyber espionage (discussed further), and the possibility of insider threat (discussed in an essay in Appendix A). Employees stealing trade secrets by misusing information technology is a common way—though not the only way—in which the secrets are lost (Thomas, 2014; Office of the National Counterintelligence Executive, 2011; “Economic impact of trade secret theft,” 2014).

In what is the current total in 2015 of ten cases prosecuted under Section 1831 since 1996, some of which have involved multiple defendants, various outcomes have been reached. In six cases, defendants were convicted under Section 1831 of economic espionage; in two other cases, individuals who had been charged under Section 1831 were acquitted of that charge, but convicted of the related Section 1832 offenses. One case led to an acquittal, and in several others the defendants fled. At least five of the principal defendants were American citizens,<sup>65</sup> and of those, four were convicted under Section 1831. One of these, Walter Liew, was sentenced in July 2014, too late to be included in the data for this study of American citizens. Two others, Fei Ye (who pled guilty in 2006) and Elliott Doxer (who pled guilty in 2011), were not included in this study but will be considered for inclusion in the future.<sup>66</sup> The only individual convicted of economic espionage who is included in the data for this study is Dongfan Chung, who spied for the Chinese for at least 25 years (Krotoski & Harrison, 2015).

Dongfan (Greg) Chung was born in China in 1936, and immigrated with his family to Taiwan as the Chinese Communists came to power after World War II. He married there, moved with his wife to the United States for graduate school, and

---

<sup>65</sup> It can be difficult to ascertain from summaries available in open sources the citizenship of people accused of economic espionage or export control violations. From their names, it seems that a large proportion of these persons could be citizens of other nations, but summaries do not reliably report this fact, and sometimes they report incorrect information on the issue of citizenship. Such cases do not attract the attention of the press to the same degree that classic espionage cases do. An otherwise excellent compilation of case summaries that is published periodically by the Department of Justice, National Security Division, titled “Summary of major U.S. export enforcement, economic espionage, trade secret and embargo-related criminal cases,” the latest of which is dated August 2015, does not consistently report on the citizenship of the individuals who are discussed in its cases.

<sup>66</sup> Fei Ye, a naturalized American citizen, along with an accomplice who was a Chinese national, pled guilty to two counts of economic espionage and one count of possessing stolen trade secrets dealing with the design and manufacturing of computer microprocessors in December 2006. They admitted they intended to use the trade secrets in a company they were setting up in the PRC, a project that was sponsored and funded by provincial Chinese authorities in the region where their company would be located. Elliott Doxer, a Jewish American citizen, sent an email to the Israeli consulate in Boston in June 2006 offering to help Israel by passing along his employer’s trade secrets. Doxer worked for Akamai Technologies, which delivered content over the Internet handling between 15% and 30% of global internet traffic. In an FBI undercover sting, Doxer passed along to the agent he thought was an Israeli Akamai’s contractual papers, customer lists, and employee lists. In August 2011 Doxer pled guilty to one count of economic espionage. Both Fei Ye and Doxer received sentences of 1 year (Krotoski & Harrison, 2015).

## ECONOMIC ESPIONAGE

became a naturalized American citizen in 1972. He worked as an employee for a series of defense contractors including McDonnell Douglas, Rockwell, and Boeing. Starting in the 1960s, he served as a structural engineer on various defense projects, and eventually focused on the NASA space shuttle. For most of his later career, he did stress analysis on the forward fuselage section of the Space Shuttle, and held a Secret security clearance. In 2002, the Boeing facility where he was working relocated, and Chung retired rather than move from Orange, California, where he and his wife had built a house. However, the next year, at age 70, he was rehired as a subcontractor at Boeing to help with the analysis of the Columbia shuttle crash (United States District Court Central District of California, Indictment, 2008; Bhattacharjee, 2014).

Like many expatriate Chinese who grew up in Taiwan, Chung and his wife evolved from their initial resolute anti-Communism to curiosity about China. After Mao Zedong's death in 1976, the country began rapidly modernizing and its economy began to accelerate. The Chungs were active in a Taiwanese immigrant association, but they began to feel constrained by the strident nationalism the group expected toward Taiwan. They wanted to understand what they had missed out on because their families had left China when they were young. During the late 1970s, it became possible to meet visiting Chinese scientists at conferences in the United States, and Chung made such contacts. The Chinese government encouraged Chinese visitors to gather any technological knowledge they could from the West (Bhattacharjee, 2014).

In 1979, Chung met a visitor from the Harbin Institute of Technology. When the visitor expressed interest in problems of stress analysis, Chung generously responded by sending copies of his own graduate course notes on stress analysis via sea freight. In an incriminating letter to this contact, found later during the investigation, Chung wrote "I don't know what I can do for the country. Being proud of the achievements by the people's efforts in the Motherland, I am regretful for not contributing anything" (Bhattacharjee, 2014).

Opportunities to contribute to China's achievements were regularly presented to Chung in a coordinated Chinese intelligence gathering operation starting in the 1980s, and continuing until 2003. He received invitations to meet with Chinese officials at gatherings in California, and in 1985, he was asked to visit China to lecture on his expertise in aerospace, one of the areas China had identified as critical to its technological advancement. He corresponded with Chinese engineers he met, and he took pains to impress them with his knowledge and his eagerness to assist them. After the Chung family's visit to China in 1985, which lasted for several months, he came home with eight pages of questions from engineers at one of their stops, the Nanchang Aircraft Manufacturing Company. He pulled together his answers and sent along 27 volumes of engineering manuals for the design of the B-1 Bomber via diplomatic pouch from the Chinese consulate in San Francisco. For the next 20 years, Chung brought materials home from his workplace at Boeing

Corporation—pilferage amounting to 300,000 pages—to save for or to send to his Chinese friends (“Ex-Boeing engineer, 2009; Flaccus, 2010).

Chung came to the attention of the FBI in the same way that Tai-Shen Kuo (discussed earlier) did: because Chi Mak, their handler, had written both names and contact information in Mak’s address books, and the FBI found them in October 2005 when they surreptitiously searched his home. A second search yielded a letter between Chung and Gu Weihao that Mak had kept. Gu was a Chinese official with the China Aviation Industry Corporation, and he asked Chung for information about airplanes and the space shuttle and thanked him for technical information he had previously sent. For at least a decade, Mak had served as the local handler for both Kuo and Chung, sending taskings from China to them, and collecting information from them to send back.

After the FBI conducted several interviews with Chung, performed secret searches of his trash, and executed a search warrant for his house, which revealed the thousands of Boeing documents stockpiled in basement rooms and crawl spaces, the FBI arrested Chung on February 11, 2008. The indictment outlined evidence of his regular interactions with Chinese officials: their discussion with Chung of cover stories for his visits to China; the advisability of sending information through Chi Mak because it was “faster and safer”; Chung’s repeated and earnest expressions of his desire to help China; his technical responses to their questions and requests; his removal from Boeing for the Chinese of books, reports, and hundreds of documents downloaded and printed out from Boeing databases; and his travel to present lectures in China which, although it was a condition of his security clearance that all foreign travel be reported, were not reported to Boeing security managers (United States District Court Central District of California, Indictment, 2008).

Despite the volume and nature of the information he removed from Boeing facilities, including 2 decades’ worth of trade secrets on the Space Shuttle, specifications on a fueling system for the Delta IV booster rocket, and the technical details on the C-17 military transport aircraft, prosecution of Chung moved slowly because although the materials were proprietary to Boeing and had been developed in its work for the federal government, they were not designated as national defense information and were not marked as classified (Flaccus, 2009, United States Court of Appeals for the Ninth Circuit, 2011).

Prosecutors shifted from their intention to charge Chung with espionage and instead charged him with economic espionage. To prove that the Boeing information he had stolen included Boeing trade secrets, they presented testimony from Chung’s Boeing colleagues about the restricted and export-controlled nature of the information, and about the proprietary agreements employees at Boeing signed, along with the nondisclosure agreements everyone signed to obtain a Secret security clearance and have access to such information. All of these promises and legal agreements Chung had violated.

## ECONOMIC ESPIONAGE

He requested a bench trial, in which only a judge hears the evidence and reaches a verdict. Chung became the first person convicted at trial under the Economic Espionage Act of 1996 (Flaccus, 2009). He was convicted in July 2009 of six counts of economic espionage, one count of lying to the FBI, one count of acting as an agent of a foreign power, and one count of entering into a conspiracy with Mak (Ex-Boeing engineer, 2009). He was sentenced on February 8, 2010, to 188 months in prison (15 years and 7 months) for betraying Boeing's proprietary information to China, information developed over 5 years at a cost estimated to have been at least \$50 million (Flaccus, 2010). In one of the letters found in Chi Mak's house, a Chinese official had written to Chung that "It is your honor and China's fortune that you are able to realize your wish of dedicating [yourself] to the service of your country," that is, to China (United States District Court Central District of California Southern Division, Memorandum of Decision, 2009).

Economic espionage is a distinct type of espionage, one that is similar to classic espionage in many respects, but different in others. Applying the characteristics of classic espionage discussed in the chapter earlier to this economic variant demonstrates this.

- A context of competition. The competition for Chung was less that between the defense contracting companies he worked for, and more the international competition between the PRC and his adopted nation, the United States.
- Secret means. Chung conspired with his handler, Chi Mak, to pass information to the PRC surreptitiously. Chung's contacts in China rehearsed cover stories he could use to explain why he and his family were spending 2 months traveling in China in 1985. As the FBI was starting to explore Chung's involvement with China they repeatedly searched his trash: each time they found Boeing proprietary documents interleaved into Chinese language newspapers in attempts to secretly dispose of them (United States District Court Central district of California, Southern Division, "Memorandum," 2009) This "Memorandum of Decision" written by the judge in Chung's trial is the source for the remaining entries in this list, unless otherwise noted.
- Goal is secrets. The goal in economic espionage is trade secrets. The FBI found detailed tasking lists from the Chinese in Chung's home that specified the information they most wanted. Included on these lists were: aircraft design manuals, fatigue design manuals, materials manuals, S-N curve manuals, military specifications user manuals, fighter jet structural details design manuals, Space Shuttle design manuals and information on the Space Shuttle's environmental conditions, the Space Shuttle's airtight cabin, the Space Shuttle's heat resistant tile design and materials composition process, the life-span extension/reliability analysis of U.S. fighter planes and airborne equipment, and S-N curves for fighter plane cabin Plexiglas and cabin canopies. The intense interest in what Chung could provide about space technologies reflects efforts by the PRC to "catch up" as latecomers to space who are determined to build on the technologies already designed by others (Elmhirst,

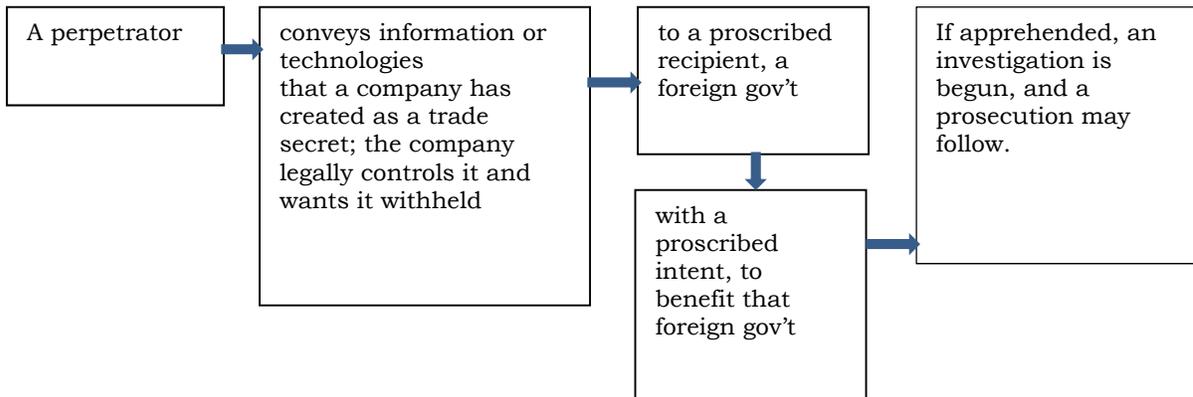
2009). At various periods of time, this type of information was designated as restricted from export, proprietary to the companies working on defense contracts, and eventually could have been classified. Work on elements of technology within a large government program proceeds in stages, and the type and degree of control over information varies over those stages. One student of espionage noted that “The Chinese...are good at positioning agents who can obtain advanced technology in the developmental stage, before it is classified” (United States District Court Central district of California, Southern Division, “Memorandum,” 2009; Gertz, 2006).

- Political, military, economic secrets. The information Chung stole from Boeing and sent to the PRC related to military technologies of the United States and its space program. As Boeing’s trade secrets, they were economic, but because Boeing is a defense contractor and was working on defense projects, many of them were also restricted military information.
- Theft. Chung exfiltrated from the company that employed him over 300,000 pages of Boeing documents, manuals, and reports over the years he worked for the company.
- Subterfuge. Chung stored these stolen documents all over his house, some in hidden places, but others in plain sight. These storage places included the crawl spaces and a specially constructed camouflaged storeroom hidden under the house, as well as under the stairs, in the fireplace, in stacks on tables in the dining room, and under the bed. In his exchanges with his Chinese contacts, Chung demonstrated his awareness that what he was doing required subterfuge—using a secure channel such as Chi Mak offered, and traveling to China in the guise of a family vacation to meetings where he could present information “in a small setting, which is very safe.”
- Surveillance. Chung sought out opportunities at Boeing and in the course of his work interacting with other companies to collect specific information requested by his Chinese contacts, if he himself was not working on a particular technology.
- Acted as an Agent of a Foreign Government. In his close and ongoing relationships with contacts in the PRC and in the Chinese consulates in California, Chung took direction from the Chinese and acted in their interests. He was convicted of one count of Acting as an Agent of a Foreign Power, Title 18 U.S.C, Section 1951.
- Psychological toll. During his long espionage career, Chung is described as serene in his workplace and personal life. He wrote to his contacts expressing his pleasure to be contributing to the modernization of China. When the FBI came to interview him, search his home, and arrest him, Chung was noticeably rattled, as if surprised at this response to his activities.
- Illegal. Chung was convicted of six counts of economic espionage, that is, possessing trade secrets for the benefit of China (Title 18 U.S.C, Section 1831);

## ECONOMIC ESPIONAGE

one count of lying to the FBI (Title 18 U.S.C, Section 1001); one count of acting as an agent of a foreign government (Title 18 U.S.C. Section 951); and one count of entering into a conspiracy with Mak (Title 18 U.S.C., Section 371).

Like the other types already discussed, economic espionage can be described in the general terms of the model of espionage derived from classic espionage.



**Figure 8 Economic Espionage in a Model of Elements of Espionage**

In Figure 8, an individual who commits economic espionage conveys a trade secret to an agent of or a foreign government itself with the proscribed intent to benefit that government, thereby disadvantaging the company that owns the secret and the United States itself.

---

---

**PART 3**

**CONTEXT AND RECOMMENDATIONS**

---

---

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

### CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

Sweeping changes in context are shaping how espionage is conducted now and how it will be conducted in the future. Two of these changes that should be considered in any analysis of current espionage are information and communications technology (ICT) and globalization. Examples discussed thus far have illustrated how recent spies have incorporated ICT in their activities and how the worldwide market for American technologies has spurred the theft of export controlled and trade secret information.

#### Information and Communications Technology (ICT)

During the past 2 decades, information technology and networked communications have quickly become so ubiquitous that it can be difficult to step back from this new normal context and recognize some of the implications of these advances—in this report specifically, implications for espionage committed by American citizens against the United States. Cyberspace and cyber security have many dimensions, only some of which are relevant here. Setting the scene for this context are statements from several officials, security professionals, and observers:

- The ubiquitous digitalization of information and pervasive connectivity of electronic networks have facilitated espionage as well as productivity.... *Joel Brenner, former National Counterintelligence Executive and former Inspector General of the National Security Agency* (Brenner, 2014).
- According to the Federal Bureau of Investigation (FBI), the theft of intellectual property (IP)<sup>67</sup>—products of human intelligence and creativity—is a growing threat which is heightened by the rise of the use of digital technologies<sup>68</sup> The increasing dependency upon information technology (IT) systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. *Gregory C. Wilshusen, Director Information Security Issues, General Accountability Organization (GAO)* (Wilshusen, 2012).
- Can the government still keep a secret? In an age of Wikileaks, flash drives and instant Web postings, leaks have begun to seem unstoppable... Still, there's been a change. Traditional watchdog journalism, which has long accepted leaked information in dribs and drabs, has been joined by a new counterculture of information vigilantism that now promises disclosures by the terabyte. A bureaucrat can hide a library's worth of documents on a key fob, and scatter

---

<sup>67</sup> Intellectual property is a category of legal rights that grants owners certain exclusive rights to intangible assets or products of the human intellect, such as inventions; literary and artistic works; and symbols, names, images, and design [footnote in original] (Wilshusen, 2012).

<sup>68</sup> Footnote in original is omitted here.

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

them over the Internet to a dozen countries during a cigarette break. *Scott Shane, reporter for the New York Times* (Shane, 2010).

- Cybercrime and cyber espionage, both political and economic,... are here and will remain the biggest cyber risks in the future. *Myriam Dunn Cavelty, Center for Security Studies, Swiss Federal Institute of Technology*. (Cavelty, 2012).
- ...Those conducting cyber espionage are targeting US government, military, and commercial networks on a daily basis. *James R. Clapper, Director of National Intelligence*. (Clapper, 2015).

In this report various characteristics of espionage against the United States by Americans have been explored, and the various types of espionage they undertake. This chapter briefly considers the impact of what the expert observers quoted earlier describe as “ubiquitous,” “pervasive,” and “unstoppable” trends in information and communications that have “revolutionized” the way we “communicate and conduct business.” The technologies we experience in daily life are moving toward the worldwide use of ICT, which is shaping the current context and will shape the future espionage threat.

The activities of cyber criminals<sup>69</sup> vary widely in scale, ranging from a lone hacker who opportunistically goes online to steal or sell another individual’s personal information, to a foreign government attacking its adversaries’ networks to disrupt critical infrastructures, take control of financial systems, overwhelm network functioning, or attack IT assets used for decision-making by military or government leaders. Along this spectrum of cyber activities, two dimensions are relevant for understanding espionage by Americans in the ICT era: (1) how an agent of an adversary, such as an American spy, currently gathers, stores, and transmits intelligence to a foreign government; and (2) how a foreign government steals controlled information directly across interconnected networks, usually in unacknowledged ways, with or without the connivance of an agent.

Reliance on computers and their related information technology (IT) and electronic files began to spread from the original users in select military and academic settings into more general use during the 1980s. IT became increasingly common during the 1990s, and after 2000, it was essential in business and professional settings. As these technical improvements became available, American spies adopted them into their activities, to the extent that the spy’s own technical proclivities and opportunities to make use of IT allowed. Table 21 summarizes by

---

<sup>69</sup> The prefix “cyber” was first used in 1991, according to the Merriam-Webster dictionary. It is defined as “of, relating to, or involving computers or computer networks, i.e., the Internet.” Thus terms such as “cyberspace” refer to the virtual environment in which computers operate over networks; it seems analogous to the military term “battlespace” that is applied to the environment—including the information and communications environment—of a battle. Cyber criminals are persons who commit crimes using computers across networks. Cyberespionage, as defined in 2015 in a Congressional Research Service report, is committed by cyberspies, who are “individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. Targets include government networks, cleared defense contractors, and private companies” (Theohary & Rollins, 2015).

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

decade, starting from 1970, the numbers and percentages of the 209 American espionage offenders in this study who used ICT in espionage.<sup>70</sup>

**Table 21**  
**Use of Information and Communications Technology by Decade Espionage Began**

<b>Decade Espionage Began</b>	<b>Number Who Began Espionage in Each Decade</b>	<b>Number of ICT Users Coded<sup>71</sup></b>	<b>% of ICT Users by Decade</b>
1970-1979	30	4	13
1980-1989	72	11	15
1990-1999	28	10	36
2000-2009	32	21	66
2010-2015	7	6	86

From the paper documents, microfiche strips, and film canisters of photographs that made up the media of a spy's information before the late 1970s, espionage offenders moved with the times into using floppy disks, then CDs, flash drives, and encrypted email attachments sent over the Internet. With the accelerating pace of technological innovation, the time lag has rapidly shrunk between when citizens of one country make a technological advance and when the rest of the world learns about and adopts it, and there is now a global technological race to keep up with the latest innovations as they appear (Limbago, 2014). Spies simply join in this race.

### ***Advantages and Disadvantages of ICT for Spies***

ICT offers a mixed bag of advantages and disadvantages to espionage agents. Its advantages are apparent to anyone who owns a computer and accesses the Internet. If they have insider access to the information they want, spies can install viruses that quickly copy large electronic files or download files from network servers onto USB drives that are inconspicuous to carry and store. Such viruses can also exfiltrate information directly to the recipients whom a spy works for. Spies can send information over the Internet by email attachment to a recipient anywhere in the world, eliminating the risk of meeting the recipient to hand over information, and the risk of leaving information in a dead drop to be picked up by the recipient later, unless the authorities find it first. They can also add encryption to the data being transmitted to enhance its security in transit ("Electronic spycraft," 2015). Among American espionage offenders since 2000 coded in the PERSEREC Espionage database, 20 of the 27 known ICT users copied information

<sup>70</sup> Use of ICT by American espionage offenders was coded from open source descriptions that did not reliably mention these details, so these figures can only provide an impression of increasing use over time.

<sup>71</sup> A person's use of ICT may have occurred late in a long espionage career rather than in the decade in which the spy first began espionage. For example, Walter Kendall Myers and his wife Gwendolyn began spying for Cuba in the 1970s, but only relied on IT as networked computers and email became common later in the 1990s.

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

from computers or downloaded it from networks; 12 are reported to have sent their information by email attachment, 2 sent theirs by fax, the rest sent their information on CDs by old-fashioned postal mail or in shipping containers.

The 209 American espionage offenders under study in this report do not include anyone with the most sophisticated ICT skills, (the closest example would be Edward Snowden), but such a person is hardly unlikely to be operating as a spy in the near future. Already in early 2016, the FBI announced an American citizen, Charles Eccleston, has pled guilty on February 2 to attempted unauthorized access and intentional damage to a protected computer system.<sup>72</sup> This charge was a plea bargain; Eccleston's scheme planned to send spear-phishing emails to federal employees in nuclear laboratories to plant a virus that could damage the government computer systems and allow a foreign government to exfiltrate classified nuclear-related information from them. He sought revenge against the Nuclear Regulatory Commission that laid him off and money for his proposition from a foreign embassy, speculated to have been the Chinese. Eccleston collected email addresses, drafted emails that would announce an innocent-seeming conference with a registration link that he thought would install the virus. However, Eccleston was working with undercover FBI agents, so this link did not do any damage and sent off no classified nuclear information (Department of Justice, 2016; Hsu, 2016; United States District Court for the District of Columbia, Indictment, 2015)

An agent like Eccleston who used hacking expertise to capitalize on fellow employees' vulnerability to phishing attacks, or someone who works with a group that brings these skills and resources to the task, can gain the ability to directly access the computers or networks of a target remotely, which adds another layer to the advantages ICT offers to espionage. Hacking into a target's computer or network can be an inexpensive way to collect information—it might be done for the cost of a computer and a network connection. It also offers the advantage of anonymity, since it is difficult to identify with certainty who was responsible for an intrusion (Schneier, 2015).

With even more determination, an agent can hack into a target computer system and install the sort of malicious software that takes over a network and removes data, silently sending the desired information off the target's network and onto a destination designated by the agent (Schneier, 2015). Other means useful for espionage that are now available include software for harvesting communications that focuses on "end-point vulnerabilities," such as keyboards and computer screens, which allow what is written or searched to be collected at the point of the target's keystrokes themselves, often evading the best encryption. It is also possible

---

<sup>72</sup> Charles Eccleston will be sentenced later in 2016. He is not included in the 209 individuals in this study since his crime was revealed after the cut-off date for analyses for this report, but he is discussed here as a timely example of a direction spies who are sophisticated with ICT are likely to take.

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

to intercept wireless network signals, and then to read what is sent by a target or potential asset in their emails or text messages (“Electronic spycraft,” 2015).

However, ICT also inflicts disadvantages on an espionage agent, because it provides counterintelligence and law enforcement officials with new tools and electronic resources that can work against the spy, while helping the authorities to identify espionage activities. Cell phones, now so common, generate metadata that can be traced to show the location of the user at a particular time, thus potentially placing a person at the scene of an information pick-up or a meeting with a recipient. The times at which a cell phone user makes calls and to whom can be analyzed, for they indicate when the person is awake and active, and when he or she usually sleeps, and thus tells the analyst which time zone the person probably lives in. If an agency can track one’s movements, it becomes difficult to clandestinely meet assets or conduct surveillance. Cell phones can also be used as bugging devices, potentially allowing the authorities to listen in on conversations taking place in their vicinity (Murphy, 2015; “Electronic spycraft,” 2015).

The same ICT means that can be used by spies are used by the authorities to apprehend the spies. The description in the leaks chapter of the investigation of Stephen Kim, the nuclear proliferation expert and contractor for the State Department and James Rosen, a Fox News reporter, illustrates this double-edged impact. Kim and Rosen temporarily worked in the same State Department building. They used their email accounts and their cell phones to communicate with each other to set up times and places to meet, although they were cautious enough to use a simple code to try to hide their activities. In order to conduct surveillance on Kim, the FBI investigators gained legal access to his and Rosen’s electronic badge records at the entrance to their building, as well as to Kim’s desk telephone records, and to all of his office computer files, as well as to records of emails to Rosen’s cell phone, to his office desk phone, and to all of Rosen’s email interactions with Kim. From these, the investigators could construct a damning time line of plans, contacts, meetings, and shared files that led to the conviction of Kim for espionage by leak to the press (United States District Court for the District of Columbia, Affidavit, 2010).

Some American espionage offenders entered the United States with the intention of building a career that would give them access to classified information that they could send back to the foreign governments sponsoring them. Larry Wu-tai Chin, Karl Koecher, and Chi Mak, all discussed earlier, are three examples of spies who came to this country as sleeper agents. Each left their previous lives at the border and either assumed new identities or shaded inconvenient elements of their pasts.

This would be more difficult now that biometric scanners scan travelers at international airports and guard entry to many offices and government buildings. These scanners record a person’s biometric characteristics, such as fingerprints, iris scans, and facial patterns, and the electronic records of these scans can be kept indefinitely. This makes changing one’s identity or assuming an identity in which

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

some parts have changed—as Chin, Koecher, and Mak did—more difficult than it was. Once their biometrics have been collected, some speculate that in the future, spies may have to become “single-use operatives” who can only operate in the one country that has the biometrics that defines their identities, unless that nation is not sharing biometrics with another one, in which case, the spy could use a different identity in each of those nations. Even then, the spy could not rest easy, since it is quite possible someone in one of those nations could be selling sensitive biometric data to an adversary (Murphy, 2015).

The photos and personal news that people post on social media persist on the Internet indefinitely, and this trail of personal data can haunt espionage agents just as it does anyone else who tries to change careers or take a new direction in life. If a foreign agent is also a social media user, and seeks an insider position in a government agency to gain access to classified information, his or her posted photos are forever available online to be compared against, again making it difficult to assume a new identity or a covert role.

On the other hand, if a young person has no online social media presence at all, potential employers may infer that this person is trying to hide or cover something up, but suddenly discontinuing an established social media presence by “going dark” can be equally suspicious (Murphy, 2015). Social media offers agents valuable insight into potential sources for recruitment, but it also ties them to their own identities and hinders them from assuming another one.

Thus, most of the advantages ICT offers for espionage come with related disadvantages. One observer notes that “A much bigger worry for spies is that the very vulnerabilities which make it easy for them to steal other people’s secrets also make it hard for them to hold on to their own” (“Electronic spycraft,” 2015).

### ***Cyber Espionage by Governments***

The second dimension of the evolution of cyber activities to be considered here is how a foreign government now can steal controlled information directly across interconnected networks, with or often without the cooperation of an agent. The focus of this report is on the activities of American agents working against the interests of the United States, rather than on the activities of the foreign governments themselves, yet because this dimension of the cyber context is developing rapidly in scope and sophistication, it will soon change the role of espionage agent.

Before the spread of the Internet, governments typically spied directly on one another either by observation or by intercepting and listening in to various signals the adversary emitted. Governments still use those methods, but new cyber methods offer relatively cheap, easy, and anonymous entry into the networks where a target’s information usually resides, rather than in the safes or locked drawers used in previous decades. Cyber intelligence tools are supplementing and may be overtaking physical surveillance and signals intelligence gathering in importance.

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

Observers report that over thirty governments around the world have already formed cyberwarfare divisions within their militaries to develop the means to infiltrate computers remotely and steal information (Schneier, 2015; Limbago, 2014).

Cyber intelligence—collecting, analyzing, and disseminating intelligence on the intentions, capabilities, and operational activities of foreign cyber actors—is one of the core objectives in the National Intelligence Strategy that the Office of the Director of National Intelligence (ODNI) produced last year to guide the activities of the Intelligence Community (Clapper, 2015). Since 2010, government agencies including the Department of Defense (DoD), the Department of Justice (DoJ), the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Department of Homeland Security, and the Director of National Intelligence (DNI) have reorganized to include cyber capabilities of intelligence gathering, countering digital impacts, and if necessary, conducting cyber offense (Viswanatha, 2014; Elkus, 2015; Bennet, 2015; ‘New intelligence agency,’ 2014; Clark, 2015).

Cyber offense takes the form of illegally hacking into a target government’s or military’s networks—surreptitiously—to learn the networks’ structures and explore the information contained therein, and then perhaps planting malware in the networks that silently extracts data for days or months, taking the information directly and electronically that spies on the ground would have to maneuver and plot to obtain. Once inside a network, cyber offense can plant false information to mislead or disrupt the target, or it could even insert destructive malware, which on a remote signal from the intruders, damages the network or brings it down, denying the target its information and its coordination capabilities (Schneier, 2015; Office of the National Counterintelligence Executive, 2011).

These scenarios are not the stuff of movie plots or projections far into the future. All the major world powers with advanced ICT systems have been conducting cyber offense against one another and sharpening their skills with it for at least a decade or more, but they were usually discrete about it (Cavelty, 2012). In September 2010, however, the impact of the Stuxnet worm on Iranian nuclear programs was revealed, marking a turning point toward more openness about these governmental cyber operations.

Gradually over some months, the public learned that apparently (although the federal government declined to acknowledge it) the United States and Israel had engineered a specialized computer worm called Stuxnet and inserted it into the control software for Iran’s nuclear fuel centrifuges, destroying some of them and deceiving the operations of others, and setting back Iran’s nuclear program by several years (Broad, Markoff, & Sanger, 2011; Denning, 2012). Other milestones of hacking revelations soon followed, which were openly acknowledged, such as Google’s admission in January 2010 that it had been hacked by elements of the Chinese government, despite a certain embarrassment that such a prominent IT systems innovator as Google could itself have been broken into (Harris, 2014b). In October 2014, commercial investigators announced that the Google hack had been

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

but one of a massive international espionage operation linked to the Chinese government that over the previous 6 years had broken into nearly 1,000 organizations, planting various types of malware and stealing data from servers across Asia, Europe, and the United States (Gertz, 2014).

China and Russia are leading cyber adversaries of the United States, but many other nations are also players in the game. One analyst describes recent instances that have been inferred and attributed to certain actors —nations rarely admit cyberespionage—this way:

In 2009, Canadian security researchers discovered a piece of malware called GhostNet on the Dalai Lama's computers. It was a sophisticated surveillance network, controlled by a computer in China. Further research found it installed on computers of political, economic, and media organizations in 103 countries—basically a who's who of Chinese espionage targets. Flame is a surveillance tool that researchers detected on Iranian networks in 2012; these experts believe the United States and Israel put it there and elsewhere. Red October, which hacked and spied on computers worldwide for five years before it was discovered in 2013, is believed to be a Russian surveillance system. So is Turla, which targeted Western government computers and was ferreted out in 2014. The Mask, also discovered in 2014, is believed to be Spanish. Iranian hackers have specifically targeted U.S. officials. There are many more known surveillance tools like these, and presumably others still undiscovered (Schneier, 2015).

In May 2014, the new Counter Intelligence and Export Controls Section in the National Security Division of the United States Department of Justice raised the stakes in the international cyber competition by indicting by name (in absentia) five Chinese military officers who were working in a Chinese Army cyberespionage unit. The five were accused of computer hacking, economic espionage, and conspiracy for hacking into six American companies and a labor union and stealing their controlled trade secrets, passwords, emails and other company correspondence, financial statements, cost projections, and research plans (Federal Bureau of Investigation, 2014; Viswanatha, 2014; "Cyber-Espionage Nightmare," 2015). The contrasting positions taken by China, which openly supports its industries with government intelligence operations, and the United States, which argues that it does not do so (this controversy was discussed earlier in the economic espionage chapter) clashed publicly as American companies like these six bitterly protested that Chinese cyberespionage was robbing them of their innovations and business models, and damaging their international competitiveness (Brenner, 2014).

In a further milestone of acknowledged international hacking, in August 2014 the Office of Personnel Management (OPM) admitted that several months earlier, the Chinese had broken into its poorly defended networks and stolen the personnel and security clearance application records of 21.5 million Americans. This serious loss

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

offers a foreign intelligence operation potential insight into personal details about individuals, their interests and weaknesses, their careers, and their families and friends that could be exploited for recruitment or blackmail (Gault, 2015; Peterson, 2015).

In September 2015, the prospect of an escalation in cyberespionage—or more damaging international cyberattacks—led to discussions during the state visit to the United States of the Chinese president, Xi Jinping, where he pledged that China would no longer pursue the kind of hacking of which the five Chinese officers stood indicted. In November 2015, at the Group of 20 Conference, China, Russia, the United States, and most of the other world economic powers negotiated an agreement stipulating that they would follow specified “global rules of responsible behavior in cyberspace,” for now (Nakashima, 2015).

In these instances of cyberespionage, the information sought and stolen was controlled. Often it was classified, but not in every instance, since sometimes it was a trade secret held by a company, or it was an unclassified but sensitive piece of information, such as some of the personal and professional details of many cleared federal employees and contractors. The information was meant to be secret and kept safe from adversaries, yet those adversaries hacked into a computer network and stole the secret, and after the fact it was usually impossible to determine for sure who did it.

Before the era of reliance on ICT, adversaries were positioned at a physical distance from one another. To gain and maintain the competitive advantage, more and better information about the unseen adversary needed to be collected. This prompted the need for and reliance on intercepting signals and on spies, who lived in or could enter the camp of the other and bring back accurate information.

Cyberespionage overcomes the physical separation between adversaries, as it links them together in the global information and communications network of the Internet. It electronically eliminates that earlier distance, and clandestinely puts an adversary into the secret heart of the other. This prompts some speculations: if secrets are now kept in electronic storehouses, and the adversary is successfully rifling them, does this not threaten the control over these secrets, and if so, can there still be espionage as it has been discussed here? Will there be no need for spies if governments can clandestinely reach into their adversaries’ information storerooms from a distance and take what they want? When adversaries have developed their cyber abilities well enough to reach into even the most strongly defended systems of the other and pluck out the secrets kept there, why will they need spies?

### **Globalization**

Before 1989 ushered in the beginning of the Soviet Union’s collapse, the United States had faced that one main nation-state adversary for 4 decades in the Cold War. In 2015, there were many adversaries: Russia and China and three or four

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

more rising nation-states including Iran contest the predominance the United States has enjoyed. These were joined by various non-state actors that are capable wielders of ICT and social media, including terrorist groups, in asymmetric attacks against the more powerful United States. Therefore, the current geopolitical context presents a multiplicity of economic competitors and potential military adversaries, and new challenges for countering espionage by them.

Adversaries issue these challenges within the current meta-context of globalization, the move toward integration of markets and interdependence of peoples that is taking place across many dimensions. This move has been accelerating for several decades, fueled by economic trends and the advances in ICT and in cheaper transportation. (National Intelligence Council, 2008; World Trade Organization, 2008; Steger & James, 2010).

### ***Economic Globalization***

As globalization has widened the field of economic interrelationships to include more peoples and more nations, the value of creative and innovative ideas on technologies has increased, especially if they can be protected in trade secrets. The pace and reach of economic competition increases with globalization. For some nations that are trying to catch up to the world's economic leaders, the increasing value of other nations' intellectual property has made it worthwhile for them to invest more effort and resources into stealing those secrets through espionage, as a shortcut in their own development (Hannas, Mulvenon & Puglisi, 2015).<sup>73</sup>

One characteristic of economic globalization is an increase in multinational corporations and worldwide patterns of manufacturing. Corporations routinely plan large-scale projects, such as aircraft development, to include companies from multiple nations, each contributing a specific part or system, while the lead company coordinates the assembly of these parts into a whole. In such projects, sharing design details and materials specifications with foreign partners is essential, yet if they might have military uses, American export control laws often prohibit the release of such advanced materials and technical concepts to non- U.S. companies. It can be difficult for an American company to both comply with export control requirements and collaborate effectively with their international partners (Beck, 2000).

For example, in 2006 Boeing Corporation planned to produce the composite plastic fuselage and wings of its new 787 aircraft in Italy and Japan, but these plans were abruptly delayed when Boeing's own engineers argued that the techniques and composite materials that were to be used had originated in secret military research

---

<sup>73</sup> This source details efforts by the People's Republic of China to covertly acquire technology to underwrite its rapid economic development. The authors argue that "While giving due credit to the Chinese people for their ability to produce, China could not have engineered this transformation, [into an world economic leader] nor sustained its progress today, without cheap and unrestricted access to other countries' technology." (Hannas, Mulvenon & Puglisi, 2015, p.2)

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

on the B-2 bomber in the 1980s (The B-2 was the plane Noshir Gowdia had worked on). In order to avoid violating ITAR restrictions on the release of technologies that could have military applications, Boeing reanalyzed each part to be used in the aircraft to determine if it had had a military origin, and if did so, Boeing tried to find an analogous part with a commercial origin to replace it. For months, Boeing delayed production while this replacement was done, despite their having provided evidence to regulators of other commercial uses for composites that had not been derived from the B-2. Dual use technologies are a thorny area, subject to judgment calls. Some argue that export control laws are dangerously outdated, that they no longer prevent the global spread of technologies that could be used against the United States, and that they should be brought into the 21<sup>st</sup> century context of globalization because they “reflect a control system designed for the Cold War rather than the new reality of economic globalization” (Gates, 2006).

Other aspects of globalized economic activity that factor into the potential for economic espionage are global supply chains that pass through uncontrolled countries, the exposure of proprietary plans and methods to more people and places that adds to the risk of trade secret theft, and the opportunities that global businesses offer to foreign intelligence services to recruit Americans, who may be exposed to their enticements in international business settings (Figliuzzi, 2012). Because modern global business must use ICT networks to exchange its sensitive information, it is as vulnerable as any intelligence or government agency to being hacked and having its information stolen (Brenner, 2014).

As discussed earlier in the section on export control violations, the AECA, IEEPA, and ITAR laws were written in the 1970s, when the sharp distinction these laws draw between U.S. persons and foreign persons made sense. At that time, most manufacturing of American products took place in the United States and was performed by American citizens. With globalization advancing, this is no longer as true, and policies in these laws that require excluding non-U.S. persons from knowing about or participating in the development of American technologies sharply clash with current expectations for collaboration and cooperation across national boundaries, as people work in multinational corporations or perform research in universities among multinational students, and as companies take advantage of joint ventures in which they pool scarce resources and expertise from various countries to manufacture a complex product (Brown, 2009). Professor John Reece’s conviction for espionage based on having hired Chinese and Iranian students to work on sensitive technology in his university lab is an example of this issue.

### ***Cultural Globalization***

One of the important impacts of economic globalization is the elimination of trade barriers such as tariffs, to encourage free trade across national boundaries. Like the falling of trade barriers, the whole thrust of globalization is to deemphasize the importance of national boundaries. It is a short step from global trade across

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

boundaries to deemphasizing the importance of a single national allegiance in favor of a global perspective. As the globalization of cultures has advanced with exposure and interaction—in languages, in music, literature, and art, in political aspirations, in shared concerns for the environment—it has invigorated the notion some have proposed since the end of the Cold War, that everyone should first of all be “global citizens...who have certain rights and responsibilities towards each other by the mere fact of being human on Earth” (Altinay, 2010). In contrast to the economic dimensions of globalization that increase competition, cultural globalization implies diminished competition between nations, and since espionage presupposes a context of competition, such “one-world-ism” is likely to have an impact on it.

Global citizenship assumes an ethical and political stance in which the social, political, economic, and environmental realities of the world demand that individuals, communities, and nation states make decisions based first on global considerations. It emphasizes the fundamental interconnectedness of all things and the reduction of cultural distinctions, sees the political and geographical boundaries of nations as increasingly irrelevant, and defines global challenges, such as climate change, as beyond the abilities of national interests to solve, requiring global solutions. A “global citizen” subsumes his or her identity as a citizen of a particular place beneath an identity in the global community. Organizations, conferences, educational curricula, and spokespersons devote themselves to encouraging global citizenship.<sup>74</sup> One advocate writes that “as a result of living in a globalized world, we understand that we have an added layer of responsibility [in addition to national identities and allegiances]; we also are responsible for being members of a world-wide community of people who share the same global identity that we have (Israel, 2012).

Individuals who, while betraying their nation’s secrets, conceived of their actions as taking place on a higher moral plane, more admirable than loyalty to one nation, are not only a result of modern globalization. Some earlier spies also felt this way. For example, Theodore Hall, a precocious American physicist working on the Manhattan project and thereafter briefly spying for the Soviets, gave American nuclear secrets to them at the end of World War II. He explained that he acted from a higher responsibility, as a citizen of the world, to even-up the sides in the Cold

---

<sup>74</sup> The idea of global citizenship is not recent or modern. One author points out that Gouverneur Morris, a delegate to the Constitutional Convention in Philadelphia, criticized “citizens of the world” from the floor of the convention on August 9th, 1787. The convention record noted that “As to those philosophical gentlemen, those Citizens of the World as they call themselves, He owned he did not wish to see any of them in our public Councils. He would not trust them. The men who can shake off their attachments to their own Country can never love any other. These attachments are the wholesome prejudices which uphold all Governments. Admit a Frenchman into your Senate, and he will study to increase the commerce of France; An Englishman, and he will feel an equal bias in favor of that of England.” ["Notes on the Debates in the Federal Convention". Yale University Avalon Project.](http://avalon.law.yale.edu/18th_century/debates_809.asp)  
[http://avalon.law.yale.edu/18th\\_century/debates\\_809.asp](http://avalon.law.yale.edu/18th_century/debates_809.asp)

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

War. By helping the Soviets develop their nuclear bomb, he thought he would reduce the danger of nuclear war. He fled prosecution in the United States and lived out his life in England (Cowell, 1999).

The claims for a global citizenship highlight how much the crime of espionage, as it has been conducted in the era of national sovereignty, depends on the existence of competing nation states, and how much countering espionage depends on those states commanding the exclusive allegiance of their citizens. As globalization continues apparently indefinitely, will the knitting together of peoples in interconnected and overlapping configurations, as global citizens no longer defined exclusively by national boundaries, diminish the resort to espionage and the attempt to enlist agents to work against their countries, or would it simply redefine the players who will undertake it in different competing configurations?

### ***Impact of the Internet***

The Internet has been both a product of globalization and a catalyst for it. It connects computer users around the world simultaneously in business transactions, consumer searches, spreading the breaking news, enabling electoral politics from near and far, and allowing participation in sports, entertainment, and public tragedies or triumphs taking place in distant countries. It allows people to move from their homelands to live in another nation, and yet to stay so connected to family, friends, and life back home that they feel as if they are living in two places at once. Access to the Internet softens the wrenching break in ties with the past life that immigrants and migrants faced, and provides another step toward becoming a global citizen (Herbig, 2008a).

The growth of international Internet and communications use is astonishing. Some statistics to illustrate the trends include: from 2000 to 2010, the number of global Internet users rose from 413 million to 2.03 billion. By January 2015, that number had risen to more than 3 billion users and the rate of increase was accelerating. Already in 2010, almost 30 percent of the world's population had access to computers; there were 1 billion Google searches performed every day, and 2 billion videos were viewed daily on YouTube. By January 2015, 40% of the world's population had Internet access, 51% used mobile communications devices such as cell phones, and 29% had active social media accounts (Kemp, 2015; Internet Live Stats, 2015).

This is the emerging context in which espionage is taking place: information and communication technologies, globalization, and increasing reliance on the Internet. As an FBI counterintelligence official noted during a 2014 Congressional hearing, "Long gone are the days when a spy needed physical access to a document to steal it, copy it, or photograph it, where modern technology now enables global access and transmission instantaneously" (Coleman, 2014). "Cyber is now part of every mission," an intelligence official explained, "It's not a specialized, boutique thing" (Miller, 2015).

**IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES**

The first part of this report described characteristics of recent American espionage offenders and trends in their activities, based on analyses of the 209 individuals under study. The second part explored the five types of espionage those 209 people committed. These five types of espionage are related to one another, but they are not identical. The intent in describing the five types in some detail is to make a case that espionage no longer only occurs in the classic type that the term “espionage” has usually described, but also in leaks, foreign agent activities, violations of export control laws, and economic espionage. Considering what the individuals that were convicted of these offenses actually did, the laws that frame each of the five types, and how the types interact, suggests that to understand the current field of espionage one must expand one’s mental categories to encompass the activities of these additional four types and place them alongside classic espionage. Not only in classic espionage but in these other types as well, the United States is losing its invaluable controlled information, ideas, technologies, and plans, and is seeing its economic advantages and national security diminished.

Given this proliferation of types of espionage, along with the transformations in context that ICT and globalization are causing, the need to re-think and revise the legal statutes that apply to espionage in the United States becomes even more compelling. This report concludes with an overview of possible approaches to revising the Espionage statutes.

**Revise Title 18 U.S.C. sections 792 through 798**

The most narrowly focused revision would consider the recommendations of legal scholars and judges<sup>75</sup> to fix the inconsistencies and ambiguities in the espionage statutes Title 18 U.S.C. sections 792 through 798. Given that these important provisions are based on laws from 1917 and were updated most completely in 1950, at a minimum they need further updating. They present other issues as well. For example, Harold Edgar and Benno C. Schmidt, Jr., writing in their seminal essay on espionage law in 1973, pointed to subsections (d) and (e) of Section 793 as especially problematic and crying out for revision. These subsections are:

- (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense,

---

<sup>75</sup> See the statement by Judge T.S. Ellis in United States District Court for the Eastern District of Virginia. (2006). Memorandum opinion, United States of America v. Steven J. Rosen and Keith Weissman.

## IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES

or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it~ or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; ....

shall be fined not more than \$10,000 or imprisoned not more than ten years or both.

Edgar and Benno, Jr. closely read the legislative record for the Congressional debates that produced the original Espionage Act in 1917, and then studied the debates in Congress during the last major update in 1950. The authors were moved to exasperation by the "hopeless imprecision" of these two subsections. "There is an additional, fundamental problem," they wrote, "the legislation is in many respects incomprehensible." The two legal scholars outlined five serious problems in this pair of subsections that cause inconsistency and confusion for those who are trying to apply them. The five problems they identified include the following:

- (1) Is publication a "communication" within the meaning of the subsections, and are communications or retentions incident to publication criminal?
- (2) What degree of culpability is required by the term "willfully?" Can the word be given a meaning narrow enough to sustain the constitutionality of the prohibitions on communication or retention in light of the vagueness of the phrase "related to the national defense?"
- (3) What constitutes protected "information" under the subsections, and what culpability is required before its transfer is criminal?

## IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES

- (4) What makes a piece of paper containing defense information a "document" or other enumerated item for purposes of the subsections?
- (5) What does "not entitled to receive it" mean for purposes of the communication and retention offenses? (Edgar & Schmidt, Jr., 1973)

Application of various interpretations of these questions have produced many of the legal issues illustrated by cases discussed in this report, including whether leaks to the press constitute acts of espionage or something else, how to demonstrate that a person's motivation to act was "willful," or how classification of information relates to these provisions—e.g., does it define who is "not entitled to receive it," despite the fact that these statutes do not even mention classification? Sorting out and clarifying the issues raised just in these two often-used subsections of section 793 could greatly improve the espionage statutes. Judge T. S. Ellis III, who presided over the convoluted prosecution of Steven Rosen and Keith Weissman for their having received oral classified information from Lawrence Franklin, wrote that

The conclusion that the statute [referring to Section 793] is constitutionally permissible [as his opinion does so conclude,] does not reflect a judgment about whether Congress could strike a more appropriate balance between these competing interests, or whether 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 statute 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 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 [passed in 1911, it was the forerunner of the Espionage Act of 1917] 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. These changes should suggest to even the most casual observer that the time is ripe for Congress to engage in a thorough review and revision of these provisions to ensure that they reflect both these changes, and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate about the United States' conduct in the society of nations (United States District Court for the Eastern District of Virginia, Memorandum opinion, 2006).

## IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES

### Revise Espionage-related Statutes to Reflect Cyber Capabilities, Globalization, and the Internet

By taking Judge Ellis’s observation to heart, broader and more ambitious revisions to the most commonly applied espionage statutes could be undertaken that would consider them together<sup>76</sup> to eliminate inconsistencies and frame better laws that reflect the current context of cyber capabilities, the Internet, and globalization.

For example, Stephen I. Vladeck, a professor of law, suggested to a House Committee at a hearing about Wikileaks in 2010, that the Espionage Act causes “problematic uncertainty” in at least five ways that could and should be addressed by reformers. These include:

- (1) Although intended to deal with classic espionage, that is, “using spies to collect information about what another government or company is doing or intends to do,” the language of the act does not require either “a specific intent to harm the national security of the United States, or to benefit a foreign power.” In its vagueness, three crimes end up being prosecuted under the one statute: “classic espionage, leaking, and the retention or redistribution of national defense information by private citizens.”
- (2) The Espionage Act does not focus only on the initial offender’s action, but criminalizes each subsequent person who “knowingly disseminates, distributes, or even retains [a piece of] national defense information.” This overly broad application complicates sorting out how leaks to the press should be considered.
- (3) The mental state specified in the Espionage Act to find that the action was intentional, is that the person acted “willfully,” but various courts that have struggled with the ambiguities of the previous two points have ruled that other mental states not specified in the Act can be required as well, including a “bad faith purpose,” which adds more complexity to an already complex statute.
- (4) The Act may interfere with the current Federal Whistleblower Protection Act, which does not address the potential conflict with the Espionage Act for those to whom a whistleblower discloses classified information.
- (5) The Act does not acknowledge the possibility that information may be improperly deemed classified or otherwise sensitive by the government, despite the common understanding that this can occur (Vladeck, 2010).

Professor Vladeck’s suggestions, in part, reflect those of many commentators on the need for a specific law that applies to leaks of classified information to the press in this era of global and instantaneous communication. The Espionage statutes are a

---

<sup>76</sup> That is, Title 18 U.S.C. sections 793, 794, 798 and Title 50 U.S.C. section 783, as well as the other relevant statutes used in espionage offenses, discussed earlier.

## IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES

crude fit for leaks, a disjuncture that has prompted charges of unfairness from persons who see themselves as acting as whistleblowers (Epstein, 2007; United States Senate Committee on the Judiciary, 2010; Barandes, 2008).

Another issue for revision that reflects the globalization underway is the disappearing ability to apply the distinction between section 793, in which the recipient is specified to be “anyone not authorized to receive” the information, whether he or she is an American citizen or a foreign citizen, and section 794, which specifies that the recipient must be any foreign government, or an agent or group of such a government. Proving a nexus in the ICT environment to a foreign entity as the recipient of information, however, becomes ever more difficult in an Internet era of multinational corporations and global manufacturing, which offer many legitimate reasons for transmitting sensitive information around the world. Automated transmission over the Internet and electronic file transfers can occur without leaving a trace as to who has received the information. In these circumstances, investigators often cannot prove, or even discern, that there was a disclosure of controlled information to a foreign recipient, a nexus required to justify prosecuting the transmission under section 794. A similar effect is seen in prosecuting trade secret theft: section 1831 requires a foreign nexus, while section 1832 does not, and cases often end up being prosecuted under section 1832 because the foreign nexus cannot be proven (Brenner, 2014; Caveltly, 2012; Clapper, 2015; Coleman, 2014).

Not surprisingly, given that the latest major update to the espionage statutes dates from 1950, it did not anticipate the impact on espionage of the now-rapidly evolving cyber capabilities to create, store, and transmit information electronically and instantaneously. Taking account of the impact of ICT on current espionage, as well as its impact on developments that may be expected in the future, would be another angle for revision that would improve the Espionage statutes and make them more relevant and useful in the 21<sup>st</sup> century.

To cite just one example that was unimaginable in 1950, Shane Harris investigated the cooperation in cyber counterespionage between United States government intelligence agencies and American communications companies, and detailed the assistance and links between them in 2014.<sup>77</sup> In an excerpt of his book, he discussed the Google hacking by the Chinese in 2009, and how Google itself had then traced the hackers to a server in Taiwan controlled by the Chinese army (Harris, 2014a).

When Google chose to make the fact of the hacking and its investigation into it public, it opened the possibility for the American government to publically protest the Chinese government’s cyber espionage program without having to discuss sensitive sources and methods of its own it might employ. “China plays a longer

---

<sup>77</sup> Harris, S. (2014). *The Rise of the Military-Internet Complex*. New York NY: Houghton Mifflin Co.

## IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES

game,” Harris writes, “Its leaders want the country to become a first-tier economic and industrial power in a single generation, and they are prepared to steal the knowledge they need to do it, U.S. officials say.” Defending against such a concerted program, according to Harris, involves the NSA, the major communications companies, prominent American corporations, and private security companies in a sharing arrangement both multi-layered and wide-ranging across sectors of the economy. Americans who could support such an international cyberespionage effort by becoming spies for the Chinese would face only the antique Espionage statutes that were framed a century ago (Harris, 2014a).

### Reconcile Statutes that Apply to the Five Types of Espionage

The broadest approach that could be taken to revising the Espionage statutes would be to consider the statutes that currently are used to prosecute all the five types of espionage, as they have been discussed here, and undertake an effort to reconcile inequities, eliminate gaps or overlaps between them, and create more consistency in the legal response to activities that are similar, even though they take place in different spheres. The DoJ’s National Security Division has been investigating and assisting with prosecutions of cases across an array of types of espionage for a decade, as the Assistant Director explained to Congress in 2008: “the clandestine intelligence collection activities of foreign nations include not only traditional Cold War style efforts to obtain military secrets, but increasingly, sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons” (United States House of Representatives Committee on the Judiciary, 2008). Testifying at the same Congressional hearing but speaking specifically about Chinese espionage activities, Larry Wortzel, chairman of the United States-China Economic and Security Review Commission, made a similar point:

Indeed, my own view is that today it is often difficult to distinguish between what we define as espionage related to the national defense under the Espionage Act (18 USC 792-8), and economic espionage or the theft of proprietary information and trade secrets covered by the Economic Espionage Act (18 USC 1831-9). Indeed, for American companies and for the national defense of the United States, the impact of espionage can be the same, robbing U.S. companies of the costs of their research, giving technology with military application to China’s armed forces, and undermining the security of American military personnel and our nation (United States House of Representatives Committee on the Judiciary. 2008).

The laws that govern each of the five types are usually different and are focused on the distinctive aspects of the crimes. The professionals working in each area—case officers, lawyers, investigators, judges—often specialize in one particular type of espionage crime, mastering its own complexities. The communities of interest that have the most at stake when an American citizen gives away or sells information in

## **IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES**

an act of one of the five types of espionage are distinct: the intelligence community, with its reliance on classification of information and clandestine sources and methods for obtaining information from and countering espionage by foreign powers, differs considerably from the corporate community with its focus on economic advantage, innovation, and ownership of its intellectual property. The people who leak government information to the press and from the press to the rest of the world, including adversaries and competitors, often differ dramatically in motive from those who agree to serve as agents of a foreign power by collecting information clandestinely in the United States, and differ yet again from those who try to profit for themselves by selling American export controlled technologies.

Yet each of these five types of espionage results in damage to the United States in various but cumulative and multiplying ways. Knowing more about the other types, and considering what they have in common, would be very advantageous to these communities and their practitioners. Thinking about them as one phenomenon could even sharpen our ability to counter them.



## REFERENCES

- 2012 ClearanceJobs compensation survey (2012). Downloaded from <http://www.clearancejobs.com> on November 12, 2014.
- Accused spy sold nothing secret, defense says. (2010, April 14). Honolulu, HI: *Star Bulletin*, p. 1 [Gowadia].
- agent. (n.d.). Dictionary.com Unabridged. Retrieved August 11, 2015, from Dictionary.com website: <http://dictionary.reference.com/browse/agent>
- Agents of Foreign Governments Act. Title 18 U.S.C. section 951. 1938
- Altinay, H. (2010, March). The case for global civics. Global Working Papers No. 35. Washington, DC: Brookings Institution.
- Amos, C. (2006, December 11). Jilted love, not political intrigue, drove a Salem man to espionage. Salem, OR: *Statesman Journal*, p. 3 [Weinmann].
- Anderson, R.H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., Van Wyk, K. (2000). Research on mitigating the insider threat to information systems—#2: Conference Proceedings. Santa Monica, CA: RAND Corporation.
- Apodaca, P. (1995, January 24). 2 accused of plot to sell Epogen formula biotech: It's the second foiled industrial espionage attempt in two years involving Amgen's signature drug. Los Angeles: *The Los Angeles Times*, p. D2 [Kota].
- Apuzzo, M. (2010, August 27). Federal contractor charged with leaking secrets. New York, NY: *Associated Press* [Kim].
- Arrillaga, P. (2011, May 8). How a networking immigrant became a spy. Miami, FL: *The Miami Herald*, p.2 [Kuo, Fondren, Bergersen].
- Ashenfelter, D. (2007, April 18). 2 Mich. Men charged as Iraqi spies—For years, they fed info to Hussein regime, U.S. says. Detroit, Michigan: *Detroit Free Press*, p. 3 [Shemami].
- Associated Press. (1976, March 1). U.S.-Soviet agent found dead. Washington, DC: *The Washington Post*, p. A1 [Rees].
- Associated Press. (2008, August 8). US man who spied for China gets nearly 16 years. Retrieved on August 8, 2008 at <http://www.mytimes.com/aponline/us/AP-Chinese-Spies.html> [Kuo, Bergersen, Kang].
- Associated Press. (2009, June 10). Man who spied for Iraq gets 46 months. Boston: *Boston Globe*, p. 10 [Shemami].
- Associated Press. (2010, February 4). Maui spy is competent to stand trial. Maui County, HI: *The Maui Weekly*, p. 1 [Gowadia].

## REFERENCES

- Associated Press. (2010, June 25). Judge cuts sentence of Louisiana man who spied for China. New Orleans, LA: *The Times-Picayune*, p. 4 [Kuo, Bergersen, Fondren].
- Associated Press. (2011, September 12). Man who tried to export jet to Iran sentenced. Retrieved on August 31, 2012 from <http://foxnews.com> [Knapp].
- Associated Press. (2012, July 20). Syrian agent working in US gets 18 months, admits spying on dissidents during Arab Spring. Washington, DC: *The Washington Post*, p. A5 [Soueid].
- Associated Press. (2012, May 7). CIA 'foiled al-Qaida bomb plot' around anniversary of Bin Laden death. London, UK: *The Guardian*, p. 10 [Sachtleben].
- Associated Press. (2012, October 1). Terror suspect Babar Ahmad files legal challenge against extradition to US at UK high court. Washington, DC: *The Washington Post*, p. A12 [Abujihaad].
- Associated Press. (2012, October 23). CIA 'whistleblower' John Kiriakou jailed for two years for identity leak." London, UK: *The Guardian*, p. 8 [Kiriakou].
- Associated Press. (2014, January 31). Gunman's doctor before rampage: 'No problem there.' New York, NY: *New York Post* p. 3 [Alexis].
- Baker, P. & Rudoren, J. (2015, November 20). Jonathan Pollard, American who spies for Israel, released after 30 years. New York, NY: *The New York Times*, p. A1 [Pollard].
- Bamford, J. (2014, August 22). The most wanted man in the world: Edward Snowden, the untold story. San Francisco, CA: *Wired Magazine*. Retrieved on September 10, 2014 from <http://www.wired.com/2014/08/edward-snowden> [Snowden].
- Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., Trzeciak, R. F. (2006, December). Comparing insider IT sabotage and espionage: A model-based analysis. Pittsburgh, PA: *Software Engineering Institute*, Carnegie Mellon University.
- Barakat, M. (2009, September 21). Retired AF officer goes on trial in China spy case. Washington, DC: *The Washington Examiner*, p. 1 [Fondren, Kuo].
- Barakat, M. (2011, January 21). US man gets 4 years in prison for attempted spy effort; received \$70K from Chinese handlers. Toronto, Canada: *The Canadian Press*, p. 8 [Shriver].
- Barandes, L. (2007). A helping hand: Addressing new implications of the Espionage Act on freedom of the press. *Cardozo Law Review*, 29: 371-403.

## REFERENCES

- Barandes, L. (2008). A helping hand: Addressing new implications of the Espionage Act on freedom of the press. Lexington, VA: *Cardozo Law Review*, 29(1), p. 371.
- Barnes, J. E. & Hodge, N. (2010, July 28). Military probe again targets Manning. New York, NY: *Wall Street Journal*, p. 13 [Manning].
- Barisic, S. (2006, December 4). Sailor pleads guilty to espionage. New York, NY: *Associated Press* [Weinmann].
- Barrett, D. (2013, September 23). Former FBI agent to plead guilty in leak case. New York, NY: *Wall Street Journal*, p. 6 [Sachtleben].
- Beck, M. (2000, Summer). Reforming the multilateral export control regimes. Monterey, CA: *The Nonproliferation review*. Journal of the James Martin Center for Nonproliferation Studies at the Monterey Institute of International Studies, Vol. 7(2), 91-103.
- Beckhusen, R. (2012, December 13). Pentagon warns: 'Pervasive' industrial spying targets U.S. space tech. New York, NY: *Wired Magazine*.
- Benkler, Y. (2014, September 8). A case for Edward Snowden's immunity. New York, NY: *The Atlantic* [Snowden].
- Bennet, B. (2015, March 6). CIA to create a digital spy division. Los Angeles, CA: *The Los Angeles Times*, p. 12.
- Berger, S. (1997, March 24). Memorandum from Samuel Berger, Assistant to the President for National Security Affairs, to George J. Tenet and John P. White, Co-Chairmen, Security Policy Board, Implementation of Executive Order 12968, Attachment. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information [the "Uniform Adjudicative Guidelines"].
- Bernstein, L. & Tate, J. (2013, August 22). Bradley Manning says he will live as a woman and seek hormone therapy in prison. Washington, DC: *The Washington Post*, p. 2 [Manning].
- Bhattacharjee, Y. (2014, May 5). A new kind of spy. New York, NY: *The New Yorker*, XC(11), 30-36 [Chung].
- Black, E. (2004, December 31). Spat erupts between neocons, intelligence community. Forward. Retrieved from <http://www.forward.com/main> [Franklin].
- Blau, E. (1976, March 1). Ex-Mobil Oil engineer linked to Soviet spying is called suicide. New York, NY; *The New York Times*, p. 5 [Rees].
- Bowman, M. E. (1995). Prosecuting spies: An uneasy alliance of security, ethics, and law. *Defense Intelligence Journal* 4(57-81).

## REFERENCES

- Boylan, P. & Perez, R. (2005, October 27). Isle man accused of selling secrets. Honolulu, HI: *The Honolulu Advertiser*, p. 1 [Gowadia].
- Boylan, P. (2005, October 28). Secrets sold: 'I did it for the money.' Honolulu, HI: *The Honolulu Advertiser*, p. 3 [Gowadia].
- Brenner, J. (2014, December 10). The new industrial espionage. *The American Interest*, 10(3). Retrieved on November 11, 2015 at <http://www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/> .
- Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 15). Israeli test on worm called crucial in Iran nuclear delay. New York, NY: *International New York Times*, p. 2.
- Brock, B. (1987, July). Spying's dirty little secret. *Money*, 16(7), 130-148.
- Brown, P. J. (2009, July 29). A midsummer tale of two Chinese spies. Los Angeles, CA: *The Los Angeles Times*, p. 6 [Chung, Shu].
- Bruce, J. B & Jameson, W. G. (2013). Fixing leaks: Assessing the Department of Defense's approach to preventing and deterring unauthorized disclosures. Santa Monica, CA: *RAND Corporation*.
- Bruce, J. B. (2002, November). Laws and leaks of classified intelligence: Costs and consequences of permissive neglect. Presented at a meeting of the National Security Committee, American Bar Association on November 22, 2002. Arlington, VA. Retrieved on May 21, 2007 from [http://cicentre.com/Documents/DOC\\_Classified\\_Leaks.htm](http://cicentre.com/Documents/DOC_Classified_Leaks.htm)
- Bumiller, E. (2010, July 8). Army leak suspect is turned in, by ex-hacker. New York, NY: *The New York Times*, p. 1 [Manning].
- Bunn, M. & Sagan, S. D. (2014). A worst practices guide to insider threats: Lessons from past mistakes. Cambridge, MA: *American Academy of Arts and Sciences*.
- Burkett, R. (2013, March). An alternative framework for agent recruitment: from MICE to RASCLS. *Studies in Intelligence*, 57(1) 7-17 (Extracts).
- Bush, J D., Dial, A. A., Fisher, J. H. (2013, January 8). Important changes to the federal Economic Espionage Act that protect trade secrets. Atlanta, GA: *Kilpatrick Townsend & Stockton LLP*. Retrieved on August 29, 2015 from <http://www.kilpatricktownsend.com/> .
- Campbell, D. Spooks admit it in private: Snowden has made them rethink their methods. London, UK: *The Guardian*, p. 3 [Snowden].
- Caplan, L. (2013, September 5). Leaks and consequences: Why treating leakers as spies puts journalists at legal risk. Washington, DC: *The American scholar*. Autumn, 2013.

## REFERENCES

- Caught on tape: Selling America's secrets. (2010, February 25). New York, NY: *CBS News*.
- Cavelty, M. D. (2012). The militarization of cyberspace: Why less may be better. 2012 4<sup>th</sup> International Conference on Cyber Conflict, C. Czosseck, R. Otis, & K. Ziolkowski, Eds. Tallinn, Estonia: NATO CCD COE Publications.
- Chaddock, G. R. (2009, June 6). How an American couple came to be spies for Cuba. *The Christian Science Monitor*, p. 3. [Myers]
- Charney, D. L. (2010, Fall/Winter). True psychology of the insider spy. *Intelligencer: Journal of U.S. Intelligence Studies*, 47-54.
- Chu, H. (1996, April 10). Retired engineer gets 2 years in Defense espionage case. Los Angeles, CA: *Los Angeles Times*, p. B4. [Charlton]
- CI Glossary—Terms and definitions of interest for DoD CI professionals. (2011, May 2). Washington, DC: Office of Counterintelligence (DXC), Defense CI & Humint Center, Defense Intelligence Agency. Retrieved May 5, 2015 from <http://fas.org/irp/eprint/ci-glossary.pdf> .
- Clapper, J. R. (2015, September 10). Statement for the record: Worldwide cyber threats. Provided to the House Permanent Select Committee on Intelligence, Washington, DC.
- Clark, C. S. (2015, April 29). CIA chief says overhaul puts spies and analysts 'cheek by jowl.' Washington, DC: *Government Executive*. Retrieved May 7, 2015 from <http://www.govexec.com/management/2015/04/cia-overhaul-puts-spies-and-analysts-cheek-jowl-brennan-says/111412/> .
- Clark, L. (2010, July 16). Ex-State Department analyst gets life for spying for Cuba. Miami, FL: *The Miami Herald*, p. 4. [Myers]
- Coen, J. (2007, April 17). 'Sleeper spy' is found guilty; Des Plaines man to remain in jail. Chicago, IL: *The Chicago Tribune*, p. 2 [Latchin].
- Cohn, D. & Caumont, A. (2016, March 31) 10 demographic trends that are shaping the U.S. and the world. Washington, DC: Pew Research Center, retrieved March 16, 2016 at <http://www.pewresearch.org/fact-tank/2016/03/31/10-demographic-trends-that-are-shaping-the-u-s-and-the-world/> .
- Coleman, R. C. (2014, May 13). Statement before the Committee on the Judiciary, Subcommittee on Crime and Terrorism. United States Senate. At a Hearing Entitled 'Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?' Washington, DC.
- Coll, S. (2013, April 1). The spy who said too much. New York NY: *The New Yorker*, 89(7): 54 [Kiriakou].

## REFERENCES

- Community members spied for Iraq. (2007, April 21). Detroit, Michigan: *The Arab American News*, p. 2 [Shemami].
- Congressional notification for authorized public disclosure of intelligence information. (2013, October 8). Directive-type Memorandum (DTM) 13-009. Washington, DC: Deputy Secretary of Defense.
- Corcoran, K. (2006, November 6). Convicted in spy case, locked away in secrecy. Indianapolis, IN: *The Indianapolis Star*. Retrieved November 8, 2006 at <http://www.indystar.com/apps/pbcs.dll/article>. [Shabaan]
- Cornell University Law School, (2015). 50 U.S. Code Chapter 35 International Emergency Economic Powers. Cornell, NY. *Legal Information Institute*. Retrieved January 13, 2015 at <http://www.law.cornell.edu/uscode/text/50/chapter-35>.
- Countering espionage, international terrorism, and the counterintelligence insider threat. (2012, May 4). Department of Defense Instruction, Number 5240.26. Washington, DC: Department of Defense.
- Cowan, A. L. & Chan, S. (2008, December 30). Ex-Army engineer pleads guilty to spying for Israel. New York, NY: *The New York Times*, p. 3 [Kadish].
- Cowell, A. (1999, November 10). Theodore Hall, prodigy and atomic spy, dies at 74. New York, NY: *The New York Times*, p. 16.
- Crawford, D. (1998) *Volunteers: The betrayal of national defense secrets by Air Force traitors*. Washington, DC: Government Printing Office [Buchanan].
- Cruz, M. (2010, August 11). Inmate dies on state's death row. San Bernardino, CA: *The Sun News*. Retrieved on July 20, 2015 from [http://www.sbsun.com/general-news/20100811/inmate-dies-on-states-death-row#disqus\\_thread](http://www.sbsun.com/general-news/20100811/inmate-dies-on-states-death-row#disqus_thread) [Diaz].
- Currier, C. (2013, July 30). Charting Obama's crackdown on national security leaks. New York, NY: *ProPublica*. Retrieved on June 19, 2015 from <https://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks>
- Cyber-Espionage nightmare: A groundbreaking online-spying case unearths details that companies wish you didn't know about how vital information slips away from them. (2015). Cambridge, MA: *MIT Technology Review* v.13.05.10.
- Daugherty, S. (2013a, August 16). Trial begins in Norfolk for ex-sailor accused of spying. Norfolk, VA: *Norfolk Virginian-Pilot*, p. 1. [Hoffman].
- Daugherty, S. (2013b, August 17). FBI targeted alleged spy by pretending to date him. Norfolk, VA: *Norfolk Virginian-Pilot*, p. 3 [Hoffman].

## REFERENCES

- Daugherty, S. (2014, February 13). Robert Hoffman: The spy who struck out. Norfolk, VA: *Norfolk Virginian-Pilot*, p. 1 [Hoffman].
- Denning, D. E. (2012, July 16). Stuxnet: What has changed? Basel, Switzerland: *Future Internet 4*, pp. 672-687.
- Denson, B. (2010, October 1). Former CIA spy Jim Nicholson passed messages to Russians via crumpled napkins, prosecutors allege in new case. Portland, OR: *The Oregonian*, p. 1 [Nicholson].
- Denson, B. (2011, May 26). The spy's kid: Jim Nicholson spares his son Nathan from a courtroom confrontation (part 6). Portland, OR: *The Oregonian*, p.10. [6-part series and related articles based on interviews with Nathaniel Nicholson, *The Oregonian*, May 21-May 26, 2011].
- Department of Defense Directive. (2014, September 10). The DoD insider threat program. Washington, DC: Office of the Undersecretary of Defense for Intelligence.
- Department of Defense Security Institute. (1990, January) The case of Randy Miles Jeffries and Acme Reporting. Richmond, VA: *Security Awareness Bulletin*, 2-90. [Jeffries].
- Department of Justice, Office of Public Affairs. (2012, July 20). Virginia man sentenced to 18 months in prison for acting as an unregistered agent of the Syrian government. Washington, DC [Soueid].
- Department of Justice, Office of Public Affairs. (2013, June 21). Former workers at Los Alamos National Laboratory plead guilty to Atomic Energy Act violations. Washington, DC [Mascheroni].
- Department of Justice. (2008, April 22). Public release: Man arrested for disclosing national defense information to Israel. New York, NY: U.S. Attorney for the Southern District of New York [Kadish].
- Department of Justice. (2011, January 13). California man pleads guilty to attempted military exports to Iran. United States District Attorney, District of Delaware [Knapp].
- Department of Justice. (2014). Report of the Attorney General to the Congress of the United States on the administration of the Foreign Agents Registration Act of 1938, as amended, for the six months ending June 30, 2015. Washington, DC.
- Department of Justice. (2015). Criminal Resource Manual: 2062. Foreign agents registration act enforcement. Washington, DC: Offices of the United States Attorneys.
- Department of Justice. (2015). National Security Division: Foreign Agents Registration Act. Washington, DC.

## REFERENCES

- Department of Justice. (2016, February). Former U.S. Nuclear Regulatory Commission employee pleads guilty to attempted spear-phishing cyber-attack on Department of Energy computers. Washington DC: Office of Public Affairs [Eccleston].
- Department of the Army. (2010, October 4). Military intelligence: Threat awareness and reporting program. Army Regulation 381-12. Washington, DC: Department of Defense.
- Dishneau, D. & Jelinek, P. (2011, December 20). US close to resting case against Manning. New York, NY: *Associated Press*. Retrieved December 20, 2011 from <http://news.yahoo.com/us-close-resting-case-against-manning-150522051.html> [Manning].
- Dolan, M. (1986, January 15). Messenger indicted in Soviet spying case. Los Angeles, CA: *Los Angeles Times*, p. 4 [Jeffries].
- Dooley, J. (2009a, January 7). Secrecy tested in Isle spy case. Honolulu, HI: *The Honolulu Advertiser*, p. 2 [Gowadia].
- Dooley, J. (2009b, January 25). Judge to rule on spy case evidence. Honolulu, HI: *The Honolulu Advertiser*, p. 2 [Gowadia].
- Dooley, J. (2010, April 14). Trial of accused spy begins. Honolulu, HI; *The Honolulu Advertiser*, p. 4 [Gowadia].
- Doyle, C. (2014, July 25). Stealing trade secrets and economic espionage: An abridged overview of 18 U. S. Code 1831 and 1832. CRS Report R42682. Washington, DC: Congressional Research Service.
- Doyle, C. (2014, July 25). Stealing trade secrets and economic espionage: An overview of 18 U.S.C. 1831 and 1832. Washington, DC: *Congressional Research Service*, R42681.
- Dsouza, L. (2012, March 14). Noshir Gowadia father of Chinese stealth technology. Retrieved from *Defence Aviation* on October 5, 2015 from <http://www.defenceaviation.com/2012/03/noshir-gowadia-father-of-chinese-stealth-technology.html> [Gowadia].
- Earley, P. (1997). Confessions of a spy: The real story of Aldrich Ames. New York, NY: Berkley Books, *The Berkley Publishing Group. Penguin Putnam, Inc.*
- Earley, P. (2001). All about Aldrich Ames. The Crime Library. Retrieved on January 17, 2003, at <http://www.crimelibrary.com/spies/ames/index.htm> .
- Economic Espionage Act. (1996). Title 18 U.S.C. sections 1831-1839.
- Economic impact of trade secret theft: A framework for companies to safeguard trade secrets and mitigate potential threats. (2014). Washington DC: *Center for Responsible Enterprise and Trade (CREATE)*

## REFERENCES

- Edgar, H. & Schmidt, Jr., B. C. (1973, May). The espionage statutes and publication of defense information. New York, NY: *Columbia Law Review* 73(5). 929-1087.
- Egan, P. (2009, January 3). Prosecutors: Metro area men spied for Saddam; Attorneys, relatives deny charges, say some were coerced by Iraqi regime. Detroit, Michigan: *The Detroit News*, p. 4 [Shemami].
- Electronic spycraft is getting easier but more controversial. The old-style human sort is getting harder but more useful. (2015, August 1). London, UK: *The Economist*. p. 20-22.
- Elkus, A. (2015, June 18). The devastating breach of US government data highlights an illusory cybersecurity paradox. *Business Insider*. Retrieved on June 19, 2015 from <http://www.businessinsider.com/the-opm-breaches-cybersecurity-paradox-2015-6> .
- Elmhirst, S. (2009, February 5). China's final frontier. London, UK: *Newstatesman*, retrieved February 6, 2009 from <http://www.newstateman.com/print/200902050023> [Chung].
- Elsea, J. (2006, December 26). Protection of national security information. Congressional Research Service: *CRS Report for Congress*. Washington, DC: Government Printing Office.
- Elsea, J. K. (2013, September 9). Criminal prohibitions on the publication of classified Defense information. Congressional Research Service, R41404. Washington, DC: Government Printing Office.
- Engelberg, S. (1986, February 22). Spy for China found suffocated in prison, apparently a suicide. New York, NY: *The New York Times*, p. A3 [Chin].
- Epstein, R.D. (2007). Balancing national security and free-speech rights: Why Congress should revise the Espionage Act. *Commlaw Conspectus*, 15: 483-512.
- Ex-Boeing engineer guilty in space shuttle spy case. (2009, July 16). New York, NY: *The New York Times*, p. 3. [Chung].
- Executive Order 13526. Classified national security information. December 29, 2009.
- Executive Order 13587. Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information, October 7, 2011.
- Executive Order 9176, Transferring the administration of the act of June 8, 1938, as amended, requiring the registration of agents of foreign principals, from the Secretary of State to the Attorney General, January 19, 1942.

## REFERENCES

- Ex-sailor charged in terror case discussed attacking military personnel, prosecutor says. (2007, July 24). Tucson, AZ: *Arizona Daily Star*, p. B3. [Abujihaad].
- Federal Bureau of Investigation Eastern District of Virginia. (2012, October 23). Former CIA officer John Kiriakou pleads guilty to disclosing classified information about CIA officer. Washington, DC: United States Attorney's Office [Kiriakou].
- Federal Bureau of Investigation Los Angeles Division. (2003). Affidavit in support of a complaint against and arrest warrant for John Jouongwoong Yai and Susan Youngja Yai. Los Angeles, CA [Yai].
- Federal Bureau of Investigation Los Angeles Division. (2014, September 8). Former Air Force employee sentenced to prison for retaining stolen government property to sell to a foreign government. Los Angeles, CA: United States Attorney's Office [Orr].
- Federal Bureau of Investigation. (2006, September 14). Congressional testimony: Statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation before the House Appropriations Subcommittee on Science, the Department of State, Justice and Commerce, and Related Agencies. Washington, DC: author. [Shabaan]
- Federal Bureau of Investigation. (2014). News. Stories: Naval espionage; Stopping a dangerous insider threat. Retrieved December 8, 2014 from <http://www.fbi.gov/news/stories/2014/march/naval-espionage-stopping-a-dangerous-insider-threat> [Hoffman].
- Federal Bureau of Investigation. (2014, May 19). News Blog: Five Chinese military hackers charged with cyber espionage against U.S. Washington, DC: Department of Justice.
- Fergusson, I. F. & Kerr, P. K. (2014, January 13). The U.S. export control system and the President's reform initiative. Washington, DC: *Congressional Research Service*, R41916.
- Fergusson, I. F. (2009, July 15). The Export Administration Act: Evolution, provisions, and debate. Washington, DC: *Congressional Research Service*, RL31832.
- Figliuzzi, C. F. (2012, June 28). Statement for the record before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives, at a hearing entitled "Economic espionage: A foreign intelligence threat to American jobs and homeland security." Washington, DC.
- Fishman, S. (2011, July 11). Bradley Manning's army of one. New York, NY: *New York Magazine*, p. 26 [Manning].

## REFERENCES

- Flaccus, G. (2009, June 24). First US economic espionage trial winds down. The Associated Press. Retrieved July 13, 2009 from [http://www.Google.com/hosted\\_news/ap/article](http://www.Google.com/hosted_news/ap/article) [Chung].
- Flaccus, G. (2009, May 31). First economic espionage trial set in Calif. Washington, DC: *The Washington Post*, p. 2 [Chung].
- Flaccus, G. (2010, February 8). Chinese-born spy gets more than 15 years for Calif. Espionage case involving space shuttle. Los Angeles, CA: *Los Angeles Times*, p. 12 [Chung].
- Foreign Agents Registration Act. (1938). 22 U.S.C section 611.
- Foreign Press Center Briefing Transcript. (2000, March 7). Intelligence gathering and democracies: The issue of economic and industrial espionage. A briefing by James Woolsey, former director, Central Intelligence Agency. Retrieved on October 19, 2015 from <http://fas.org/irp/news/2000/03/wool0300.htm> .
- Former sailor is convicted in terror case. (2008, March 6). New York, NY: *The New York Times*, p. A1 [Abujihaad].
- Former US officer leaked secrets to Chinese girlfriend. (2014, September 18). Washington, DC: *Agence France-Press* [Bishop].
- Freeman, C. (2014, December 17). US-Cuba prisoner exchange—who are the ‘Cuban five?’ London, UK: *The Telegraph*, p. 2 [Guerrero].
- Gates, D. (2006, January 22). Separation anxiety: The wall between military and commercial technology. Seattle, WA: *The Seattle Times*, p. 3.
- Gault, M. (2015, June 17). Has China learned how to build the perfect U.S. spy? London, UK: *Reuters*, p. 5.
- Gentile, C. (2009, June 18). Cuban spies’ shortwave radios defy detection. Washington, DC: *Washington Times*, p.1. [Myers]
- Gerstein, J. (2006, July 14). A novel-like tale of cloak, dagger unfolds in court. New York, NY: *The New York Sun*, p. 4 [Keyser].
- Gerstein, J. (2013, September 23). Ex-FBI agent admits to AP leak. New York, NY: *Politico*, p. 4 [Sachtleben].
- Gerstein, J. (2015, February 3). Intelligence agencies tout transparency. New York: NY: *Politico*, p. 2 [Snowden].
- Gerth, J. (1989, March 10). Ex-Sergeant’s spy case is said to grow in seriousness. New York, NY: *The New York Times*, p. A10 [Conrad, Szabo].
- Gertz, B. (1993, February 6). Ex-DIA official pleads guilty in document leak. Washington, DC: *Washington Times*, p. 2 [Hamilton].

## REFERENCES

- Gertz, B. (2006, November 23). China bought bomber secrets. Washington, DC: *The Washington Times*, p. 2 [Gowadia].
- Gertz, B. (2006, September 18). Enemies. Washington, DC: *The Washington Times*, p. 21 [Chi Mak, Chung].
- Gertz, B. (2007, December 12). Engineer indicted on spying. Washington, DC: *The Washington Times*, p. 1 [Gowadia].
- Gertz, B. (2009, July 29). Defense analyst in spy case was FBI double agent. Washington, DC: *Washington Times*, p. 1 [Franklin].
- Gertz, B. (2014, June 10). U.S. in talks with Snowden on possible plea deal. Washington, DC: *The Washington Free Beacon*, p. 1 [Snowden].
- Gertz, B. (2014, October 31). New Chinese intelligence unit linked to massive cyber spying program: Axiom likely a Ministry of State security spy unit. Washington, DC: *The Washington Free Beacon*, p. 3.
- Gertz, B. (2015, January 22). NSA details Chinese cyber theft of F-35, military secrets. Chinese hackers pillaged U.S. defense, contractor networks for critical data. Washington, DC: *The Washington Free Beacon*, p. 1 [Snowden].
- Gilpin, R. with Gilpin, J. M. (2000). The challenge of global capitalism: The world economy in the 21<sup>st</sup> century. Princeton, NJ: *Princeton University Press*, chap. 1 *passim*.
- Glod, M. (2010, May 25). Former FBI employee sentenced for leaking classified papers. Washington, DC: *The Washington Post*, p. 3 [Leibowitz].
- Golden, T. (2002, October 17). Ex-U.S. aide sentenced to 25 years for spying for Cuba. New York, NY: *The New York Times*, p. A6 [Montes].
- Golden, T. (2007, October 21). Naming names at Gitmo. New York, NY: *The New York Times*, p. D1 [Diaz].
- Goodman, J.D. (2011, October 12). U.S. accuses Virginia man of espionage at Syria protests. New York: *The New York Times*, p. 17 [Soueid].
- Gordon, M. (2005, October 28). Grave consequences possible, experts say: Secrets sold: 'I did it for the money.' Honolulu, HI: *The Honolulu Advertiser*, p. 2 [Gowadia].
- Greenwald, G, MacAskill, E., & Poitras, L. (2013, June 11). London, UK: *The Guardian*, p. 1 [Snowden].
- Grieco, E. M., Acosta, V. D., de la Cruz, G. P., and 5 others. (2012, May) The foreign-born population in the United States: 2010. *American Community Survey Reports*. Washington, DC: United States Census Bureau.

## REFERENCES

- Hammer, D. (2008, May 14). Spy for Chinese pleads guilty. New Orleans, LA: *Times-Picayune*, p. 3 [Kang, Kuo, Bergersen].
- Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). Chinese industrial espionage: Technology acquisition and military modernization. New York, NY: *Routledge*, chaps. 7-10 *passim*.
- Harnden, T. (2009, October 5). Spying for Fidel: The inside story of Kendall and Gwendolyn Myers. Washington, DC: *Washingtonian Magazine*. Retrieved December 11, 2009 at <http://www.washingtonian.com/articles/people/spying-for-fidel-the-inside-story-of-kendall-and-gwen-myers/>
- Harris, C. R., Jenkins, M., & Glaser, D. (2006, July). Gender differences in risk assessment: Why do women take fewer risks than men? Online journal hosted at University of Pennsylvania: *Judgment and Decision Making*, 73(5): 48-63.
- Harris, S. (2010, July 21). Plugging the leaks: Barack Obama hates leaks, and thanks to a tenacious prosecutor, the Justice Department is on its way to setting a record for leak prosecutions. Washington, DC: *The Washingtonian*. Retrieved on July 26, 2011 from <http://www.washingtonian.com/articles/people/plugging-the-leaks/>
- Harris, S. (2014a, May 27). Exclusive: inside the FBI's fight against Chinese cyber-espionage. *Foreign Policy*. Retrieved on November 3, 2015 from <http://fpgroup.foreignpolicy.com/> .
- Harris, S. (2014b, November 16). Google's secret NSA alliance: The terrifying deals between Silicon Valley and the security state. *Salon*. Retrieved November 30, 2015 from [http://www.salon.com/writer/shane\\_harris/](http://www.salon.com/writer/shane_harris/) .
- Harris, S. (2015, May 6). CIA's ex-no. 2 says ISIS 'learned from Snowden.' Retrieved on May 15, 2015 from <http://www.thedailybeast.com/articles/2015/05/06/cia-s-ex-no-2-says-isis-learned-from-snowden.html> .
- Hattem, J. (2016, March 30). Former intelligence chairman: More foreign spies in U.S. than ever. Washington, DC: *The Hill*. Retrieved on April 6, 2016 at <http://thehill.com/policy/national-security/274704-former-intel-chairman-more-foreign-spies-in-us-than-ever-before>.
- Herbig, K. L. & Wiskoff, M. F. (2002). Espionage against the United States by American citizens 1947-2001. Monterey, CA: Defense Personnel Security Research Center.
- 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*. Westport, CT: *Praeger*.

## REFERENCES

- Herbig, K. L. (2008, December). Allegiance in a time of globalization. Monterey, CA: Defense Personnel Security Research Center.
- Herbig, K. L. (2008, March). Changes in espionage by Americans: 1947-2007. Monterey, CA: Defense Personnel Security Research Center.
- Heskett, J. (2009, November 4). What is the role of government vis-à-vis capitalism? Working Knowledge. Cambridge, MA: Harvard Business School, retrieved on October 20, 2015 from <http://hbswk.hbs.edu/item/6304.html> .
- Heuer, Jr., R. J. (1992). Compulsive gambling: Background information for security personnel. Monterey, CA: Defense Personnel Security Research Center.
- Heuer, Jr., R. J. (2008, May 8). FOUO. Potential counterintelligence risk indicators. Working Paper 08-03. Monterey, CA: Defense Personnel Security Research Center.
- Horwitz, S. (2013, September 23). Ex-FBI agent to plead guilty in leak to AP. Washington, DC: *The Washington Post*, p. 9 [Sachtleben].
- Hosenball, M. & Strobel, W. (2013, November 7). Exclusive: Snowden persuaded other NSA workers to give up passwords—sources. New York, NY: *Reuters*, p.2 [Snowden].
- House of Representatives 110 Congress, Second Session. Committee on the Judiciary. Subcommittee of Crime, Terrorism, and Homeland Security. (2008, January 29). Hearing: Enforcement of federal espionage laws. Washington, DC; U.S Government Printing Office.
- Hsu, S. S. (2010, August 28). State Dept. contractor charged in leak to news organization. Washington, DC: *The Washington Post*, p. A14 [Kim].
- Hsu, S. S. (2010, July 16). U.S. analyst spying for Cuba gets life in prison; wife gets more than 6 years. Washington, DC: *The Washington Post*, p. A6 [Myers].
- Hsu, S. S. (2016, February 2). Former Energy Dept. employee pleads guilty in nuclear secrets sting case. Washington, DC: *The Washington Post*, p. A2 [Eccleston].
- Ignatius, D. (2014, June 5). Edward Snowden took less than previously thought, says James Clapper. Washington, DC: *The Washington Post*, p. 12 [Snowden].
- Immigration and Customs Enforcement. (2011, September 12). News Releases: California man sentenced to nearly 4 years in prison for attempting to export military items to Iran. Retrieved on August 31, 2012, from <http://www.ice.gov/news/releases> [Knapp].

## REFERENCES

- Internal review of the Washington Navy Yard shooting. (2013, November 20). A report to the Secretary of Defense. Washington, DC: Under Secretary of Defense for Intelligence.
- Internet Live Stats. (2016). Internet users by year. Retrieved on January 14, 2016 from <http://www.internetlivestats.com/internet-users/#trend> .
- Israel, R. C. (2012, Spring/Summer). What does it mean to be a global citizen? *Kosmos: Journal for Global Transformation*. Retrieved on December 21, 2015 from [http://www.kosmosjournal.org/featured-topics/living\\_earth/](http://www.kosmosjournal.org/featured-topics/living_earth/) .
- Jaffe, G. & Nakashima, E. (2011, February 2). Leak suspect wasn't fit for war. Washington, DC: *The Washington Post*, p. 1 [Manning].
- Jenkins, B. M. (2011). Stray dogs and virtual armies: Radicalization and recruitment to Jihadist terrorism in the United States since 9/11. Santa Monica, CA: *RAND Corporation*.
- Joffe-Walt, C. & Spiegel, A. (2012, May 1). Psychology of fraud: Why good people do bad things. Retrieved May 2, 2012 from <http://www.npr.org/2012/05/01/151764534/psychology-of-fraud-why-good-people-do-bad-things>
- Johnson, C. (2008, April 23). Man, 84, is charged with spying for Israel in 1980s. Washington, DC: *The Washington Post*, p. A04 [Kadish].
- Johnston, D. (2006, January 21). Former military analyst gets prison term for passing information. New York, NY: *The New York Times*, p. 6 [Franklin].
- Joint CIA-FBI press release on arrest of Harold James Nicholson. (1996, November 18). Washington, DC: Federal Bureau of Investigation. [Nicholson].
- Kemp, S. (2015, August). Digital, Social, & Mobile in 2015. New York, NY: *We Are Social, Inc*. Retrieved on December 16, 2015 at <http://wearesocial.com/us/special-reports/global-statshot-august-2015> .
- Kenber, B. (2013, August 28). Nidal Hasan sentenced to death for Fort Hood shooting rampage. Washington, DC: *The Washington Post*, p. A1.
- Kennedy, S. & Ruggles, S. (2014, Jan. 08). Breaking up is hard to count: The rise of divorce in the United States, 1980-2010. *Demography* 51(2): 587-598.
- Kershaw, S. (2004, February 19). Guardsman charged with trying to spy for Al Qaeda. New York, NY: *The New York Times*, p. 3 [Anderson].
- Kiriakou, J. (2014, March 9). I got 30 months in prison. Why does Leon Panetta get a pass? Los Angeles, CA: *The Los Angeles Times*, p. 24 [Kiriakou].
- Klopott, F. (2009, October 20). Defense official wants his espionage conviction tossed. Washington, DC: *The Washington Examiner*, p. 5 [Fondren, Kuo].

## REFERENCES

- Koerner, B. (2003, July 10). Who must register as a foreign agent? New York, NY: *Slate*.
- Kotowoski, J. (2011, January 7). Man sentenced to 5 years for acting as a foreign agent. Bakersfield, CA: *The Bakersfield Californian*, p. 1 [Ali].
- Kredo, A. (2010, June 3). Shamai Leibowitz sentenced for leaking FBI secret. Washington, DC: *Washington Jewish Week*, p. 1 [Leibowitz].
- Krikorian, G. (2003, February 6). FBI watched spy suspect for 7 years. Los Angeles, CA: *Los Angeles Times*, p. 6 [Yai].
- Krotoski M. L. (2009, November). Common issues and challenges in prosecuting trade secret and economic espionage cases. Columbia, SC: *United States Attorneys' Bulletin*, 57(5), pp. 2-23.
- Krotoski, M. L. & Harrison, J. (2015, May 8). Reviewing the first foreign economic espionage cases. Washington, DC: *Bloomberg BNA: Patent, Trademark, & Copyright Journal*, 90 (PTCJ 1951), pp. 1-8.
- Kundnani, A. & Theoharis, J. (2014, July 23). Breaking the spell of the official terrorism narrative. London, UK: *The Guardian*, p. 3 [Abujihaad].
- Kuntz, R. L. (2013, September 1). How not to catch a thief: Why the economic Espionage Act fails to protect American trade secrets. Berkeley, CA: *Berkeley Technology Law Journal*, 28(4), 901-932.
- LaFraniere, S. (2013, July 20). Math behind leak crackdown: 154 cases, 4 years, 0 indictments. New York, NY: *The New York Times*, p. A3.
- Lamothe, D. (2015, January 23). Army details the strange, downward spiral of Fort Hood shooter Ivan Lopez. Washington, DC: *The Washington Post*, p. 4 [Lopez].
- Landivar, L. C. (2013). Disparities in STEM employment by sex, race, and Hispanic origin. American Community Survey (ACS) ACS-24, Washington, DC: U.S. Census Bureau.
- Leinwand, D. (2008, March 2). FBI follows paper trail to uncover Iraqi spies. McLean, Virginia: *USA Today*, p. 5 [Shemami].
- Lentz, P. (1985, June 13). Why spy? Try greed, high tech, lax controls. Chicago, IL: *The Chicago Tribune*, p. A1.
- Levine, J. (2012, July 1). Reevaluating ITAR: A holistic approach to regaining critical market share while simultaneously attaining robust national security. Miami, FL: *University of Miami National Security & Armed Conflict Law Review*, Vol. 2(1), 1-8.

## REFERENCES

- Lewis, N.A. & Johnston, D. (2009, May 9). U.S. to drop spy case against pro-Israel lobbyists. New York, NY: *The New York Times*, p. 1 [Kadish].
- Lewis, N.A. (2008, July 10). Spy cases raise concerns on China's intentions. New York, NY: *The New York Times*, p. A-2 [Bergersen, Kuo, Kang, Chung].
- Lichtblau, E. & Risen, J. (2009, April 16). Officials say U.S. wiretaps exceeded law. New York, NY: *The New York Times*, p. 6.
- Lichtblau, E. (2009, January 30). Jailed C.I.A. mole kept spying for Russia, via son, U.S. says. New York, NY: *The New York Times*, p. 3 [Nicholson].
- Limbago, A. L. (2014, August 20). The more things change...Espionage in the digital age. Retrieved on November 20, 2015 from <https://www.endgame.com/blog/more-things-changeespionage-digital-age> .
- Lindsey, R. (1979). *The Falcon and the Snowman*. New York, NY: *Simon & Schuster*. [Boyce, Lee].
- Lotrionte, C. (2015, Winter). Countering state-sponsored cyber economic espionage under international law. Chapel Hill, NC: *North Carolina Journal of International Law*, 40(2), 443-541
- Mahony, E. H. (2009, March 5). Judge overturns 1 of ex-sailor's 2 terror convictions. Hartford, CT: *The Hartford Courant*, p. 2 [Abujihaad].
- Management of serious security incidents involving classified information. (2014, October 27). ). Department of Defense Directive, Number 5210.50. Washington, DC: Department of Defense.
- Manual for Courts-Martial United States (2012 Edition). (2012). Washington, DC: Joint Service Committee on Military Justice. Retrieved on May 5, 2015 from <http://www.apd.army.mil/pdffiles/mcm.pdf> .
- Marimow, A. E. (2013, June 25). A rare look into w Justice Department leak probe. Washington, DC: *The Washington Post*, p. 4 [Kim].
- Marimow, A. E. (2014, April 2). Ex-State Dept. advisor Stephen J. Kim sentenced in leak case. Washington, DC: *The Washington Post*, p. 3 [Kim].
- Marimow, A. E., & Leonnig, C. D. (2013, December 3). Lawyers for ex-State Dept. worker Stephen J. Kim urge Holder to drop leak charges. Washington, DC: *The Washington Post*, p. 2 [Kim].
- Markon, J. & Johnson, C. (2008, April 1). Former Pentagon official pleads guilty to espionage. Washington, DC: *The Washington Post*, p. 4 [Fondren].
- Markon, J. (2005a, July 3.) FBI tapped talks about possible secrets. Washington, DC: *The Washington Post*, p. A2 [Franklin].

## REFERENCES

- Markon, J. (2005b, October 6). Defense analyst guilty in Israeli espionage case. Washington, DC: *The Washington Post*. p. A4 [Franklin].
- Markon, J. (2008, February 12). Defense official is charged in Chinese espionage case. Washington, DC: *The Washington Post*, p. A01 [Bergersen, Kuo].
- Markon, J. (2009, May 1). Prosecutors to drop charges against two former AIPAC lobbyists. Washington, DC: *The Washington Post*, p. p. 3 [Franklin].
- Macavoy, A. (2008, August 3). Hawaii man accused of helping China design missile. McLean, VA: *USA Today*, p. 7 [Gowadia].
- McDonnell, P. J. (2010, February 9). Chinese-born engineer gets 15 years in spying for China. Los Angeles, CA: *Los Angeles Times*, p. 6 [Chung].
- McGlone, T. (2006, December 10). Why a patriotic teen joined the Navy and then turned to espionage. Norfolk, VA: *Norfolk Intelligencer-Pilot*, p. 4 [Weinmann].
- McGlone, T. (2008a, September 25). Scientist charged with illegally selling technology to China. Hampton Roads, VA: *The Virginian-Pilot*, p. 1 [Shu].
- McGlone, T. (2008b, September 30). Physicist charged with selling technology free on bond. Hampton Roads, VA: *The Virginian-Pilot*, p. 3 [Shu].
- McGlone, T. (2012, December 12). Former Va. Beach sailor denied bond in spying case. Norfolk, VA: *Norfolk Virginian-Pilot*, p. 5 [Hoffman].
- McKenna, M. (2010, August 7). 'Spy' turned to stealth after ADF deal fell through. Melbourne, AU: *The Australian*, p. 1 [Gowadia].
- Medina, J. (2007, March 9). Sailor started e-mail on terror, U.S. says. New York, NY: *The New York Times*, p. 9 [Abujihaad].
- Meiman, Y. (2008, April 24). The timing/conspiracy theories abound. Retrieved on April 24, 2008 from <http://www.Haaretz.com/hasen/spages/977463.html> [Kadish].
- Miami Spy-hunting. (2000, February 19). Miami, FL: *The Miami Herald*, p. 4 [Alonso, Santos, Linda Hernandez, Nilo Hernandez, Guerrero].
- Michigan Technological University. (2015). Research: Export control laws and regulations. Retrieved on September 22, 2015 from <http://www.mtu.edu/research/administration/integrity-compliance/export-controls-foreign-nationals/export-control/>.
- Miller, B. & Pincus, W. (1994, April 22). Wife in spy case cites 'confusion' in interview. Washington, DC: *The Washington Post*, p. D1 [Rosario Ames].
- Miller, G. (2013, June 12). The low-profile, tech-savvy intelligence risk. Washington, DC: *The Washington Post*, p. 4 [Manning, Snowden].

## REFERENCES

- Miller, G. (2015, February 23). CIA looks to expand its cyber espionage capabilities. Washington, DC: *The Washington Post*, p. 6.
- Molotsky, I. (1985, June 6). Money said to have replaced ideology as main spy motive. New York: NY: *The New York Times*, p. B13.
- Monaco, L. O. (2014, February 11). Near-term measures to reduce the risk of high-impact unauthorized disclosures. White House Memorandum. Washington, DC: Assistant the President for Homeland Security and Counterterrorism.
- Montlake, S. (2008, April 2). Former Pentagon official pleads guilty in China spy case. Retrieved on April 3, 2008 from <http://www.csmonitor.com/World/terrorism-security/2008/0401/p99s01-duts.html> [Bergersen, Kuo, Kang].
- Morris, T. (2008, August 1). Woman sentenced in Chinese spy case. New Orleans, LA: *Times-Picayune*, p. 6 [Kang, Bergersen, Kuo].
- Murphy, J. (2015, March 24). How technology is changing the future of espionage. SOFREP News. Retrieved on November 20, 2015 from <http://sofrep.com/40315/technology-changing-future-espionage/> .
- Myers, S. L. (2013, October 31). In shadows, hints of a life and even a job for Snowden. New York, NY: *The New York Times*, p. 11 [Snowden].
- Nakashima, E. & Tate, J. (2011, December 18). Soldier's gender identity issues are raised in Wikileaks case. Washington, DC: *The Washington Post*, p. 4 [Manning].
- Nakashima, E. (2010, July 29). FBI, Justice Dept. help investigate sources of leaked war documents. Washington, DC: *The Washington Post*, p.7 [Manning].
- Nakashima, E. (2011, May 8). Bradley Manning is at the center of the WikiLeaks controversy. But who is he? Washington, DC: *The Washington Post*, p. D1 [Manning]. This seminal article is based on 30 interviews with Manning's family and friends.
- Nakashima, E. (2014, February 13). NSA employee implicated in Snowden probe resigned, memo says. Washington, DC: *The Washington Post*, p. 5 [Snowden].
- Nakashima, E. (2015, November 16). World's richest nations agree hacking for commercial benefit is off-limits. Washington, DC: *The Washington Post*, p. 2.
- National Intelligence Council. (2008). Global trends 2025: A world transformed. NIC 2009-003. Washington, DC.
- Navy lawyer on trial for leaking info. (2007, May 14). *Morning Edition*. National Public Radio, transcript [Diaz].

## REFERENCES

- Neumeister, L. (2008, April 23). Ex-prosecutor: New arrest shows reach of 1980s spy ring. Washington, DC: *The Washington Post*, p. 3 [Kadish].
- Neumeister, L. (2009, May 29). Ex-Army engineer who gave documents to Israelis gets no NY prison term but is fined \$50,000. Retrieved on June 5, 2009 from <http://www.wpix.com/news/nationworld/sns-ap-us-arrest,0,1950531,print.story> [Kadish].
- New intelligence agency established. (2014, December 1). Washington, DC: WTOP All News Radio Station.
- Newman, A. & Fahim, K. (2008, April 24). New Jersey neighbors sift memory for evidence that a spy was among them. New York, NY: *The New York Times*, p. 4 [Kadish].
- Newman, A. (2008, April 23). Ex-engineer for Army is accused of spying for Israel in 1980s. New York, NY: *The New York Times*. p. 2 [Kadish].
- Nicks, D. (2010, September 23). Private Manning and the making of Wikileaks. Retrieved March 4, 2011 from <http://thislandpress.com/09/23/2010/private-manning-and-the-making-of-wikileaks-2/print/> [Manning].
- Niese, M. (2010, August 10). Stealth expert guilty of selling secrets to China. San Diego, CA: *San Diego Union-Tribune*. Retrieved on October 5, 2015 from <http://www.sandiegouniontribune.com/news/2010/aug/10/stealth-expert-guilty-of-selling-secrets-to-china/> [Gowadia].
- Norfolk Naval officer faces court-martial in espionage case. (1995, September 13). Washington, DC: *The Washington Post*, p. D4 [Schwartz].
- O'Harrow, Jr., R. (1992, December 29). Man stepping off plane at Dulles is arrested on espionage charges. Washington, DC: *The Washington Post*, p. B1 [Baynes].
- O'Sullivan, S. (2011, January 13). Delaware courts: Man admits he violated export ban, pleads guilty. Retrieved on July 11, 2011 from <http://www.Delawareonline.com> [Knapp]
- Office of the National Counterintelligence Executive. (2011, October). Foreign spies stealing U.S. economic secrets in cyberspace. Washington, DC.
- Olive, R. J. (2006). Capturing Jonathan Pollard. Annapolis, MD: *Naval Institute Press*.
- Osborn, A. & Anishchuk, A. (2013, July 2). Snowden threatens new U.S. leaks, asks numerous countries for asylum. New York, NY: *Reuters*, p. 2 [Snowden].

## REFERENCES

- Pearce, M. (2016, January 20). Where are Iran's billions in frozen assets, and how soon will it get them back? Los Angeles: *Los Angeles Times*, p. 16.
- Pentagon man jailed over spying. (2006, January 20). *British Broadcasting Corporation News*. Retrieved from <http://news.bbc.co.uk/go/pr/fr> [Franklin].
- Pentagon officials charged in China espionage case. (2009, May13). Washington, DC: *Agence-France Presse*, p. 1 [Fondren, Kuo, Bergersen, Kang].
- Perez, E. (2010, July 17). Spy for Cuba, unrepentant, gets life. New York, NY: *The Wall Street Journal*, p. 4 [Myers].
- Peterson, A. (2015, July 13). It's not just OPM: Cybersecurity across the federal government is pretty awful. Washington, DC: *The Washington Post*, p. 6.
- Pilkington, E. (2013, July 31). Bradley Manning verdict: Cleared of 'aiding the enemy' but guilty of other charges. London, UK: *The Guardian*, p. 2 [Manning].
- Pincus, W. (2009, May 5). A look at the dropping of espionage charges. Washington, DC: *The Washington Post*, p. 8 [Franklin].
- Pincus, W. (2010, November 8). Imprisoned former CIA official pleads guilty again. Washington, DC: *The Washington Post*, p. 6 [Nicholson].
- Pincus, W. (2013, July 9). Questions for Snowden. Washington, DC: *The Washington Post*, p. A7 [Snowden].
- Poole, P. (2010). 10 failures of the U.S. government on the domestic Islamist threat. Washington, DC: *The Center for Security Policy* [Mohamed].
- Popkin, J. (2013, April 25). Woman indicted in Cuba spy case is in Sweden and out of U.S. reach. Washington, DC: *The Washington Post*, p. A5 [Velazquez].
- Potter, D. (2008, November 13). Va. Scientist pleads guilty to China tech sales. New York, NY: *Associated Press*, p. 2 [Shu].
- Pozen, D. E. (2013, December 20). The leaky leviathan: Why the government condemns and condones unlawful disclosures of information. *Harvard Law Review* 127(2) , 513-635.
- Predicting violent behavior. (2012, August). Defense Science Board Task Force Report. Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics.
- Prepared statement of Gabriel Schoenfeld. (2010, December 16). ). Hearing before the Committee of the Judiciary, House of Representatives, 111 Congress 2<sup>nd</sup> Session. "Espionage Act and the legal and Constitutional issues raised by Wikileaks." Washington, DC: U.S. Government Printing Office.

## REFERENCES

- Pressley, S. A. (1998, September 15). 10 arrested on charges of spying for Cuba; Military facilities targeted, FBI alleges. Washington, DC: *The Washington Post*, p. A01 [Alonso, Gari, Linda Hernandez, Nilo Hernandez, Santos].
- Protecting the force: Lessons from Fort Hood. (2010, January). Report of the DoD independent review. Washington, DC: Department of Defense.
- Raab, S. (1984, November 29). Friend says spy suspect 'hated Communists.' New York, NY: *The New York Times*, p. A2 [Koecher].
- Rafalko, F. J. [Ed.]. (no date). Post-World War II to closing the 20<sup>th</sup> century. A counterintelligence reader, Volume 3. Washington, DC: The National Counterintelligence Executive.
- Rakowsky, J. (1995, October 19). Northborough man charged with espionage. Boston: *The Boston Globe*, p. 41 [Kota].
- Ratcliffe, R. (2015, July 19). Babar Ahmad returns to UK after being sentenced for supporting terror groups. London, UK: *The Guardian*, p. 6 [Abujihaad].
- Recent cases. (2012). Criminal law—economic espionage—ninth circuit upholds first trial conviction under Section 1831 of the Economic Espionage Act of 1996,—*United States v. Chung*, 659 F.3d 815 (9<sup>th</sup> Cir. 2011), *cert denied*, No. 11-1141, 2012 WL 929750 (U.S. Apr, 2012). Boston, MA: *Harvard Law Review*, 125(2177), pp. 2177-2184 [Chung].
- Reilly, T. (2009, November). Economic espionage charges under Title 18 U.S.C. Section 1831: Getting charges approved and the “foreign instrumentality” element. Columbia, SC: *United States Attorneys’ Bulletin*, 57(5), pp. 24-26.
- Reporters Committee for Freedom of the Press. (2015). Emily Peterson, Wikileaks and the Espionage Act of 1917. Retrieved on April 22, 2015 from <http://www.rcfp.org/browse-media-law-resources/news-media-law/wikileaks-and-espionage-act-1917>.
- Reitman, J. (2013, December 19). Snowden and Greenwald: The men who leaked the secrets. New York, NY: *Rolling Stone*, p. 1 [Snowden].
- Robles, F. & Davis, Julie H. (2014, December 18). U.S. frees last of the ‘Cuban Five,’ part of a 1990s spy ring. New York, NY: *The New York Times*, p. A17 [Guerrero].
- Rogers, R. (2008, November 17). Former Marine outlines secret dossiers; Muslims, Arabs not targeted, FBI says. San Diego, CA: *The San Diego Union-Tribune*, p. B-1 [Maziarz].
- Rosenberg, C. (2007a, May 17). Lawyer: U.S. policy shielded list of captives. Miami, FL: *The Miami Herald*, p. 2 [Diaz].

## REFERENCES

- Rosenberg, C. (2007b, May 18). Navy lawyer guilty of spilling secrets. Miami, FL: *The Miami Herald*, p, 4 [Diaz].
- Ross, G. (2011, July). Who watches the watchmen? The conflict between national security and freedom of the press. Washington, DC: *National Intelligence University*.
- Roth, S. (2001, March 5). Spy prosecution is an intelligence high-wire act. San Francisco, CA: *American Lawyer Media: The Recorder*, p. 3.
- Sample, H. A. (2009, November 10). Hearing begins for Maui man accused of being spy. Retrieved on October 5, 2015 from <http://comsecllc.blogspot.com/2009/11/hearing-begins-for-maui-man-accused-of.html> [Gowadia].
- Sanger, D. E. & Peters, J. W. (2013, June 13). A promise of changes for access to secrets. New York NY: *The New York Times*, p. A18.
- Sanger, D. E. & Schmitt, E. (2014, February 8). Snowden used low-cost tool to best N.S.A. New York, NY: *The New York Times*, p. A6 [Snowden].
- Satterfield, J. (2008, August 26). Roth was warned, lawyers allege: U.S. official told professor he was breaking the law. Knoxville, TN: *Knoxville News Sentinel*, p. 2 [Roth].
- Savage, C. & Huetteman, E. (2013, August 21). Manning sentenced to 35 years for leaking government secrets. New York, NY: *The New York Times*, p. A1 [Manning].
- Savage, C. (2013a, July 12). Holder tightens rules on getting reporters' data. New York, NY: *The New York Times*, p. A7.
- Savage, C. (2013b, August 13). Manning played vital role in Iraq despite erratic behavior, supervisor says. New York, NY: *The New York Times*, p. 2 [Manning].
- Savage, C. (2013c, September 23). Former F.B.I. agent pleads guilty in leak to A.P. New York, NY: *The New York Times*, p. A5 [Sachtleben].
- Savage, C. (2014, February 7). Ex-State Department contractor pleads guilty in leak case. New York, NY: *The New York Times*, p. 5 [Kim].
- Savage, C. (2015, May 7). N.S.A. phone data collection is illegal, appeals court rules. New York, NY: *The New York Times*, p. p. 5 [Snowden].
- Savage, C. (2017, January 17). Chelsea Manning to be released early as Obama commutes sentence. New York: *The New York Times*, p. 2 [Manning].
- Schehl, M. L. (2015, February 24). Fort Hood soldier shoots four and himself, police say. Washington, DC: *Army Times*, p. 1.

## REFERENCES

- Schmitt, B. (2009, June 10). Sterling Heights man sentenced after spying for Iraq. Detroit, Michigan: *The Free Press*, p. 2 [Shemami].
- Schneier, B. (2015, March 2). What the future of government surveillance looks like. Washington, DC: *Defense One*. Retrieved on December 15, 2015 from <http://www.defenseone.com/technology/2015/03/what-future-government-surveillance-looks/106425/> .
- 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](http://www.navytimes.com/news/2007/05/navy_guantanamo-trial) [Diaz].
- Secretary of Defense, (2012, October 18). Memorandum: Deterring and preventing unauthorized disclosure of classified information. Washington DC: Author.
- Security from within: Independent review of the Washington Navy Yard shooting. (2013, November). Washington DC: Secretary of Defense Independent Review of the Washington Navy Yard Shooting.
- Semko, R. (2013, March 21). More on Bishop spy case. Retrieved on May 20, 2014 from <http://www.raysemko.com/home/> [Bishop].
- Serrano, R. A. & Reza, H. G. (2008, February 12). Orange County man is accused of being a spy. Los Angeles, CA: *Los Angeles Times*, p. 1 [Chung].
- Serrano, R.A. (2003, March 2). The Falcon and the Fallout. Los Angeles, CA: *Los Angeles Times*, p. D1 [Boyce].
- Shane, S. (2010, December 11). Keeping secrets wikisafe. New York, NY: *The New York Times*, p. WK1.
- Shane, S. (2011a, January 13). Accused soldier in brig as Wikileaks link is sought. New York, NY: *The New York Times*, p. A3 [Manning].
- Shane, S. (2011b, September 6). Leak offers look at efforts by U.S. to spy on Israel. New York, NY: *The New York Times*, p. A12 [Leibowitz].
- Shane, S. (2013a, January 5). Former CIA officer is the first to face prison for a classified leak. New York, NY: *The New York Times*, p. 20 [Kiriakou].
- Shane, S. (2013b, June 21). Ex-contractor is charged in leaks on N.S.A. surveillance. New York, NY: *The New York Times*, p. A4 [Snowden].
- Shanker, T. (2010, July 9). Loophole may have aided theft of classified data. New York, NY: *The New York Times*, p. 10 [Manning].
- Shaw, E. D., Fischer, L. F., & Rose, A. E. (2009, August). Insider threat evaluation and audit. Monterey, CA: Defense Personnel Security Research Center.
- Shaw, E., Payri, M., Cohn, M., & Shaw, I. R. (2013). How often is employee anger an insider risk I? Deterring and measuring negative sentiment versus insider

## REFERENCES

- risk in digital communications. Daytona Beach, FL: *Journal of Digital Forensics, Security and Law*, 8(1): 39-71.
- Shaw, E., & Sellers, L. (2015, June). Applications of the critical-path method to evaluate insider risks. *Studies in Intelligence*, 59(2): 41-48.
- Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., & Flynn, L. (2012, December). Common sense guide to mitigating insider threats 4<sup>th</sup> edition. Pittsburgh, PA: *Software Engineering Institute*, Carnegie Mellon University.
- Simon, S. (1998, January). The Economic Espionage Act of 1996. Berkeley, CA: *Berkeley Technology Law Journal*, 13(1/20), pp. 305-317.
- Smith, J. H. (2010, November 30). Prosecute Wikileaks, then reform our espionage laws. Washington DC: *The Washington Post*, p. 14.
- Southern Poverty Law Center. (2015, February 12). Age of the wolf: A study of the rise of the lone wolf and leaderless resistance terrorism. Montgomery, AL: Author.
- Spiro, P. J. (2008). Beyond citizenship: American identity after globalization. Oxford, UK: *Oxford University Press*.
- Spotlight on the Economic Espionage Act. (2012, March 22). Los Angeles, CA: *Quinn Emanuel Urquhart & Sullivan*, retrieved on August 25, 2015 from <http://www.jdsupra.com/legalnews/spotlight-on-the-economic-espionage-act>.
- Statement of Thomas Blanton. (2010, December 16). Hearing before the Committee of the Judiciary, House of Representatives, 111 Congress 2<sup>nd</sup> Session. "Espionage Act and the legal and Constitutional issues raised by Wikileaks." Washington, DC: U.S. Government Printing Office.
- Steger, M. B. & James, P. (2010). "Ideologies of Globalization," in Paul James and Manfred B. Steger, Eds., *Globalization and Culture: Vol. 4, Ideologies of Globalization*. London, UK: *Sage Publications*.
- Stein, J. (2010, July 8). Past Russian spies have found post-swap life gets a bit sticky. Washington, DC: *The Washington Post*, p. 16 [Koecher].
- Stein, J. S. (2008, April 25). Israel might have many more spies here, officials say. Retrieved April 28, 2008 from [http://www.Cqpolitics.com/frame-templates/print\\_template.html](http://www.Cqpolitics.com/frame-templates/print_template.html) [Kadish].
- Sulick, M. J. (2013). American spies: Espionage against the United States from the Cold War to the present. Washington, DC: *Georgetown University Press*.
- Tate, J. (2013, August 21). Bradley Manning sentenced to 35 years in Wikileaks case. Washington, DC: *The Washington Post*, p. 3 [Manning].

## REFERENCES

- The DoD insider threat program. (2014, September 30). Department of Defense Directive, Number 5205.16. Washington, DC: Department of Defense.
- Theohary, C. A. & Rollins, J. W. (2015, March 27). Cyberwarfare and cyberterrorism: In brief. Washington, DC: *Congressional Research Service*.
- The psychology of espionage. (n.d.). Declassified studies in intelligence article. Retrieved March 11, 2015 from [http://www.foia.cia.gov/sites/default/files/DOC\\_0001407031.pdf](http://www.foia.cia.gov/sites/default/files/DOC_0001407031.pdf)
- Thomas, J. R. (2014, January 15). The role of trade secrets in innovative policy. Washington, DC: *Congressional Research Service*, R41391.
- 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].
- Thompson, G. (2009, June 19). Couple's capital ties said to veil spying for Cuba. New York, NY: *The New York Times*, p. 11. [Myers].
- Thompson, T. J. (2014). Toward an updated understanding of espionage motivation. *International Journal of Intelligence and Counterintelligence*, 27: 58-72.
- Tsukayama, H. (2014, January 19). NSA program defenders question Snowden's motives. Washington, DC: *The Washington Post*, p. 15 [Snowden].
- Uniform Code of Military Justice. (2015). Retrieved on May 27, 2015 from <http://www.ucmj.us/> .
- United States Attorney's Office District of Connecticut. (2007, March 7). Former member of US Navy arrested in Arizona on terrorism and espionage charges. Hartford, CT: District of Connecticut. [Abujihaad].
- United States Attorney's Office District of Hawaii. (2014, March 13). Hawaii man pleads guilty to communicating national defense information to an unauthorized person. Honolulu, HI: United States Department of Justice [Bishop].
- United States Attorney's Office Eastern District of Virginia. (2014, February 10). Former sailor sentenced to 30 years in prison for attempted espionage. Alexandria, VA: Eastern District of Virginia [Hoffman].
- United States Attorney's Office Eastern District of Virginia. (2008, August 8). Press release. New Orleans man sentenced to more than 15 years in prison for espionage involving China. Washington, DC: United States Department of Justice [Kuo].
- United States Court of Appeals for the Ninth Circuit, United States of America, Plaintiff-Appellee v. Dongfan Greg Chung, Defendant-Appellant (2011,

## REFERENCES

- September 26). Petition for rehearing and for rehearing en banc; Opinion on the appeal [Chung].
- United States Department of Commerce. Bureau of Industry and Security. (2015a) Lists of parties of concern: Denied persons list. Retrieved on September 11, 2015 from <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list> .
- United States Department of Commerce. Bureau of Industry and Security. (2015b) Lists of parties of concern: Entity list. Retrieved on September 11, 2015 from <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list> .
- United States Department of Defense. Defense Security Service. (2013). Targeting U.S. technologies: A trend analysis of cleared industry reporting, 2014. Quantico, VA.
- United States Department of Defense. Defense Security Service. Center for Development of Security Excellence. (2015). Job aids/tools: Counterintelligence awareness. Understanding espionage and national security crimes. Retrieved on September 9, 2015 from <http://www.cdse.edu/documents/cdse/ci-jobaidseries-understandingespionage.pdf> .
- United States Department of Justice Southern District of Indiana. (2006, May 26). Central Indiana man sentenced for working with former Iraqi intelligence officers. Indianapolis, IN: United States Attorney. [Shabaan]
- United States Department of Justice, District of Hawaii, Press release. (2011, January 25). Hawaii man sentenced to 32 years in prison for providing Defense information and services to People's Republic of China; Former B-2 bomber engineer helped PRD design stealthy cruise missile. Honolulu, HI [Gowadia].
- United States Department of Justice, Press Release. (2009, April 3). Former member of the U.S. Navy Hassan Abu-Jihaad sentenced to 10 years in federal prison for disclosing classified information. Washington, DC [Abujihaad].
- United States Department of Justice, United States Attorney Charles M. Oberly, III, District of Delaware. (2011, January 13). California man pleads guilty to attempted military exports to Iran. Washington, DC [Knapp].
- United States Department of Justice, United States Attorney Edward H. Kubo, (2006, November 9). Hawaii man indicted for selling national defense secrets to the People's Republic of China. Honolulu, HI [Gowadia].

## REFERENCES

- United States Department of Justice. (1996, November 18). Joint CIA-FBI press release on arrest of Harold James Nicholson. Washington, DC: Office of Public Affairs. [Nicholson]
- United States Department of Justice. (2008, August 1). Press release. New Orleans woman sentenced to prison for aiding and abetting unregistered agent of China. Washington, DC. [Kang]
- United States Department of Justice. (2008, July 11). Press release. Former Defense Department official sentenced to 57 months in prison for espionage violations. Washington, DC. [Bergersen]
- United States Department of Justice. (2008, September 3). Retired University of Tennessee professor convicted of Arms Export Violations. Retrieved March 4, 2009, at <http://www.usdoj.gov/opa/pr> [Roth].
- United States Department of Justice. (2009, January 29). Press release. Imprisoned spy and his son indicted on charges of acting as Russian agents and money laundering. Washington DC. [Nicholson].
- United States Department of Justice. (2009, July 1). Press release. Retired University professor J. Reece Roth sentenced to four years in prison for Arms Export Control Violations involving citizen of China. Retrieved July 1, 2009 at <http://www.justice.gov/opa/pr> [Roth].
- United States Department of Justice. (2009, September 25). Press release. Jury convicts Defense Department official James W. Fondren Jr. of unlawful communication of classified information and making false statements. Washington, DC [Fondron].
- United States Department of Justice. (2010, July 16). Press release. Former State Department Official sentenced to life in prison for nearly 30-year espionage conspiracy. Washington DC: Office of Public Affairs. [Myers].
- United States Department of Justice. (2011, October 12). Virginia man accused of acting as unregistered agent of Syrian government and spying on Syrian protestors in America. Washington, DC: *Justice News*. [Soueid].
- United States Department of Justice. (2012, July 20). Virginia man sentenced to 18 months in prison for acting as unregistered agent for Syrian government. Washington DC: *Justice News*. [Soueid].
- United States Department of Justice. (2015). Criminal Resource Manual at 1123: Introduction to the Economic Espionage Act. Retrieved on January 13, 2015 at <http://www.justice.gov/usam/criminal-resource-manual-1122-introduction-economic-espionage-act> .
- United States Department of Justice. (2015). Criminal Resource Manual at 2057: Synopses of key national defense and national security provisions. Retrieved

## REFERENCES

- on April 17, 2015 at <http://www.justice.gov/usam/criminal-resource-manual-2057-synopses-key-national-defense-and-national-security-provisions> .
- United States Department of Justice. (2015). Offices of the United States Attorneys. Priority Area: National Security. Counterespionage/ Counter Proliferation Efforts. Retrieved April 23, 2015 at <http://www.justice.gov/usao/priority-areas/national-security/counter-espionage-counter-proliferation-efforts>
- United States Department of Justice District of Hawaii, Press release. (2010, August 9). Noshir Gowadia convicted of providing Defense information and services to People's Republic of China. Washington, DC [Gowadia].
- United States Department of Justice. Federal Bureau of Investigation. (2008, September 19). Redacted Affidavit in support of a criminal complaint and arrest warrant for Shu Quan-sheng. Washington, DC [Shu].
- United States Department of Justice. Federal Bureau of Investigation. National Security Branch. (2015). Counterproliferation overview. Retrieved on September 19, 2015 from <https://www.fbi.gov/about-us/nsb/nsb-brochure> and from <https://www.fbi.gov/about-us/nsb/counterproliferation-overview>
- United States Department of Justice. The Eastern District of Virginia. (2008, September 24). Press release. Virginia Physicist arrested for illegally exporting space launch data to China and offering bribes to Chinese officials. Newport News, VA [Shu].
- United States Department of State. (2015). A resource on strategic trade management and export controls. Red flags and watch lists: U.S. Embargo reference chart. Retrieved on September 11, 2015 from <http://www.state.gov/strategictrade/redflags/>
- United States Department of State. (2015). State sponsors of terrorism. Retrieved on August 17, 2015 at <http://www.state.gov/j/ct/index.htm> .
- United States Department of State. Directorate of Defense Trade Controls (2015a). Getting started. Retrieved on September 16, 2015 from [https://www.pmdtc.state.gov/documents/ddtc\\_getting\\_started.pdf](https://www.pmdtc.state.gov/documents/ddtc_getting_started.pdf).
- United States Department of State. Directorate of Defense Trade Controls. (2015b). United States munitions list. Retrieved September 21, 2015 from [http://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5#se22.1.121\\_11](http://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5#se22.1.121_11) >
- 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 [Diaz].

## REFERENCES

- United States District Court Central District of California Southern Division. (2009, July 16). United States of America v. Dongfan “Greg” Chung, Memorandum of Decision [Chung].
- United States District Court Central District of California. (October 2008). Grand Jury, United States of America, Plaintiff, v. Dongfan “Greg” Chung, Defendant. Indictment [Chung].
- United States District Court Eastern District of Michigan Southern Division. (2007, March 28). Indictment: Najib Shemami.
- United States District Court for the Central District of California (June 2002). Grand Jury, United States of America, Plaintiff, v. John Joungwoong Yai and Susan Youngja Yai, Defendants. Indictment [Yai].
- United States District Court for the District of Columbia. (2004, February 6). United States of America v. Marta Rita Velazquez: Indictment.
- United States District Court for the District of Columbia. (2009, June 4). United States of America v. Walter Kendall Myers and Gwendolyn Steingraber Myers: Indictment.
- United States District Court for the District of Columbia. (2010, May 28). Affidavit in support of application for search warrant. Stephen Jin-Woo Kim.
- United States District Court for the District of Columbia. (2015, April 23). United States of America v. Charles Harvey Eccleston, Indictment. Washington, DC.
- United States District Court for the District of Connecticut. (2007). Warrant for arrest, United States v. Hassan Abujihad a/k/a “Paul R. Hall.” [Abujihad].
- United States District Court for the District of Delaware. (2010, July 20). Criminal complaint: United States of America v. Marc Knapp. Wilmington, Delaware [Knapp].
- United States District Court for the District of Hawaii. (2007, October 25). United States of America vs. Noshir S. Gowadia. Second superseding indictment. Honolulu, HI [Gowadia].
- United States District Court for the Eastern District of Virginia, Alexandria Division. (2001, February 12). United States of America v. Robert Philip Hanssen. Affidavit in support of criminal complaint, arrest warrant and search warrants [Hanssen].
- 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.

## REFERENCES

- United States District Court for the Eastern District of Virginia. (2005). Motions hearing (reduction of sentence). *United States of America v. Lawrence Anthony Franklin*.
- 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 District Court for the Eastern District of Virginia. (2008, February 6) *United States v. Tai Shen Kuo, Gregg William Bergersen, and Yu Xin Kang*: Affidavit in support of criminal complaint, three arrest warrants, and three search warrants.
- United States District Court for the Eastern District of Virginia, Alexandria Division. (2009, June 11). *United States v. Lawrence Anthony Franklin*, Motions hearing: reduction of sentence. Alexandria, VA [Franklin].
- United States District Court for the Eastern District of Virginia, Alexandria Division. (2010, October 22). *United States of America v. Glenn Duffie Shriver*. Statement of Facts. Alexandria, VA [Shriver].
- United States District Court for the Eastern District of Virginia, Alexandria Division. (2010, October 22). *United States of America v. Glenn Duffie Shriver*. Plea Agreement. Alexandria, VA [Shriver].
- United States District Court for the Eastern District of Virginia, Alexandria Division. (2011, October). *United States of America v. Mohamad Anas Haithan Soueid*. Indictment. Alexandria, VA [Soueid].
- United States District Court Southern District of Florida. (2007, February 26). *United States of American vs. Carlos Alvarez and Elsa Alvarez*: United States sentencing memorandum and response to Carlos Alvarez's request for downward departure. [Alvarez].
- United States District Court Southern District of Indiana, Indianapolis Division. (2013, October 21). *United States v. Donald John Sachtleben*. Government's combined sentencing memorandum. Indianapolis, IN [Sachtleben].
- United States Fleet Forces Command. (2006, November 30). Public Affairs Office Media Release: Court martial for sailor begins Dec. 4. Norfolk, VA [Weinmann].
- United States Government Accountability Office. (2015, June). Report to Congressional Committees. *Insider Threats: DOD should strengthen management and guidance to protect classified information and systems*. GAO-15-544. Washington, DC.
- United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence. (2012, June 28).

## REFERENCES

- Hearing: Statement of John P. Woods, Assistant Director, U.S. Immigration and Customs Enforcement, National Security Homeland Security Investigations, regarding a Hearing on “Economic espionage: A foreign intelligence threat to American jobs and homeland security.” Washington, DC.
- United States House of Representatives Committee on the Judiciary. (2008, January 29). Hearing by the Subcommittee on Crime, Terrorism, and Homeland Security: Statement of J. Patrick Rowan concerning “Enforcement of federal espionage laws.” Washington, DC.
- United States House of Representatives Committee on the Judiciary. (1996, September 16). Report on the Economic Espionage Act of 1996. Washington, DC. Report 104-788.
- United States House of Representatives Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet. (2014, June 24). Trade secrets: Promoting and protecting American innovation, competitiveness, and market access in foreign markets. Washington, DC. Report 113-97.
- United States Immigration and Customs Enforcement. (2011, September 12). California man sentenced to nearly 4 years in prison for attempting to export military items to Iran. Retrieved on August 31, 2012 from <http://www.ice.gov/news/releases/1109/110912wilmington.htm> [Knapp].
- United States Immigration and Customs Enforcement. (2015). Counter-Proliferation Investigations Program: Overview and Mission. Retrieved on January 13, 2015 from <http://www.ice.gov/cpi> .
- United States Senate Committee on Governmental Affairs. (1985, April 16 -18 and 25). Hearing by the Permanent Subcommittee on Investigations: Witness statement by Christopher J. Boyce during a Hearing on “Federal government security clearance programs.” Washington, DC [Boyce].
- United States Senate Committee on the Judiciary. (2010, May 12). Testimony of Jeffrey H. Smith during a Hearing on “The espionage statutes: A look back and a look forward.” Washington, DC.
- United States v. Manning, Bradley E., PFC. (2011, December 2). Defense request for article 32 witnesses. Fort Myer, VA: U.S. Army [Manning]. [Despite sections having been blacked out, this list of defense witnesses and the tenor of their potential testimony reveals details of Manning’s Army experience.]
- Van Cleave, M. K. (2013, Fall/Winter). What is counterintelligence? A guide to thinking and teaching about CI. *The Intelligencer*, 20(2). Falls Church, VA: Association of Former Intelligence Officers.
- Venteicher, W. (2013, April 25). Justice Department accuses U.S. citizen of being Cuban spy. Los Angeles, CA: *Los Angeles Times*, p. 3. [Velazquez]

## REFERENCES

- Vise, D. A. (2002). *The bureau and the mole: The unmasking of Robert Philip Hanssen, the most dangerous double agent in FBI history*. New York, NY: *Atlantic Monthly Press*. [Hanssen].
- Viswanatha, A. (2014, October 21). U.S. national security prosecutors shift focus from spies to cyber. New York, NY: *Reuters*. Retrieved on December 10, 2015 from <http://www.reuters.com/article/us-usa-justice-cybersecurity-idUSKCN0IA0BM20141021> .
- Vladeck, S. I. (2010, December 16). Prepared statement of Stephen I. Vladeck. Hearing before the House of Representatives Committee on the Judiciary, “The Espionage Act and the legal and constitutional issues raised by Wikileaks.” Washington, DC.
- Volkman, E. (1994). *Spies: The secret agents who changed the course of history*. New York, NY: *John Wiley & Sons, Inc.*
- Walker, P. (2013, July 30). Bradley Manning trial: what we know from the leaked Wikileaks documents. London, UK: *The Guardian*, retrieved on August 20, 2015 from <https://www.theguardian.com/world/2013/jul/30/bradley-manning-wikileaks-revelations>.
- Warner, J. (2014, May 7). Fact sheet: The women’s leadership gap; Women’s leadership by the numbers. Washington, DC: *Center for American Progress*.
- Weaver, J. (2007, February 27). U.S.: Couple shared vital data with Cuba. Miami, FL: *The Miami Herald*, p. 1 [Alvarez].
- Weaver, J. (2009, October 13). Convicted Cuban spy’s life sentence reduced to 22 years. Miami, FL: *The Miami Herald*, p. 2 [Guerrero].
- Weiser, B. & Risen, J. (1998, December 1). The masking of a militant: A special report.; A soldier’s shadowy trail in U.S. and in the Mideast. New York, NY: *The New York Times*, p. A18 [Mohamed].
- White & Case Technology Newsflash. (2013, January 15). Amendments to the Economic Espionage Act broaden trade secret protection. New York, NY: *White & Case LLP*. Retrieved on August 28, 2015 from <http://www.whitecase.com/publications/article/amendments>
- White House. FOUO. (2014, February 11). Near-term measures to reduce the risk of high-impact unauthorized disclosures. Washington, DC: Government Printing Office.
- White, J. (2006, August 10). Sailor from Oregon charged with espionage. Washington, DC: *The Washington Post*, p. 6 [Weinmann].
- White, J. (2007, March 8). Former sailor accused of providing data to terrorist web site. Washington, DC: *The Washington Post*, p. A8 [Abujihaad].

## REFERENCES

- Whitlock, C. (2005, August 8). Briton used internet as his bully pulpit. Washington, DC: *The Washington Post*, p. A1 [Abujihaad].
- Whitlock, C. & Jaffe, G. (2014, April 4). Argument over paperwork sparked shooting spree, witnesses say. Washington, DC: *The Washington Post*, p. 15 [Lopez].
- Wilentz, S. (2014, January 19). Would you feel differently about Snowden, Greenwald, and Assange if you knew what they really thought? New York, NY: *The New Republic*. Retrieved on January 31, 2014 from <http://www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe> [Snowden].
- Williams, L. & McCormick, E. (2001, November 4). Al Qaeda terrorist worked with FBI/ex-Silicon Valley resident plotted embassy attacks. San Francisco, CA: *The San Francisco Chronicle*, p. 4 [Mohamed].
- Wilshusen, G. C. (2012, June 28). Information security: Cyber threats facilitate ability to commit economic espionage. Testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives. Washington, DC: General Accountability Office.
- Wiltrout, K. (2006, August 29). Navy lawyer once posted at Cuba base is charged. Norfolk, VA: *The Norfolk Virginian-Pilot*, Retrieved on <http://home.hamptonroads.com/stories> [Diaz].
- Wiltrout, K. (2006a, August 12). Accused spy carried cash, secret files, agents say. Norfolk, VA: *Norfolk Virginian-Pilot*, p. 2 [Weinmann].
- Wiltrout, K. (2006b, August 10). Father dismisses “speculation’ on espionage charges against sailor. Norfolk, VA: *Norfolk Virginian-Pilot*, p. 2 [Weinmann].
- Wiltrout, K. (2007, May 19). Naval officer sentenced to six months in prison, discharge. Norfolk VA: *The Norfolk Virginian-Pilot*, p. 3 [Diaz].
- Wise, D. (2012, June 7). Mole-in-training: How China tried to infiltrate the CIA. Washington, DC: *The Washingtonian*, p. 3 [Shriver].
- Wittes, B. (2014, May 29). Thoughts on the Edward Snowden interview. Lawfare: Hard national security choices. Retrieved on June 9, 2014 from <http://www.lawfareblog.com/2014/05/thoughts-on-edward-snowdens-interview/> [Snowden].
- Wood, S. (2001, October). Public opinion of selected national security issues: 1994-2000. Monterey, CA: Defense Personnel Security Research Center.
- Wood, S., Crawford, K. S., Lang, E. L. (2005, May). Reporting of counterintelligence and security indicators by supervisors and coworkers. Monterey, CA: Defense Personnel Security Research Center.

## REFERENCES

- Wood, S. & Marshall-Mies, J. C. (2003, January). Improving supervisor and coworker reporting of information of security concern. 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.
- World Trade Organization. (2008). Trends in Globalization. Retrieved December 10, 2015 from [https://www.wto.org/.../res.../wtr08-2b\\_e.pdf](https://www.wto.org/.../res.../wtr08-2b_e.pdf)
- Youssef, N. A. (2011, January 28). Probe: Army ignored warnings over soldier. Miami, FL: *Miami Herald*, p. 1 [Manning].
- Zimmerman, M. (2014, September 19). Oahu defense contractor sentenced on espionage charges. *Watchdog.org*. Retrieved September 29, 2014 from <http://watchdog.org/171751/espionage-related-charges/> [Bishop].



**APPENDIX A:  
ESPIONAGE AS AN INSIDER THREAT**

**APPENDIX A: ESPIONAGE AS AN INSIDER THREAT**

The essay that follows is the result of a viewpoint exercise, a way of seeing familiar material anew. Typically, in the literature on insider threat, espionage is considered as one example among several threats from insiders. These various insider threats, espionage among them, are usually compared and contrasted in order to tease out commonalities that can then become the basis for observations about insider threat as a phenomenon. Unlike that approach, this exercise started from the viewpoint of espionage and considered how selected studies of insider threat could improve and enlarge on our understanding of espionage. Therefore, the studies included here are not representative of insider threat literature, but instead were included because they offer particular help in explicating espionage itself.

The concept of insider threat has changed significantly since the terrorist attacks of 9/11. The term was being applied during the 1990s to employees and other persons who had insider access to computers and who misused them and the information on them. As computers became standard office equipment and people increasingly stored and accessed sensitive or classified information on them, the threat of information loss or theft, sabotage of information systems, and even cyberespionage by foreign entities became thinkable. Often, early work on insider threat focused on systems security, survivable architectures, auditing and monitoring of system users, and the modeling of likely threats and responses to plan effective countermeasures (Anderson et al., 2000).

The 9/11 attacks changed the understanding of insider threat by demonstrating the global reach and potential attractiveness of transnational terrorist organizations such as Al Qaeda and its offshoots. The nineteen 9/11 hijackers were not Americans, but their example soon attracted adherents, copycats, and wannabes among American citizens. As Americans, more of these in turn attempted or actually performed acts of domestic terrorism. Some domestic terrorism in the United States has been linked to international Islamist extremism, but there are also many American causes that provoke terrorism, such as animal rights, racism, anti-abortion, neo-Nazism, or anarchism. From the initial focus on computer misuse and crimes, the nature of insider threat expanded in the 2000s to include domestic and transnational terrorism, and this threat increased over time. A 2011 study of domestic jihadist terrorism reported that there had been 6 cases in 2002, but year by year, instances grew until in 2010 there were 20 cases. A 2015 study of jihadist and domestic terrorism reported that a foiled or completed terrorist attempt happened every 34 days in the United States (Jenkins, 2011; Southern Poverty Law Center, 2015). As Americans read in the press about dramatic bombings, murders, and arson by domestic terrorists, the potential physical threat from fellow-citizens, though statistically small, became real.

A series of shocks, starting in 2009, amplified concern about threat from Americans with inside accesses, and further expanded the focus of insider threat. Some of the major events included:

## APPENDIX A: ESPIONAGE AS AN INSIDER THREAT

- The Ft. Hood attack by Army psychiatrist Maj. Nidal Hasan, on November 5, 2009. Hasan killed thirteen persons and wounded 43 more by gunfire on a U.S. Army base in Texas (“Protecting the Force,” 2010; Kenber, 2013).
- Wikileaks, an online publisher of purloined information, published thousands of classified reports and documents on the Iraq War and sensitive American diplomacy leaked to it by Bradley, now Chelsea, Manning, starting on February 28 and continuing through July 25, 2010 (Shane, 2011); Secretary of Defense, 2012; Executive Order 13587, 2011).
- Various newspapers published excerpts from thousands of documents detailing classified intelligence programs and NSA surveillance leaked to them by Edward Snowden, an NSA contractor, starting in June 2013, and ongoing in 2015 (Shane, 2013b; Sanger & Schmitt, 2014; Wilentz, 2014; Bamford, 2014).
- Aaron Alexis, an employee of a Department of Defense (DoD) contractor, attacked co-workers at the Washington Navy Yard on September 16, 2013. Alexis fatally shot 12 persons and himself, and wounded 3 additional people (“Internal Review, 2013; Associated Press, 2014; Department of Defense Directive, 2014)
- A second attack at the Ft. Hood Army Base by Army Specialist Ivan Lopez occurred on April 2, 2014. Lopez shot 3 people and then himself, and wounded 16 others (Lamothe, 2014; Whitlock & Jaffe, 2014).<sup>78</sup>

These incidents dramatized additional threats, on top of computer misuse, sabotage, and domestic or international terrorism, including mass shootings in workplaces and schools, the leaking of unheard-of amounts of classified materials, and shootings of military personnel on U.S. military bases. Workplace violence, normally a small but potential threat in any employment setting, was heightened in Nidal Hasan’s case by his self-radicalization to jihadist terrorism. Bradley Manning and Edward Snowden, both of whom were information systems and intelligence insiders with high-level security clearances, transmitted massive amounts of classified information to recipients who they knew intended to publish it to the world. Aaron Alexis passed repeated background investigations to maintain his security clearance and consulted medical and security personnel about his mental health complaints within a month of taking his guns to his place of employment. Ivan Lopez struggled as a soldier, lied and deceived his officers and friends, and reacted to a series of personal losses and frustrations by suddenly starting to shoot his fellow soldiers. The blows to trust in systems of vetting, monitoring, and managing one’s fellow workers and citizens, and the loss of faith in technical security systems protecting sensitive information have come quickly through these incidents, and they have created new categories of insider threat.

---

<sup>78</sup> As of April 1, 2015, there have been two additional shootings by soldiers at Fort Hood in 2015, both murder-suicides; one killed four people and wounded one, the other killed two people (Schehl, 2015).

Reactions to these developments have been wide-ranging, and they are continuing. The federal government extensively studied the attacks at federal facilities and the loss of classified materials (for example, “Protecting the Force, 2010; “Predicting Violent Behavior, 2012; “Internal Review,” 2013).

Based on those studies, the government has issued a series of new policies addressing insider threat. It has set up task forces and new agency groups charged with mitigating threats in comprehensive ways. It has mandated that all federal agencies and the military services take steps to reduce the likelihood, to detect, and to respond to such threats (Executive Order 13587, 2011; “Countering Espionage,” 2012; “Congressional Notification, 2013; Department of Defense Directive, 2014; Monaco, 2014; “ Management of Serious Security Incidents,” 2014; “Predicting Violent Behavior, 2012). Whole new fields of academic study and analysis, consulting services, and conference circuits have grown up around problems of and solutions to insider threat. It is impossible now to think about workplace violence, fraud, domestic or jihadist terrorism, leaking of controlled information, sabotage, and computer misuse and systems hacking without conceiving of it as insider threat.

Since early in this evolving concept of insider threat, espionage by Americans has been included in the list of such threats. For decades, people who betrayed their privileged access to classified or sensitive information by selling or giving it to other nations or causes have been described as examples of betrayal by insiders, although less often by the term “insider threat” until recently, so including spies among these categories was to be expected.

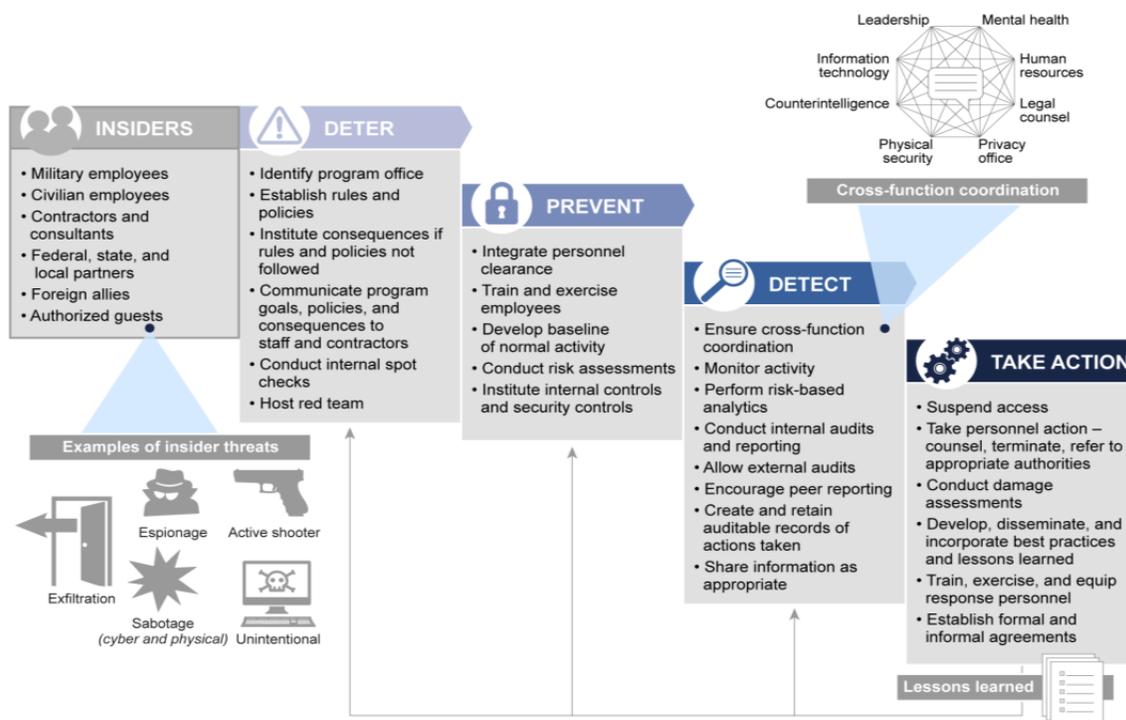
In some ways, the study of espionage is not much advanced by this appropriation into the universe of insider threat. In order to frame analytical categories that fit each of the various phenomena included in an insider threat study—and there is no consistent definition from study to study of which concerns should be included—inevitably these analytical categories become general and somewhat abstract. The categories do raise awareness of the dimensions found across the range of insider actions, and they do allow one to compare and contrast various insider threats. They can be applied to the particulars of espionage, but they can also be applied to the particulars of any of the other crimes or mischief that people with access to organizations and information systems can commit. Many findings of current insider threat studies are at such a level of abstraction and generalization that they do not really advance an understanding of espionage itself, or they are obvious and predictable.

For example, the GAO’s 2015 report to the House of Representatives Armed Service Committee on DoD insider threat programs assessed these programs using a broad definition of insider threat, because that is how the programs themselves approach the issue. Figure 7 reproduces one of the GAO’s figures from its report. It is not shown here because it is deficient but because it is typical. It is a summary of the populations that might be insider threats; the steps taken by successful programs

## APPENDIX A: ESPIONAGE AS AN INSIDER THREAT

against insider threats, including deterrence, prevention, detection, and taking action; examples of types of insider threats; and authorities that should be coordinated. Espionage is one of the threats. The others that are included here are exfiltration, sabotage (cyber and physical), unintentional, and active shooter. To encompass the breadth of these selected types of threat, ranging from an employee sitting at his or her desk carelessly attaching a classified document to an email to an active shooter who is stalking the hallways, the categories are necessarily open-ended and generalizable (United States Government Accountability Office, 2015). Were one trying to learn how best to respond to the threat of espionage, one would do better to consult the literature on espionage itself than insider threat studies at these higher levels of abstraction.

### GAO's Framework of Key Elements To Incorporate at Each Phase of DOD's Insider-Threat Programs



Source: GAO analysis of Department of Defense (DOD), U.S. government, and private-sector guidance and reports. | GAO-15-544

**Figure A-1 The Government Accountability Office's Summary of Key Elements in Insider Threat Programs**

In some ways, however, studies of insider threat do offer valuable insights that can be applied specifically to espionage. Contributions from several areas of insider threat research that are helpful for understanding and responding to espionage are considered here: (1) personal crises that provoke acts of espionage; (2) indicators of insider threat as a means of recognizing impending adverse acts; and (3) analyzing organizational culture.

## Personal Crises and Triggers

The data on which this report is based include variables coded for personal crises and for triggers of espionage. Although there are much data not reported for these variables, what is available suggests some typical issues and themes. A consideration of these data for espionage-related offenses will be followed by a look at how insider threat studies expand the categories.

Descriptions of how people begin to commit an espionage-related offense usually point to preconditions that are common for most crimes: motive, opportunity, lack of countervailing internal or external constraints, means, and often, a trigger—that is, something that happens to propel the person into acting on the intention (Herbig, 1994). Thompson provides insight into this notion of a trigger. He writes:

A trigger is an event, usually negative, which serves as the “straw that breaks the camel’s back” and pushes the spy over the edge to espionage. The prospective spy tends to struggle with a crisis for a period of time, during which tension builds up and pushes him/her toward the act.

Then something in the near term triggers the act of espionage that the person has thought about and resisted for some time—it now becomes the solution to the immediate problem. “A trigger merely taps into an existing cauldron of tension and spurs action,” Thompson describes. An apt example is a person in the middle of a divorce, facing the financial and emotional upheavals divorce brings, until just one more lawyer’s bill arrives in the mail, and the bill serves as a trigger. Suddenly the person who was holding on cannot cope any more, and puts the espionage plan in motion (Thompson, 2014).

Many instances of espionage support the notion of a two-stage buildup to an act of espionage: first, a personal problem develops over some months into an impending crisis that becomes the context for planning an act of espionage; and second, some event serves as the final straw that precipitates the person to try to solve the problem by beginning espionage, which has come to seem the only course left. Table A-1 reports on personal crises and more immediate trigger events from the data collected by PERSEREC.

**Table A-1**  
**Precipitating Personal Crises and Triggers as Contextual Factors in 209**  
**Espionage-related Offenders**

<b>Characteristics</b>	<b>n<sup>79</sup></b>	<b>% of 209 individuals</b>
<b>Precipitating triggers that seem to have caused the beginning of espionage</b>		
Separation or divorce from significant other	5	2
Immediate financial crisis	16	8
Facing a threat to self or family	2	1
Conflict (interpersonal or job-related)	16	8
<b>Contextual personal problems or evolving crises within 6 months before date of beginning espionage</b>		
<b>Before beginning espionage</b>		
Separation or divorce from significant other (includes the 5 above for whom this was a trigger)	19	9
Death of family member or close friend	7	3
Diagnosis of terminal illness	5	2
Physical separation from significant other	8	4
Marital problems	20	10
New engagement or marriage	11	5
New significant other	10	5
Began extramarital affair	20	10
Physically relocated	13	6
Reported to have shown financial irresponsibility	22	11
Reported to be having trouble with debt	68	33
Reported to have wanted money, been greedy	36	17
Reported to have shown radically different behavior (from his or her norm) prior to espionage only	7	3
<b>During espionage</b>		
Reported to have shown radically different behavior (from his or her norm) prior to and during espionage	9	4
Reported to have shown radically different behavior (from his or her norm) during espionage only	13	6

<sup>79</sup> A person may have more than one entry.

<b>Characteristics</b>	<b>n<sup>79</sup></b>	<b>% of 209 individuals</b>
Reported to have shown unexplained affluence during espionage	44	21
Spending beyond means was reported by others	23	11
Bought a new house	1	>1
Bought a new vehicle	2	>1
Spending reported and a new house	5	2
Spending reported and a new vehicle	8	4
Spending reported, a new house, + a new vehicle	5	2

The preferred research method to explore nuances of timing and motive in an individual’s decision to take an irrevocable action, such as beginning to commit espionage, would be to interview the person and ask questions from a validated protocol to be used with each subject. The sources available that went into making Appendix Table 1 were not interviews with espionage-related offenders, but instead, were in large part open source print materials written after the events. What is lost by using these materials—deeper insights into each person’s issues—may be gained in breadth of coverage across 209 instances and 7 decades.

Not surprisingly, the themes cluster on basic human issues that can become crises in a person’s life: marriage and family, making a home, procuring a livelihood, advancing a career, interacting with co-workers and bosses in a workplace, maintaining financial stability, and ensuring physical health are common issues.

In addition, six of the variables in Appendix Table 1 rely on the reports of other people, despite the known fact that people resist making such reports (Wood & Marshall-Mies, 2003). The person seemed financially irresponsible, was struggling with debt, was noticeably greedy, was acting very differently than normal just before espionage began, was acting very differently during espionage, or showed unexplained affluence during espionage. The first four of these reinforce the finding that money, the need for it and the desire for it, is the predominant motive for espionage-related offenses among Americans. The variables here that involve money are the highest numbers among these incomplete data, including 11% of the 209 cases who demonstrated financial irresponsibility, 33% who struggled with debt, 17% who seemed greedy to their coworkers or friends, and 21% who displayed unexplained affluence while spying.

Typically, insider threat studies that generalize from a variety of crimes report personal crises and triggers drawn from cases. Findings from studies with a broader insider threat focus alert students of espionage to additional factors and patterns they should try to apply specifically to espionage to see if they fit. Since there are thousands of relevant studies—typing the phrase “scholarly articles insider threat” into the Google search engine, for example, returns 37,600 entries in

## APPENDIX A: ESPIONAGE AS AN INSIDER THREAT

early April 2015—for the sake of keeping this report focused on espionage, this discussion only describes a few of the relevant insider threat studies.

An Insider Threat team at the Software Engineering Institute (SEI) at Carnegie Mellon University has published a series of studies looking at insider threat through different lenses, often applying modeling techniques. The 2006 study that compares Information Technology (IT) sabotage with espionage illustrates their approach (Band, et al, 2006). Using cases from sabotage and from espionage by Americans, their comparison yielded six observations common to both types of insider threat:

Observation #1: Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.

Observation #2: In most cases, stressful events, including organizational sanctions, contributed to the likelihood of insider IT sabotage and espionage.

Observation #3: Concerning behaviors were often observable before and during insider IT sabotage and espionage.

Observation #4: Technical actions by many insiders could have alerted the organization to planned or ongoing malicious acts.

Observation #5: In many cases, organizations ignored or failed to detect rule violations.

Observation #6: Lack of physical and electronic access controls facilitated both insider IT sabotage and espionage (Band, et al, 2006).

It is Observation #2 on “stressful events” that most directly relates to the personal crises and triggers under discussion here. Band and his colleagues analyze some of the tensions in workplaces that can escalate into crises that provoke people to commit sabotage or espionage. They provide a useful discussion of the interactions between the “personal predispositions” in the first bullet with the “stressful events” of the second. The study defines personal predispositions as “relating directly to maladaptive reactions to stress, financial and personal needs leading to personal conflicts and rule violations, chronic disgruntlement, strong reactions to organizational sanctions, concealment of rule violations, and a propensity for escalation during work-related conflicts.” These interact with “stressful events,” which are not experienced in the same way by everyone: the researchers note that “what insiders perceived as stressful, how they contributed to the occurrence of stress, and how they reacted to stress were viewed as influenced directly by personal predispositions” (Band et al, 2006).

Shaw and colleagues applied some of the insights from the SEI research to a particular insider threat issue: recognizing anger in employees and evaluating that anger as a potential insider threat (Shaw, et al, 2013). Their study reported on the development of two observational scales, one for measuring levels of negative

sentiment and the other for measuring insider risk, which they applied to archived emails in order to perform sentiment analysis. While the results of their sentiment analysis are useful, they are not especially relevant to this discussion, but the components of their “Scale of Insider Risk in Digital Communication” helps to extend the categories of personal crises and triggers that may be applicable to espionage. The seven components in their scale are:

- *Process*: variables that indicate the extent to which subject behavior that could be directly associated with, or contribute to, the accomplishment of insider actions is present [or] increasing (i.e., preparations, rehearsals, [acquisition of weapons] etc.);
- *Psychological State*: variables that indicate the extent that subject attitudes, beliefs, and feelings are consistent with individuals who have committed insider acts;
- *Personal Predisposition*: variables that indicate the extent to which the subject’s observed history, experiences, personal characteristics, and contacts mirror those of previous insider subjects;
- *Personal Stressors*: variables defined as changes in personal or social responsibilities or conditions requiring significant energy for adaptation and do not involve direct workplace or financial issues;
- *Professional Stressors*: variables that include changes in professional, school, and/or work conditions or responsibilities that require significant energy for adaptation, exclusive of financial and personal implications;
- *Concerning Behaviors*: include variables such as violations of workplace or other rules, traditions, laws, policies, or procedures that indicate the extent to which the subject has had difficulty controlling his behavior consistent with expectations, in a manner similar to other insiders; and
- *Mitigating factors*: variables indicating that the subject’s level of insider risk may be modified by personal or other characteristics that reduce the level of risk (Shaw, et al, 2013).

Shaw argued that individuals contemplating an insider crime may follow a “critical pathway” that can be described in general terms to apply to variety of crimes. In this conception, one or more of the personal “stressors,” such as “death of a family member, marriage, divorce, births, [or] moves” could become the personal crisis that might move the person along the critical pathway toward espionage or other types of insider actions. The professional “stressors” here include “graduation, attending a new institution or taking a new job, demotion, termination, promotion, transfer, retirement, consulting jobs, [or] taking side jobs” (Shaw, et al, 2006). Note

that stressors can be positive as well as negative conditions that may temporarily de-center a person.<sup>80</sup>

### Indicators of Insider Threat

From the recent dramatic and usually violent instances of insider threat—bombings, mass shootings, leaks of large collections of classified information—has come an urgency to identify and interrupt these threats. This has caused the field of insider threat studies to focus on ways to recognize and interrupt such events by studying “indicators” in the life and behavior of an insider. These may be general attributes, such as having relatives in a foreign country, or more specific “behavioral indicators,” which another person (co-workers, supervisors, or family members) would be able to notice in the behavior of the individual. Many insider threat studies provide lists of indicators, usually drawn from cases and described in generalized terms so that they apply to various insider threats. Two examples among the many hundreds available are noted here. In 2008, a study by PERSEREC titled “Potential Counterintelligence Risk Indicators” presented indicators from a counterintelligence officer’s perspective. These include 1) indicators that a person may be an attractive target for recruitment by a foreign intelligence service, 2) indicators that a person may be susceptible to espionage or terrorism, and 3) indicators that a person may actually be engaging in espionage, terrorism, or subversive activity (Heuer, Jr., 2008).

A second example dates from 2010. In response to the recent series of incidents described as insider threats, the U.S. Army revised and reissued its Army Regulation 381-12 as the *Military Intelligence: Threat Awareness and Reporting Program*, or TARP. The regulation includes lists of indicators of espionage, potential international terrorism, and extremist activity that may pose a threat to DoD or U.S. military operations. These are framed in behavioral terms and assume that an observer will report them. For example, espionage indicators include “Unreported contact with foreign government officials outside the scope of one’s official duties,” “attempts to obtain information for which the person has no authorized access or need to know,” and “unexplained or undue affluence without logical income source.” Examples of indicators of terrorism-related insider threats in the TARP regulation include “advocating support for terrorist organizations or objectives,” or “purchasing bomb-making materials.” Among the indicators listed as potential extremist activity is “expressing a political, religious, or ideological obligation to engage in unlawful violence directed against U.S. military operations or foreign policy” (Department of the Army, 2010).

---

<sup>80</sup> Eric Shaw and Laura Sellers further develop the implications for insider threat of a critical path of actions in their article “Applications of the Critical-Path Method to Evaluate Insider Risks,” *Studies in Intelligence*, 59(2), June 2015. Espionage examples are considered, along with incidents of workplace violence and leaks of classified information.

Providing these lists of indicators presupposes that someone who observes these behaviors will recognize them as indicators and then report them to a supervisor, security officer, or counterintelligence agent. Yet there is a general resistance in American culture to reporting the potential misbehavior of others to an authority, reflecting the feeling that this would be “turning them in.” PERSEREC sponsored research about national security in a national public opinion poll in 1994 and reported that

The public was asked...about what people should do if they saw a person violating security rules. Would they be loyal to their employer—the government—or to their coworker? Respondents were evenly split between those who would immediately report the violation and those who would try to intervene, before reporting, by advising the person to stop the behavior. In other words, they would give the person a chance to change his/her behavior. This is significant, given the fact that cleared individuals are required by regulation to report to authorities any behavior observed among colleagues that may be of security relevance. Presently, the rate of such reporting is extremely low.

A 2003 PERSEREC technical report documented research that followed up on the issue of reporting security violations or behavioral indicators. It found this resistance and discussed the explanations people gave for the low rate of reporting by co-workers and supervisors (Wood & Marshall-Mies, 2003). One claim by people in focus groups stood out: if they recognized that what the person was doing was a serious threat and it was clearly related to security, they would overcome their reluctance and go ahead and report it.

This finding led to a second PERSEREC study in 2005, which researched available official lists of indicators that observers were directed to report, and from them in focus groups framed a core list of the most serious reportable behaviors (Wood, Crawford, & Lang, 2005). An example of a reportable indicator of recruitment by a foreign intelligence service, for example, would be “you become aware of a colleague having contact with an individual who is known to be, or suspected of being, associated with a foreign intelligence, security, or terrorist organization.” A behavior indicating information collection would be “you find out that a colleague has been keeping classified material at home or may other unauthorized location.” Such behaviors demonstrate a clearer nexus with security violations than personal behaviors such as alcoholism, absenteeism, or marital problems, and focus groups assured the researchers they could understand the reason to report these security concerns and would do so (Wood, Crawford, & Lang, 2005).

The researching and compiling of lists of insider threat indicators offers students of espionage a shorthand source for re-thinking and possibly expanding the usual espionage indicators to include more that reflect information technology, domestic or international terrorism mixed with espionage, and the other evolving species of insider threats.

### Analyzing Organizational Culture

In addition to a broader exploration of the role of personal crises and triggers as precursors to beginning espionage as one of many insider threats, and an exhaustive compilation of indicators, a third contribution from insider threat research to better understanding espionage is its focus on organizations. Insiders, by definition, work and operate inside organizations or institutions. Threats such as workplace violence, fraud, sabotage of IT systems, or the theft of proprietary data from IT storage and systems take place in organizations. Analyzing how organizational structures and cultures encourage or inhibit insider threats has been a major focus and contribution of the research.

A PERSEREC technical report from 2009 published an audit tool with which organizations could evaluate their risk of insider threats and take action to reduce those risks. It described the contextual elements of organizations that may magnify the incidence of malicious insider actions, including economic and social pressures, sector-specific forces such as technological change, and disruptive forces such as increased competition or declining resources (Shaw, Fischer, & Rose, 2009). It then pulled together research literature on the most effective approaches organizations can take to frame their policies, such as employee screening, or monitoring IT systems, critical users, and staff, and termination procedures. The report discusses seventeen policy issues that carry potential insider threat risk. It provides research findings and approaches to improve organizational actions, including recruitment of employees or contractors, reemployment screening, training, education, program effectiveness, continuing evaluation, and management interventions such as demotion or termination. Evidence suggests that when an insider leaves an organization, especially if it is a forced leave-taking, but even when it is voluntary, the person often chooses that time to damage, steal, undermine, or otherwise act against an organization, so firings and retirements are identified as critical security milestones (Shaw, Fischer, & Rose, 2009).

SEI has published a series of similar studies focused on various insider threats to organizations and how organizations should more effectively respond. Their *Common Sense Guide to Mitigating Insider Threats 4<sup>th</sup> edition* focuses on threats of intellectual property theft, IT sabotage, and fraud. The report advances nineteen best practices based on case studies, and it divides its advice by the part of the organization most responsible for the issue, including human resources, legal, physical security, data owners, information technology (and information assurance), and software engineering (Silowash, et al, 2012). Although espionage itself is not discussed in this report, an example relevant to espionage is Practice 8: “Enforce separation of duties and least privileges,” which encourages organizations to divide functions between employees and encourage cooperation among them on tasks to minimize solo misuse or abuse of access to systems. Reading case studies on insider crimes like these, which are related to but not actually espionage, and applying the suggestions for responding to other insider threats to espionage

examples is a useful mind-expanding exercise that encourages fresh ideas and insights (Silowash, et al, 2012).

Students of espionage could benefit from systematically analyzing the organizational context in which acts of espionage have occurred. This is not a typical approach in the field because data on the organizations in which espionage-related offenders operated is usually sparse, if not missing entirely. Those who investigate such crimes, usually law enforcement or counterintelligence officials, would like to collect evidence beyond what is relevant for prosecuting the offender from co-workers, supervisors, and organizational policy documentation. Sometimes such evidence is available, sometimes not. Studies that include this focus are especially valuable, since having insight into how an organization may have nurtured or hindered a spy, and how it responded to espionage as it was carried out in its offices and hallways, is important for framing effective countermeasures.

A final example presented here—among the many that are available—of insider threat research that contributes to organizational analysis is an article published in 2014 titled *A Worst Practices Guide to Insider Threat: Lessons from Past Mistakes* (Bunn & Sagan, 2014). The focus in this article is on nuclear facilities, and its intended audience is nuclear security managers, but it draws examples and cases not only from nuclear accidents and security incidents, but from the experiences of intelligence agencies, the military, bodyguards of political figures, banking and finance, gambling, and the pharmaceutical industry. This results in a lively discussion that can usefully be applied to espionage cases as well as common glitches in organizations where espionage occurs.

One example of a “worst practice” is Lesson #1: “Don’t Assume that Serious Insider Problems are NIMO (Not In My Organization).” The authors point out that some businesses, such as diamond mining or gambling, just assume their employees are thieves and act accordingly toward them, but many other organizations consider their employees to be part of a carefully screened elite, and such organizations emphasize loyalty and staff morale to encourage the devotion and commitment they need from them. The authors suggest intelligence agencies and nuclear organizations usually fall into this category, with their highly educated and trained staffs. The stress on loyalty, and comparing “our” loyalty favorably to other organizations with presumably less staff loyalty, can lead managers “to falsely assume that insider threats may exist in other institutions, but not in their organizations” (Bunn & Sagan, 2014). The counter example given is of the assassination of President Indira Gandhi in 1984 by the very Sikh bodyguards she most trusted and had insisted should be the only ones to guard her.

A second example that would apply as well to numerous instances of espionage is Lesson #8: “Don’t Assume that Security Rules are Followed.” This section points out that security procedures and personnel screening policies are often in tension with other goals of an organization, such as maintaining production, meeting deadlines, or generating collegial relationships among employees. Sometimes this

## **APPENDIX A: ESPIONAGE AS AN INSIDER THREAT**

tension results in a bending or breaking of a security rule in the name of a higher goal. Often this would be done by employees, but sometimes even managers do so. The management practice of resting on the unexamined assumption that employees are in fact following the existing rules can be dangerous, as the examples of security guards at nuclear facilities asleep at their desks or propping open the doors illustrate. Advice to think about what are an organization's incentives for its employees and then aligning them to elicit good security practices, rather than eliciting the evasion of security rules, applies equally well to organizations in which espionage takes place (Bunn & Sagan, 2014).

**APPENDIX B:**  
**LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED  
CHARACTERISTICS**



**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

**Table B-1  
List of the 209 Individuals in this Study and Selected Characteristics**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
Abouelaila	Gladys Ferris	Civilian	67/00/00	69/00/00	V	<b>Egypt</b>
Abujihaad	Hassan	Navy	01/07/19	07/03/07	V	<b>Al Qaeda</b>
Ali	Amen Ahmed	Civilian	87/00/00	06/09/07	V	<b>Yemen</b>
Allen	Michael Hahn	Civilian	86/00/00	86/12/04	V	<b>Philippines</b>
Alonso	Alejandro M.	Civilian	94/00/00	98/09/10	V	<b>Cuba</b>
Alvarez	Carlos	Civilian	77/00/00	06/01/09	R	<b>Cuba</b>
Alvarez	Elsa	Civilian	82/00/00	06/01/09	R	<b>Cuba</b>
Ames	Aldrich Hazen	Civilian	85/04/00	94/02/21	V	<b>Soviet Union</b>
Ames	Maria del Rosario	Civilian	92/00/00	94/02/21	R	<b>Soviet Union</b>
Anderson	Ryan Gilbert	Army	04/01/00	04/02/12	V	Al Qaeda
Anzalone	Charles Lee Francis	Marines	90/11/00	91/02/13	V	Soviet Union
Aragoncillo	Leandro	Marines	00/08/00	05/09/10	R	<b>Philippines</b>
Baba	Stephen Anthony	Navy	81/09/01	81/10/09	V	South Africa
Barnett	David Henry	Civilian	76/10/00	80/03/18	V	<b>Soviet Union</b>
Baynes	Virginia Jean	Civilian	90/00/00	92/00/00	R	<b>Philippines</b>
Bell	William Holden	Civilian	78/10/00	81/06/24	R	<b>Poland</b>
Bergersen	Gregg William	Civilian	07/03/00	08/02/11	R	<b>China</b>
Bishop	Benjamin Pierce	Civilian	12/15/14	13/03/15	V	<b>China</b>
Boeckenhaupt	Herbert William	Air Force	65/06/00	66/10/24	V	<b>Soviet Union</b>
Boone	David Sheldon	Army	88/00/00	98/10/10	V	<b>Soviet Union</b>
Borger	Harold Noah	Civilian	59/10/00	61/03/03	R	<b>East Germany</b>
Boyce	Christopher John	Civilian	75/05/10	77/01/16	V	<b>Soviet Union</b>
Brandon	Charles Frederick	Air Force	77/10/00	78/00/00	V	<b>Soviet Union</b>
Brown	Joseph Garfield	Civilian	90/00/00	92/12/27	R	<b>Philippines</b>
Brown	Russell Paul	Navy	89/04/00	89/07/25	V	Soviet Union

<sup>81</sup> The field “Date Began” refers to when the individual began espionage activity. It is expressed as year, month, and lastly day. If only the year is known, the month and day are given as zeros. “Date of Arrest” follows the same date order.

<sup>82</sup> Actual transmission of information to the recipient is noted by bolding the name of the recipient; non-bolded recipients were attempts that did not transmit information.

**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
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	<b>Soviet Union</b>
Carney	Jeffrey Martin	Air Force	83/04/00	91/04/22	V	<b>East Germany</b>
Cascio	Guiseppe	Air Force	52/00/00	52/09/21	V	<b>North Korea</b>
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	<b>China</b>
Chiu	Rebecca Laiwah	Civilian	83/00/00	05/10/28	R	<b>China</b>
Chung	Dongfan	Civilian	79/00/00	06/09/11	R	<b>China</b>
Clark	James	Civilian	76/00/00	97/10/04	R	<b>East Germany</b>
Conrad	Clyde Lee	Army	74/00/00	88/08/23	R	<b>Hungary, Czecho-slovakia</b>
Cooke	Christopher Michael	Air Force	80/12/23	81/05/05	V	<b>Soviet Union</b>
Cordrey	Robert Ernest	Marines	84/04/12	84/05/16	V	Soviet Union
Davies	Allen John	Civilian	86/09/22	86/10/27	V	Soviet Union
DeChamplain	Raymond George	Air Force	71/06/05	71/07/02	R	<b>Soviet Union</b>
Dedeyan	Sahag Katcher	Civilian	73/03/00	75/06/27	R	<b>Soviet Union</b>
Diaz	Matthew	Navy	05/01/15	07/01/08	V	<b>United States</b>
Dolce	Thomas Joseph	Civilian	79/00/00	88/04/16	V	<b>South Africa</b>
Drummond	Nelson Cornelious	Navy	58/00/00	62/09/28	R	<b>Soviet Union</b>
Dubberstein	Waldo Herman	Civilian	77/00/00	79/00/00	R	<b>Libya</b>
Dunlap	Jack Edward	Army	60/06/00	63/00/00	V	<b>Soviet Union</b>
Ellis	Robert Wade	Navy	83/02/09	83/02/09	V	Soviet Union
Faget	Mariano	Civilian	98/12/12	00/02/17	R	<b>Cuba</b>
Fondren, Jr.	James Wilbur	Civilian	04/11/00	09/05/13	R	<b>China</b>
Ford, Jr.	Kenneth W.	Civilian	04/01/00	04/01/12	V	unknown
Franklin	Lawrence Anthony	Civilian	03/06/26	05/05/04	V	<b>Israel</b>
French	George Holmes	Air Force	57/04/05	57/04/06	V	Soviet Union
Garcia	Wilfredo	Navy	85/00/00	87/00/00	R	<b>Philippines</b>
Gari	George	Civilian	91/00/00	01/08/31	R	<b>Cuba</b>
Gessner	George John	Army	60/12/07	61/01/00	V	<b>Soviet Union</b>

**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
Gilbert	Otto Attila	Civilian	82/04/17	82/04/17	R	Hungary
Gowadia	Noshir	Civilian	99/12/12	05/10/25	V	<b>China, Israel, Germany, Switzerland, Austria, Lichtenstein, 2 others</b>
Graf	Ronald Dean	Navy	89/00/00	89/03/03	V	unknown
Gregory	Jeffrey Eugene	Army	84/03/00	93/04/29	R	<b>Hungary, Czecho-slovakia</b>
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, III	James William	Army	82/12/00	88/12/21	V	<b>East Germany, Soviet Union</b>
Hamilton	Frederick Christopher	Civilian	91/02/00	92/00/00	V	<b>Ecuador</b>
Hamilton	Victor Norris	Civilian	62/00/00	63/00/00	V	<b>Soviet Union</b>
Hanssen	Robert Philip	Civilian	79/00/00	01/02/18	V	<b>Soviet Union</b>
Harper, Jr.	James Durward	Civilian	75/00/00	83/10/15	R	<b>Poland</b>
Harris	Ulysses Leonard	Army	67/02/08	67/08/25	V	<b>Soviet Union</b>
Hawkins	Stephen Dwayne	Navy	85/00/00	85/08/07	V	unknown
Helmich, Jr.	Joseph George	Army	63/00/00	81/07/15	V	<b>Soviet Union</b>
Hernandez	Linda	Civilian	94/00/00	98/09/10	R	<b>Cuba</b>
Hernandez	Nilo	Civilian	92/00/00	98/09/12	R	<b>Cuba</b>
Hoffman, II	Robert Patrick	Civilian	12/10/21	12/12/06	R	Russia
Hoffman	Ronald Joshua	Civilian	86/09/09	90/06/15	V	<b>Japan</b>
Horton	Brian Patrick	Navy	82/06/00	82/09/30	V	Soviet Union
Howard	Edward Lee	Civilian	84/09/00	85/00/00	V	<b>Soviet Union</b>
Humphrey	Ronald Louis	Civilian	76/00/00	78/01/31	V	<b>Vietnam</b>
Inson	Seivirak	Army	09/00/00	12/06/00	V	<b>Cambodia</b>
Irene	Dale Vern	Civilian	84/08/12	84/08/23	R	Soviet Union

**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
Jeffries	Randy Miles	Civilian	85/12/14	85/12/20	V	<b>Soviet Union</b>
Jenott	Eric O.	Army	96/00/00	96/06/26	V	<b>China</b>
Johnson	Robert Lee	Army	53/02/00	65/04/05	V	<b>Soviet Union</b>
Jones	Geneva	Civilian	91/00/00	93/08/03	V	<b>Liberia</b>
Kadish	Ben-Ami	Civilian	79/06/05	08/04/22	R	<b>Israel</b>
Kampiles	William Peter	Civilian	78/02/00	78/08/17	V	<b>Soviet Union</b>
Kauffman	Joseph Patrick	Air Force	60/09/00	61/12/00	R	<b>East Germany</b>
Keyser	Donald Willis	Civilian	95/00/00	04/09/15	R	<b>Taiwan</b>
Kim	Robert Chaegon	Civilian	96/04/00	96/09/24	V	<b>South Korea</b>
Kim	Stephen Jin-Woo	Civilian	09/03/00	10/08/27	V	<b>United States</b>
King	Donald Wayne	Navy	89/10/00	80/30/3	V	unknown
Kiriakou	John C.	Civilian	07/12/08	12/01/23	V	<b>United States</b>
Knapp	Marc	Civilian	09/12/24	10/07/20	V	Iran, Russia
Koecher	Karel Frantisek	Civilian	73/02/00	84/11/27	R	<b>Czechoslovakia</b>
Kota	Subrahmanyam	Civilian	85/00/00	95/10/18	R	<b>Soviet Union</b>
Kunkle	Craig Dee	Civilian	88/12/00	89/01/10	V	Soviet Union
Kuo	Tai Shen	Civilian	07/03/00	08/02/11	R	<b>China</b>
Lalas	Steven J.	Army	77/00/00	93/05/03	9	<b>Greece</b>
Latchin	Sami Khoshaba	Civilian	93/00/00	04/08/31	R	<b>Iraq</b>
Ledbetter	Gary Lee	Navy	67/04/00	67/05/00	R	<b>Soviet Union</b>
Lee	Andrew Daulton	Civilian	75/05/18	77/01/17	V	<b>Soviet Union</b>
Lee	Peter H.	Civilian	85/00/00	97/00/00	V	<b>China</b>
Leibowitz	Shemai Kedem	Civilian	09/04/00	09/08/00	V	<b>United States</b>
Lessenthien	Kurt G.	Navy	96/00/00	96/04/22	V	Russia
Leung	Katrina M.	Civilian	90/04/00	03/04/09	R	<b>China</b>
Lipka	Robert Stephan	Army	65/09/00	96/02/23	V	<b>Soviet Union</b>
Lonetree	Clayton John	Marines	86/01/00	86/12/00	R	<b>Soviet Union</b>
Madsen	Lee Eugene	Navy	79/07/26	79/08/14	V	unknown
Mak	Chi	Civilian	83/00/00	05/10/28	R	<b>China</b>
Manning	Bradley E.	Army	09/11/19	10/05/26	V	<b>United States</b>
Martin	Bryan Minkyu	Navy	10/11/15	10/12/01	V	China

**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
Martin	William Hamilton	Civilian	60/08/00	61/0000	V	<b>Soviet Union</b>
Mascheroni	Marjorie Roxby	Civilian	07/09/00	10/09/17	R	Venezuela
Mascheroni	Pedro Leonardo	Civilian	07/09/00	10/09/17	V	Venezuela
Maziarz	Gary	Marines	04/00/00	06/10/00	R	<b>United States</b>
Mehalba	Ahmed	Civilian	03/00/00	03/09/29	R	<b>Egypt</b>
Millay	William Colton	Army	11/06/00	11/10/28	V	Russia
Miller	Richard William	Civilian	84/05/00	84/10/03	R	<b>Soviet Union</b>
Mintkenbaugh	James Allen	Army	53/06/00	65/04/05	R	<b>Soviet Union</b>
Mira, F.	Francisco de Asis	Air Force	82/05/00	83/03/25	V	<b>Soviet Union</b>
Mitchell	Bernon Ferguson	Civilian	60/08/00	61/00/00	V	<b>Soviet Union</b>
Mohamed	Ali Abdelseoud	Army	89/00/00	98/09/10	V	<b>Al Qaeda</b>
Montaperto	Ronald N.	Civilian	83/00/00	04/02/04	R	<b>China</b>
Montes	Ana Belen	Civilian	80/00/00	01/09/21	R	<b>Cuba</b>
Moore, II	Edwin Gibbons	Civilian	76/12/22	76/12/22	V	Soviet Union
Morison	Samuel Loring	Civilian	84/07/00	84/10/01	V	<b>United Kingdom</b>
Mortati	Thomas	Civilian	81/00/00	89/12/01	R	<b>Hungary</b>
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
Myers	Gwendolyn S.	Civilian	80/00/00	09/06/04	R	<b>Cuba</b>
Myers	Walter Kendall	Civilian	80/00/00	09/06/04	R	<b>Cuba</b>
Nesbitt	Frank Arnold	Civilian	89/09/00	89/10/14	R	<b>Soviet Union</b>
Nicholson	Harold James	Civilian	94/06/27	96/11/16	V	<b>Soviet Union</b>
Nicholson	Nathaniel James	Civilian	06/06/00	09/01/29	R	<b>Russia</b>
Nour	Almaliki	Civilian	03/00/00	06/10/00	V	<b>Al Qaeda</b>
Nozette	Stewart David	Civilian	09/09/03	09/10/19	R	Israel
Oakley	Roy Lynn	Civilian	06/10/17	07/08/02	V	France
Orr	Brian Scott	Civilian	13/09/00	13/11/15	V	China
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	<b>East Germany</b>
Pelton	Ronald William	Civilian	80/01/15	85/11/25	V	<b>Soviet Union</b>
Peri	Michael Anthony	Army	89/02/20	89/03/04	V	<b>East Germany</b>

**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
Perkins	Walter Thomas	Air Force	68/12/00	71/10/21	R	<b>Soviet Union</b>
Petersen, Jr.	Joseph Sidney	Civilian	48/03/01	54/10/09	V	<b>Netherlands</b>
Pickering	Jeffrey Loring	Navy	82/00/00	83/00/00	V	<b>Soviet Union</b>
Pitts	Earl Edwin	Civilian	87/07/00	96/12/18	V	<b>Soviet Union</b>
Pizzo, II	Francis Xavier	Civilian	85/08/11	85/08/13	V	Soviet Union
Pollard	Anne Henderson	Civilian	85/11/00	85/11/22	R	<b>Israel, China</b>
Pollard	Jonathan Jay	Civilian	84/06/00	85/11/21	R	<b>Israel, China</b>
Ponger	Kurt Leopold	Civilian	49/06/15	53/01/14	R	<b>Soviet Union</b>
Ramsay	Roderick James	Army	83/09/00	90/06/07	R	<b>Hungary, Czechoslovakia</b>
Rees	Norman John	Civilian	42/00/00	71/0000	V	<b>Soviet Union</b>
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	<b>Soviet Union</b>
Richardson	Daniel Walter	Army	88/01/00	88/01/14	V	Soviet Union
Rohrer, G.	Glenn Roy	Army	58/00/00	65/0000	R	<b>Czechoslovakia</b>
Rondeau	Jeffrey Stephen	Army	85/00/00	92/10/22	R	<b>Hungary, Czechoslovakia</b>
Roth	John Reece	Civilian	04/01/00	08/05/21	V	<b>China</b>
Sachtleben	Donald John	Civilian	09/00/00	12/05/11	V	<b>United States</b>
Safford	Leonard Jenkins	Army	67/02/08	67/08/25	V	<b>Soviet Union</b>
Santos	Joseph	Civilian	95/00/00	98/09/10	R	<b>Cuba</b>
Sattler	James Frederick	Civilian	67/00/00	74/0000	R	<b>East Germany</b>
Scarbeck	Irvin Chambers	Civilian	60/12/22	61/06/13	R	<b>Poland</b>
Schoof	Charles Edward	Navy	89/10/00	89/12/01	V	Soviet Union
Schuler	Ruby Louise	Civilian	79/05/01	83/00/00	R	<b>Poland</b>
Schwartz	Michael Stephen	Navy	92/11/00	96/00/00	9	<b>Saudi Arabia</b>
Scranage	Sharon Marie	Civilian	83/12/00	85/07/11	R	<b>Ghana</b>
Seldon	Phillip Tyler	Civilian	92/11/00	96/00/00	R	<b>El Salvador</b>
Shaaban	Shaaban Hafed	Civilian	02/11/00	05/03/03	V	Iraq
Shemami	Najeb Elias	Civilian	02/00/00	07/04/17	R	<b>Iraq</b>
Sherman	Daniel Max	Civilian	04/01/00	08/04/15	V	<b>China</b>
Shriver	Glenn Duffie	Civilian	04/10/00	10/06/24	R	China

**APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS**

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
Shu	Quan-Sheng	Civilian	03/01/00	08/09/24	V	<b>China</b>
Slatten	Charles Dale	Army	84/02/00	84/04/14	V	Soviet Union
Slavens	Brian Everett	Marines	82/08/31	82/09/04	V	Soviet Union
Smith	Richard Craig	Civilian	81/00/00	84/05/04	V	<b>Soviet Union</b>
Smith	Timothy Steven	Civilian	00/04/07	00/04/07	V	Al Qaeda
Sombolay	Albert T.	Army	90/12/00	91/03/29	V	<b>Jordan, Iraq</b>
Soueid	Mohamad	Civilian	11/03/00	11/10/11	R	<b>Syria</b>
Souther	Glenn Michael	Civilian	80/00/00	86/00/00	V	<b>Soviet Union</b>
Squillacote	Theresa M.	Civilian	80/00/00	97/10/07	R	<b>East Germany</b>
Stand	Kurt Allen	Civilian	72/00/00	97/10/04	R	<b>East Germany</b>
Szabo	Zoltan	Army	67/00/00	89/05/21	R	<b>Hungary</b>
Thompson	Robert Glenn	Air Force	57/06/00	65/00/00	V	<b>Soviet Union</b>
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	<b>Soviet Union</b>
Tsou	Douglas S.	Civilian	86/03/00	88/02/09	V	<b>Taiwan</b>
Tumanova	Svetlana	Civilian	78/00/00	87/09/28	R	<b>Soviet Union</b>
Underwood	Bryan	Civilian	11/03/01	11/09/01	V	China
Velazquez	Marta Rita	Civilian	83/00/00	02/06/00	R	<b>Cuba</b>
Verber	Otto	Civilian	49/06/15	53/01/14	R	<b>Soviet Union</b>
Walker	Arthur James	Civilian	81/00/00	85/05/29	R	<b>Soviet Union</b>
Walker, Jr.	John Anthony	Navy	68/01/00	85/05/20	V	<b>Soviet Union</b>
Walker	Michael Lance	Navy	83/09/00	85/05/22	R	<b>Soviet Union</b>
Waring	James Earnest	Air Force	60/00/00	63/00/00	R	<b>Soviet Union</b>
Warren	Kelly Therese	Army	86/00/00	97/07/10	R	<b>East Germany</b>
Weinmann	Ariel Jonathan	Navy	05/07/00	06/03/26	V	<b>Russia</b>
Whalen	William Henry	Army	59/12/00	66/07/12	R	<b>Soviet Union</b>
Whitworth	Jerry Alfred	Navy	75/02/00	85/06/03	R	<b>Soviet Union</b>
Williams	Herman Carleton	Air Force	64/00/00	72/00/00	V	<b>Soviet Union</b>
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

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

<b>Surname</b>	<b>Given Name</b>	<b>Affiliation</b>	<b>Date Began<sup>81</sup></b>	<b>Date of Arrest</b>	<b>Volunteer or Recruit</b>	<b>Actual or Attempted Recipient<sup>82</sup></b>
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	<b>Soviet Union</b>
Yai	John Joungwoong	Civilian	97/12/00	03/02/04	R	<b>North Korea</b>