



COUNTERINTELLIGENCE THEORY AND PRACTICE

Hank Prunckun

Counterintelligence Theory and Practice

Security and Professional Intelligence

Education Series

Series Editor: Jan Goldman

In this post-September 11, 2001, era there has been rapid growth in the number of professional intelligence training and educational programs across the United States and abroad. Colleges and universities, as well as high schools, are developing programs and courses in homeland security, intelligence analysis, and law enforcement, in support of national security.

The Security and Professional Intelligence Education Series (SPIES) was first designed for individuals studying for careers in intelligence and to help improve the skills of those already in the profession; however, it was also developed to educate the public in how intelligence work is conducted and should be conducted in this important and vital profession.

1. *Communicating with Intelligence: Writing and Briefing in the Intelligence and National Security Communities*, by James S. Major. 2008.
2. *A Spy's Résumé: Confessions of a Maverick Intelligence Professional and Misadventure Capitalist*, by Marc Anthony Viola. 2008.
3. *An Introduction to Intelligence Research and Analysis*, by Jerome Clauser, revised and edited by Jan Goldman. 2008.
4. *Writing Classified and Unclassified Papers for National Security: A Scarecrow Professional Intelligence Educational Series Manual*, by James S. Major. 2009.
5. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*, revised edition by Don McDowell. 2009.
6. *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation*, by David L. Perry. 2009.
7. *Tokyo Rose / An American Patriot: A Dual Biography*, by Frederick P. Close. 2010.

8. *Ethics of Spying: A Reader for the Intelligence Professional*, edited by Jan Goldman. 2006.
9. *Ethics of Spying: A Reader for the Intelligence Professional*, Volume 2, edited by Jan Goldman. 2010.
10. *A Woman's War: The Professional and Personal Journey of the Navy's First African American Female Intelligence Officer*, by Gail Harris. 2010.
11. *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, by Hank Prunckun. 2010.
12. *Handbook of Warning Intelligence: Assessing the Threat to National Security*, by Cynthia Grabo. 2010.
13. *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, by William J. Lahneman. 2011.
14. *Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats, Second Edition*, by Jan Goldman. 2011.
15. *Counterintelligence Theory and Practice*, by Hank Prunckun. 2012.

S.P.I.E.S

Counterintelligence Theory and Practice

Hank Prunckun

ROWMAN & LITTLEFIELD PUBLISHERS, INC.
Lanham • Boulder • New York • Toronto • Plymouth, UK

Published by Rowman & Littlefield Publishers, Inc.
A wholly owned subsidiary of The Rowman & Littlefield Publishing Group, Inc.
4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706
www.rowman.com

10 Thornbury Road, Plymouth PL6 7PP, United Kingdom

Copyright © 2012 by Rowman & Littlefield Publishers, Inc.

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without written permission from the publisher, except by a reviewer who may quote passages in a review.

British Library Cataloguing in Publication Information Available

Library of Congress Cataloging-in-Publication Data

Prunckun, Henry W.
Counterintelligence theory and practice / Hank Prunckun.
p. cm.
Includes index.
ISBN 978-1-4422-1911-3 (alk. paper)—ISBN 978-1-4422-1933-5 (pbk. : alk. paper)—ISBN 978-1-4422-1912-0 (electronic)
1. Intelligence service. I. Title.
JF1525.I6P775 2012
327.1201—dc23
2012030929

 The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992.

Printed in the United States of America

To the memory of my father, who, almost half a century ago, was in the vanguard of those who recognized the value of open-source intelligence. In this regard, he taught me that whatever you wanted to know could be found in books. His view of knowledge changed my world and I hope I am able to pass on his insight in order to keep the spirit of knowledge philanthropy, which he engendered in his approach to learning, alive.

Editor's Foreword

Editor's Foreword

Counterintelligence is one of the most popularized aspects of intelligence work. Intelligence analysis, imagery interpretation, and developing the intelligence requirements (i.e., questions that need to be answered) all take a backseat to the media and public perception of the glamour of counterintelligence. In a nutshell, counterintelligence is preventing your enemy from knowing what you are doing, in your determination to collect information on them. If collecting information in order to turn it into intelligence is the goal, then counterintelligence is to deny that effort to collect that information.

There are plenty of counterintelligence books that display the cat-and-mouse of intelligence operatives who seek to avoid getting captured by the enemy. A quick search of novels and movies over the last fifty years produces a treasure trove of results. Additionally, in the academic world, there are countless books on the history of counterintelligence operations. However, this book is different.

I am extremely proud to say that this book is one of the few unclassified publications that actually describes what constitutes a successful counterintelligence operation, as well as the elements that compose such an operation. In essence, counterintelligence is about a government's ability to keep secrets, and this book explains how to do it from both an academic and practitioners' point of view, which makes this a very special publication.

Jan Goldman, EdD
Series Editor

Preface

Preface Preface

The English philosopher and scientist Francis Bacon is attributed with saying: “He that will not apply new remedies must expect new evils; for time is the greatest innovator.” If intelligence officers and analysts are to avoid “new evils” when it comes to the security of classified information and the secret operations these data underpin, it follows that they must apply new remedies. To do this, a book that addresses the issues of counterintelligence theory and practice is needed.

This book attempts to fill a void in the subject literature that has remained for some time. For instance, during my twenty-eight years as a practitioner in the fields of security, investigation, intelligence, and research, I have found that there was a dearth of texts available on counterintelligence that discussed in simple, clear terms the craft’s theory and practice. This is not to say that there are only a few texts on the subject—to the contrary, there are many. However, many of these books tend to be written with disappointingly little practical explanation and no theoretical base. Because of this, many of these texts view counterintelligence simply as “security,” which it is not. As such, although there are a number of texts on library shelves that contain the title *counterintelligence*, they are, in my view, narrow and somewhat limiting in their coverage and do not place counterintelligence in the context in which it needs to sit. For the new recruit to counterintelligence, or for the instructor teaching the subject, these texts leave them wanting.

My awareness that such advice was lacking in the counterintelligence field was first realized through my experience as a government investigator and later as an intelligence analyst and strategic researcher. Then, the revelations of the 9/11 Commission into the U.S. terrorist attacks, as well as other inquiries into the worldwide phenomena of radical Islamic terrorism, underscored the importance for agencies in both the public and private sectors to guard confidential

information. The implications of not doing so are discussed in the first chapter. This book was written, therefore, to provide vital, no-nonsense assistance to practicing professionals and students who are in need of “new remedies.”

This book aims to provide the reader with more than just the basics of counterintelligence; instead it equips them with an advanced understanding of the underlying theory that supports the art and science of the craft. This book is arranged in fourteen chapters that take the reader from an examination of the challenges that present for counterintelligence to the practicalities of defensive and offensive counterintelligence.

The book covers a range of topics in a funnel approach—starting from the general and moving to the specific. The book starts by illustrating some events that encapsulate the key challenges for counterintelligence officers as a way of setting the scene. It then moves to explain the fundamentals and practical aspects of what counterintelligence involves, including what a counterintelligence function might look like in operation. Following this scene setting, the book then takes the reader through the theoretical underpinnings of counterintelligence.

The bulk of the book examines the two main foci of counterintelligence—that is, defensive and offensive counterintelligence. Chapters four through thirteen take the reader through the practical aspects of applying the theory (chapter three) to real-world situations. The book concludes with a general treatment of ethical issues as they apply to the profession (chapter fourteen), and this is followed by four appendixes that provide examples relating to issues discussed in the text.

As one of the book’s intended purposes is as a text for students and instructors, each chapter concludes with a list of key words and phrases and a number of study questions and learning activities. Instructors can use these teaching aids as-is or use them as a base from which to develop their own materials for assessment. Students can use these aids to test their understanding independent of whatever assessments their instructors assign, or, if the reader is progressing through the book as some type of “self-paced study” or “self-

improvement” undertaking (perhaps as part of their continuing professional development), they can use these learning aids for self-assessment. There are two preliminary pieces of advice for students entitled “About the Study Questions” and “Key Concepts to Note” that appear in the front portion of this book.

I am grateful to Dr. Rosemary Woolston (Head of School, Australian Graduate School of Policing and Security, Charles Sturt University, Sydney) for encouraging my research and for providing me with the time to research and write the text. I am indebted to several people for their feedback on early drafts of the manuscript, in particular: Dr. Petrus “Beer” Duvenage (State Security Agency, South Africa), Dr. Charles Vandepoor (University of Adelaide, South Australia), Dr. Anna Corbo Crehan (Charles Sturt University, Goulburn, New South Wales), Professor Mick Keelty (Charles Sturt University, Canberra), Associate Professor Nick O’Brien (Charles Sturt University, Canberra), Mr. Jeff Corkill (Edith Cowan University, Western Australia), and Mr. Grant Pink (Visiting Fellow, Australian National University, Canberra). Although these colleagues provided insightful comments on various aspects of this book, if there are any shortcomings, they remain mine and mine alone.

Dr. Hank Prunckun

Sydney, 2012

About the Study Questions

About the Study Questions

Here is some advice about the study questions listed at the end of each chapter and how to approach and ultimately answer them:

Explain/List/Describe	This type of question asks you to outline the factors associated with the issue under study.
Argue	This type of question asks you to present the factors associated with the issue under investigation, but requires you to select one of the factors so that you can defend it.
Discuss	This type of question asks you to form a view (or judgment) after weighing the factors for, the factors against, and the factors that influence the issue under study.

Key Concepts to Note

Key Concepts to Note

Please bear in mind that this book addresses counterintelligence from a wide perspective. As a “compass,” it uses the definition of “an activity aimed at protecting an agency’s intelligence program against an opposition’s intelligence service” to facilitate a universal approach to the topic.

So, throughout this book, there are two terms that are used generically; they are the *agency* and the *opposition*. As this book is a treatment of the theory and practice of counterintelligence from the widest perspective, terms that reflect “friend” and “foe,” regardless of the “industry” or environment in which counterintelligence is practiced, were needed. The solution was to adopt the generalized terms of *agency* for all friendly forces (whether military, government, business, or private individuals) and *opposition* for all forms of foe (which is consistent with the military concept of an opposing force).

The use of the term *agency* can therefore refer to any organization, or even a nation-state. The term *opposition* can be used to mean any person or group (including a nation-state, etc.) with hostile intent. In this way, such a definition is applied throughout the book to issues that span national security, military, law enforcement, and business/corporate intelligence, or even private affairs. This wide approach makes the treatment of counterintelligence current and applicable across today’s threat environment.

Chapter 1

Challenges for Counterintelligence

Chapter 1 1 Challenges for Counterintelligence

This topic provides an introduction to the challenges of counterintelligence by examining:

1. Why counterintelligence;
2. Selected historical lessons; and
3. Some concluding thoughts.

WHY COUNTERINTELLIGENCE?

As his vehicle came to a stop at a crowded intersection in Lahore, Pakistan, Raymond Davis, a Central Intelligence Agency (CIA) contract operative, noticed a motorcycle driver and passenger pass him and stop in front of his car. In an instant Davis knew he was in danger. The passenger raised a handgun and leveled it at Davis but, before he was able to aim and fire, Davis shot him five times—Davis's bullets piercing his own car's windshield and then the body of the would-be attacker. Davis later killed the motorcycle's driver and recorded the two assailants' faces with his camera. Although this was a successful defense, Davis's intelligence operation was now compromised and he could think of only one thing—evasion and escape.^[1]

This event took place on 27 January 2011 in Lahore while Davis's employer was mounting operations against targets openly hostile to the United States of America and, consequentially, to its allies and their intelligence services—namely, those of Australia, Canada, New Zealand, and the United Kingdom—collectively known as the *Five-Eyes*.

The motives of Davis's attackers and those who they represented were not understood at the time of the attack and were still a mystery at the time of this writing. Nevertheless, someone knew of the role of the American operative and the intelligence agency he worked for, and therefore they knew his movements that day. As such, they were able to

disrupt the intelligence operation and, in the process, expose secrets about the operative and the U.S. agency. In the end, Davis was arrested and an attempt was made by the Pakistani authorities to interrogate him; but his training and personality held and no information, other than some superficial details, was revealed.

The lesson to be drawn from this case is that, at some time during the operation or its planning, details were gathered by forces hostile to the Americans and these data were used to mount a counteroperation to neutralize it. Somewhere along the way counterintelligence failed to protect Davis and his mission's managers. In the end, the counterintelligence practices failed to protect the interests of the United States and, consequentially, those of its Five-Eyes partners.

Stating these shortcomings is not to try and attribute blame to anyone or any agency—it is acknowledged there are risks in conducting all intelligence operations and all intelligence research projects. But it is important to understand the consequences of mission failure in addition to understanding how failure occurred. By doing so an agency can understand how to apply counterintelligence theory in order to develop better counterintelligence procedures and practices.

So, was the Davis case in Lahore an atypical event or was it symptomatic of a much wider issue to be considered in the context of counterintelligence? Undoubtedly this was a case of great national security concern that, arguably, crossed over to include aspects of military counterintelligence too. But there are cases much less dramatic than this one that involved law enforcement, private security, and business intelligence that are no less concerning for those involved. Take, for instance, the case involving private investigators hired by Hewlett-Packard who allegedly accessed personal telephone records of some of the company's directors in an attempt to identify the source of the company's leaks to the media.^[2] Or the case of Hollywood private investigator Anthony Pellicano, who was convicted of wiretapping and racketeering in 2008, and was sentenced to a federal prison.^[3]

Then again, these are not isolated cases—a search of archived media reports will uncover hundreds of security breaches like these.

Examples of where counterintelligence was less than adequate can be seen in this list:

- practicing government-licensed private security guards who had links to outlaw motorcycle gangs;
- security officers who left secret access code numbers posted in plain view on gates to an airport restricted zone;
- a Pakistani police guard who was assigned to protect dignitaries only later revealed as a link to an insurgent group;
- government legislators who had their computer facilities penetrated by suspected foreign intelligence services;
- a multinational computer company whose corporate database was penetrated by unknown persons who stole thousands of items of personal client information;
- police officers who have sold law enforcement information to private investigators;
- a juror who made contact with a defendant during a criminal trial via a social networking website;
- outlaw motorcycle gang members who target civil servants in an attempt to bribe them into providing confidential government records, or modifying records that were held and maintained by motor vehicle registries or courts;
- hundreds of government-licensed private security officers who were banned from working in the industry because of drug, alcohol, firearms, and violence offenses; and
- an official of the U.S. National Security Agency who leaked secret information regarding a highly classified communications intercept program.

Failure to protect secrets has widespread ramifications with clear evidence of peril, and these dangers must be addressed. Let us examine some selected cases that underscore the depth and breadth of the challenge that counterintelligence must withstand.

SELECTED HISTORICAL LESSONS

Nathan Hale

During the American War of Independence, the colonial forces suffered a serious defeat during the battle for Long Island (August 27, 1776). This defeat suggested to General George Washington that his forces needed better intelligence to aid battle plans. He is reported to have called for volunteers to go behind the British lines and obtain information on aspects of the British position.

Answering this call was Nathan Hale. As history records, Hale was a patriot of unequalled spirit and one who went undercover without fear in order to try and penetrate British operations. But, lacking training in counterintelligence, Hale and his intelligence operation were discovered early in the mission. Before he was able to pass on any useful intelligence, Hale was executed uttering the now famous words: “I only regret that I have but one life to lose for my country.”^[4]

If only Hale’s bravery was matched by skills in the tradecraft of counterintelligence, he may have left the nation with an equally inspiring legacy—other than those loyal words—that is, a successful penetration of a formidable opposition force.

Pentagon Papers

The Pentagon Papers was the name given to a study of America’s involvement in Vietnam from 1945 to 1967.^[5] Its official title was *United States–Vietnam Relations, 1945–1967: A Study Prepared by the Department of Defense*. The study was commissioned in 1967 by the then secretary of defense, Robert S. McNamara. The study was essentially an encyclopedic history of the Vietnam War that comprised “thirty-seven studies and fifteen collections of documents contained in forty-three volumes.”^[6] These were classified “Top Secret—Sensitive.” The study was written by a team of thirty-six analysts—termed the “Vietnam Task Force”—at the Pentagon who used secondary data from official archival sources.^[7]

In 1971 the *New York Times* began publishing a series of extracts that were leaked by Dr. Daniel Ellsberg, an analyst who once worked on

the secret history. The ethical issues surrounding Ellsberg's motivation for leaking the documents aside, this case highlights that, even with a document classification system and physical controls over the documents, a person with intent (whether motivated by what they see as a higher principle, just plain greed, the thrill, or the benefit to a foreign intelligence service) was able to photocopy thousands of pages of top secret documents and publicly air their contents.^[8] The fact that classified material was released without the sanction of legal authority is a standout example of the need for a counterintelligence function—one that was repeated in 2010 with the leaking of some 250,000 classified documents (see WikiLeaks Affair below).

Arguably, the leaking of these classified documents set in motion events that led to several other counterintelligence operations that started off, perhaps, well intentioned but, in the end, were misguided and, in many aspects, illegal. Known as the Watergate Affair, these events involved the White House Plumbers and an informant with the code name of “Deep Throat.”

White House Plumbers

In 1971, and partially in response to the Ellsberg-leaked Pentagon Papers, the Nixon White House established a group of counterspies—the Special Investigation Unit (also known as the *Plumbers*—for those who stop leaks . . .). History has shown that the individuals who comprised this unit conducted a number of illegal covert intelligence operations in their attempt to stop government leaks. These included a break-in of Dr. Ellsberg's psychiatrist's office in California, and an aborted attempt to discredit Ellsberg—slipping him the hallucinogenic drug LSD before he was scheduled to speak at a fundraising dinner in Washington, DC.^[9]

The low point of these operations came with the break-in of the Democratic National Committee headquarters in the Watergate office complex in Washington, DC, in June 1972. History records the various investigations, hearings, and court trials that followed, with volumes of classified information being revealed as a consequence of the operatives' actions. Aside from the ethical and legal issues that this case

raised, the lack of understanding of, and/or the lack of proficiency in employing, the principles and practices of counterintelligence was apparent.

In an interesting tangent, in 1988 E. Howard Hunt, one of those convicted of the Watergate break-in, wrote a fictional spy thriller entitled *The Sankov Confession*. In it, Hunt painted a cynical portrayal of counterintelligence through the dialogue of the story's central character, Brent Graves:

Sorting out logistic problems: inventorying boots, uniforms, weapons, radios, field equipment. My heart wasn't in it. Then the program closed down and I came back to another half-assed assignment—counterintelligence. I knew less about it than the average typist. [10]

Hunt's uncomplimentary categorization of counterintelligence and the insinuation that a low-level, office-based clerical staffer might know more about counterintelligence than a field operative is ironic. It could be argued that Hunt's lack of sound counterintelligence theory and practice was instrumental in ending the Watergate "black bag" operation he was party to in June 1972, as well as his and his fellow operatives' subsequent imprisonment (for illegal entry into the headquarters of the Democratic National Committee at the Watergate building in Washington, DC).

Deep Throat

One of the inquiries that was conducted in relation to the Watergate break-in was that of investigative reporters Bob Woodward and Carl Bernstein of the *Washington Post*. [11] Arguably, it was their investigation that exposed the operation and gave rise to the subsequent public events. [12] However, it is acknowledged that their investigation would not have been as successful as it was had it not been for the information provided by an informer—Deep Throat. W. Mark Felt was at the time (1972) second-in-charge of the Federal Bureau

of Investigation (FBI) but still leaked critical information that guided the two reporters' investigation using this code name.

Deep Throat is an interesting case as it highlights two simultaneous counterintelligence issues—first, the leaking of classified information by a trusted government employee (again, regardless of the motive and ethics) and the inability of the FBI or other security or intelligence agency to identify and prevent leaking; second, the high level of counterintelligence tradecraft practiced by Felt. For instance, until Woodward revealed the identity of Felt in his 2005 book, *The Secret Man*, [13] the identity of Deep Throat was a mystery. [14] Even a team of investigative journalists under the supervision of Pulitzer Prize-winning investigative journalist William C. Gaines could not identify Deep Throat [15] after years of probing. [16]

Woodward's book describes the counterintelligence methods used by Felt when he passed Woodward information. The procedures Woodward described were, by any account, first class and, not surprisingly, the basis on which the secret remained a mystery for over thirty years. Ironically, the lack of counterintelligence controls by government agencies and the high level of controls practiced by Felt are examples of why the counterintelligence profession faces continued challenges.

Richard Welch Assassination

Richard Welch became the Central Intelligence Agency's chief of station in Athens, Greece in July 1975. However, his assassination in December 1975 underscores several counterintelligence issues that he should have been aware of and addressed through sound counterintelligence practice: (1) he stayed in a house that was occupied by a number of his CIA predecessors; [17] (2) his name and address had been published in Greek newspapers (his name and identity as a CIA officer was also published in an East German publication, [18] the left-wing magazine *CounterSpy* [19]); (3) he was able to be followed by four

men in a stolen vehicle on his way home; and (4) he was able to be approached without warning or challenge and, hence, killed at close range after being followed home.^[20]

The number of counterintelligence miscalculations that occurred in this case and the magnitude of what took place—his assassination—were surprising given the important position Mr. Welch held in the agency,^[21] especially in the hostile political-left atmosphere that existed in Greece at the time.

Aldrich Ames

Aldrich Ames was a career officer and analyst employed by the Central Intelligence Agency. His area of specialization was Soviet affairs, and at different times in his career he was assigned to recruiting and supervising agents, as well as the behind-the-scenes planning. Reports showed that his performance varied, but one thing bears out: he was successful in providing a large volume of classified information to the Soviet, and later the Russian, intelligence services.^[22]

This information led to the execution of a number of friendly agents. Beginning in 1985 and continuing until his arrest in 1994, Ames is reported to have received US\$4.6 million for his espionage activities. Although there were indicators early on, counterintelligence was not able to identify that there was a security issue, and, when it did, it took some ten months to investigate the matter before culminating in his arrest on February 21, 1994.^[23]

Some of the events that were potential indicitors of his espionage activities and were not adequately addressed included: alcohol abuse, extramarital relationships with foreign nationals, security violations, and failure to comply with agency administrative regulations.^[24] There were purchases made that were far in excess of his annual CIA salary occurring over many years—standout items included paying cash for a house and the purchase of a luxury Jaguar motor vehicle.^[25] The Select Committee on Intelligence found that the CIA:

Failed to aggressively investigate the cases compromised by Ames with adequate resources until mid-1991, six years after the compromises occurred; the CIA had failed to adequately limit Ames's assignments and access to classified information after suspicions concerning him had been raised; and the CIA had failed to advise the oversight committees of the losses caused by Ames despite a statutory requirement to advise of "significant intelligence failures." The FBI had failed to devote sufficient resources to the mole-hunt and delayed for too long in opening a formal investigation of Ames.^[26]

The Select Committee found other issues too, like the CIA's failure "to adequately coordinate the operational activities of Ames by allowing him to meet alone with Soviet Embassy officials at a time when he had access to extraordinarily sensitive information pertaining to Soviet nationals working clandestinely with the CIA."^[27]

These counterintelligence miscalculations resulted in, as Ames is reported to have declared: the compromise of "virtually all Soviet agents of the CIA and other American and foreign services known to me."^[28] This was not the only opposition agent operating with a friendly agency —there were others to come—and collectively these events remind us of the challenges for counterintelligence theory and practice.

WikiLeaks Affair

WikiLeaks was a web-based organization created in 2007 to bring "important news and information to the public . . . [via] . . . an innovative, secure and anonymous way for sources to leak information."^[29] This declaration should be a concern for every counterintelligence officer. Illustrating this point is the alleged leaking in 2010 by Private First-Class Bradley Manning, an intelligence analyst with the U.S. Army stationed in Iraq, of some 250,000 classified documents to the WikiLeaks organization.^[30] This event generated a tempest of controversy that resounded in news, academic, and government circles long after the event and was still reverberating at the time this book

went to print. Like the Ellsberg leaks regarding the Pentagon Papers almost forty years prior, there were ethical justifications given for the leaking of these documents and the ethical debate was one of the dominant discussions following the wholesale public release of these documents onto the Internet.

The point, though, for counterintelligence is how could a low-level army intelligence analyst in an operational environment (i.e., tactical/operational) been given access to such wide-ranging data, much of which could be considered strategic? How could he have extracted these data from classified computer systems in such volumes and then removed them from a classified area to ultimately place them in the hands of an organization that by that organization's own admission was dedicated to "leaking information"? As U.S. Secretary of Defense Robert Gates stated: "The battlefield consequences of the release of these documents are potentially severe and dangerous for our troops, our allies and Afghan partners, and may well damage our relationships and reputation in that key part of the world. Intelligence sources and methods, as well as military tactics, techniques and procedures, will become known to our adversaries."^[31]

If, as alleged, Manning was responsible for this mammoth leak, how could counterintelligence not have noticed and/or acted on the warning signs before he handed over these data? For instance, it was reported that Manning was demoted from specialist to private first-class for assaulting a fellow soldier,^[32] and was sent to a chaplain after officers noticed what was called "odd behaviors."^[33] Posts to the social networking website Manning was said to have been using at the time were reported to reflect a psychologically troubled soldier. Even though U.S. Secretary of Defense Gates advised that "We will aggressively investigate and, wherever possible, prosecute such violations,"^[34] the ramifications of missing these potentially rich counterintelligence indicators, and promptly acting on them, were reflected in the months of controversy that followed the WikiLeaks affair.^[35]

Sony's PlayStation

The ability of the opposition to penetrate national security agencies, as well as the unauthorized release of classified documents by trusted employees, was highlighted in the previous selected cases. But counterintelligence goes beyond the government and military and extends to other sectors, including those in the commercial and industrial arenas. The Sony PlayStation case in early 2011 is just one of a number of examples of how corporate enterprises fail in terms of their counterintelligence responsibilities.

Sony said that, as a result of the attack, an “unauthorized person” had obtained personal information about account holders, including their names, addresses, e-mail addresses, and PlayStation user names and passwords. Sony warned that other confidential information, including credit card numbers, could have been compromised, warning customers through a statement to “remain vigilant” by monitoring identity theft or other financial loss.*

* An excerpt from a newspaper report of the data theft incident. Nick Bilton and Brian Stelter, “Sony Says PlayStation Hacker Got Personal Data,” *New York Times*, April 26, 2011, B1, New York ed.

It could be said that, if a person’s house is burgled, the owner knows it—the TV may be gone, jewelry stolen, and cash missing—but, when data is stolen, the “original” is still there. This makes “information burglary” more difficult to detect. When it comes to computer systems, the only clue that data has been “taken” may come in the form of an entry in an access log (that is, if the person penetrating the system has not deleted his trail or altered it to throw the counterintelligence investigators off track).

In the case of the Sony PlayStation penetration, the impact was troubling in several ways: “Sony has estimated that the hacker attacks will cost it at least 14 billion yen (about \$175 million) in damages, including spending on information technology, legal costs, lower sales and free offers to lure back customers.”^[36] There were a number of counterintelligence issues raised by this case, including the identification

of data that needed classifying (and hence protection), storage, access, and compartmentalizing.



“Wilderness of Mirrors”—a reproduction of Leonardo da Vinci’s Room of Mirrors that demonstrates the inventor’s fascination with optical tricks. His room finds metaphor in the craft of counterintelligence as was famously pointed out by the late James Jesus Angleton, chief of counterintelligence at CIA (1954–1974) when he was reported to have referred to counterintelligence as a wilderness of mirrors. Meaning, an atmosphere where one finds it hard to distinguish between reality and illusion. (The saying is attributed to a passage in T.S. Eliot’s 1920 poem “Gerontion” [T.S. Eliot, *Selected Poems*, New York: Brace and World, 1964]. It was subsequently the title of David C. Martin’s book on counterintelligence at CIA during the cold war [*Wilderness of Mirrors*, New York: Harper and Row, 1980].)

Courtesy of the author.

John Deutch

But it is not just staff of agencies—officers, operatives, and agents—who are the subject of counterintelligence mistakes. When John Mark Deutch left the post of director of central intelligence there was an allegation that he had mishandled classified information. It was alleged that he stored sensitive data on his unclassified home computer and that this information was susceptible to being compromised when he

visited Internet websites.^[37] The CIA’s Office of Inspector General investigated the matter and found that:

Deutch was aware of prohibitions relating to the use of unclassified computers for processing classified information. He was further aware of specific vulnerabilities related to the use of unclassified computers that were connected to the Internet. Despite this knowledge, Deutch processed a large volume of highly classified information on these unclassified computers, taking no steps to restrict unauthorized access to the information and thereby placing national security information at risk.^[38]

GLOBAL OUTLAWS

Unlike in the county in which a person lives, there is no “sheriff” in cyberspace. This makes the Internet like the proverbial Wild West—or the *Wild Web* as some critics have referred to it. It can sometimes appear to be an unsettled and lawless environment where global outlaws roam.

Chief of MI6

Normally the chief of Britain’s secret intelligence service would keep a low profile, as would any serving intelligence officer. This is because the potential for exploitation by opposition forces by publishing personal information about these persons carries serious consequences, as was pointed out in the case of CIA Chief of Station Richard Welch, who was assassinated in Greece in 1975.

However, in July 2009, the world’s media carried the story that Sir (Robert) John Sawers—the soon-to-be chief of Britain’s secret intelligence service (MI6)—had his personal details along with a number of photographs publicly displayed on his wife’s social networking profile on Facebook.^[39] As innocent as this may seem on the surface, a skilled intelligence analyst could use these details to complement existing data holdings on Sir John to develop, say, a psychoanalytic profile^[40] of him

as a leader, his decision-making aptitude for intelligence matters, and so on.

"Hackers trawl social networking sites such as Twitter and Facebook seeking people who have revealed too much personal information, with politicians a favorite because their systems are linked to Departmental systems with valuable public service information."*

* An excerpt from a newspaper report on cyber criminals. Miles Kemp, "We're at War with Hackers," *The Advertiser*, Adelaide, Australia, March 30, 2011, 13.

From a counterintelligence point of view this was a security risk that showed naïveté. Although the James Bond-esque mysteries about the British secret intelligence service are no longer cloaked in secrecy, experience has shown that there is a reason why personnel security forms an important part of counterintelligence practices and procedures. In this case, it may be close to impossible to assess what harm may have been incurred by MI6 because of such a pause in security.

***News of the World* and Alleged Telephone Hacking**

In mid-2011 the world's news media published articles alleging that a wide range of people's personal cell phone messages and records were illegally accessed and details purchased by the now-defunct British newspaper *News of the World* to be used as part of the stories they were reporting. Several of the newspaper's executives who were alleged to be involved in the scheme were arrested and the head of the Metropolitan Police (known as Scotland Yard) resigned.

The hacking allegations centered on the unauthorized access of the telephone accounts of various celebrities, politicians, and members of the British royal family. There were also allegations that the records of a young murdered schoolgirl, relatives of deceased British soldiers, and victims of the 7/7 London bombings were also accessed. The allegations

“that may have included identity theft and bribery of police officers”^[41] outraged the British public and as a result the newspaper’s advertisers withdrew their support, which was reported to have contributed to the *News of the World*’s closure on July 10, 2011 (after 168 years of publication). In January 2012 over thirty civil settlements, which included financial compensation for damages as well as legal costs to some of the alleged victims, were announced.^[42]

Taliban Disclosure of Loya Jirga Security Plans

On November 13, 2011, the Taliban in Afghanistan claimed it had obtained the government’s security plan for the opening of the grand assembly of leaders known as the “Loya Jirga” (see figure 1.2). The Taliban stated on its public website that it had obtained the documents “from two Ministries and from the special security corps of the government.”^[43] The “Mujahideen of Islamic Emirate” stated that:

Our upcoming attacks will become even more lethal and precise with the acquisition of such intelligence material. . . . Besides this, it is also necessary to remind those people who want to participate in this Jirga or agree to its illegitimate resolutions that their lists and actions will be noted down and they will be put on trial.^[44]

The unauthorized release of these security plans not only placed the assembly of leaders at risk at the time of the meeting but, as the threat made clear, for the future too. By implication, the Taliban threatened that its undercover operatives would be noting those who participated for “trial” at a later date.



A security map posted on the Internet by the Taliban to validate the authenticity of the leaked Afghanistan security plans it alleged it had obtained. (Islamic Emirate of Afghanistan, Mujahideen Acquire and Disclose the Security Plans for the Upcoming Supposed Loya Jirga.)

Source: Public domain ([http://shahamat-english.com/index.php?option=com_content&view=article&id=12755:mujahideen-acquire-and-disclose-the-security-plans-for-the-upcoming-supposed-loyal-jirga\[accessed November 15, 2011\]](http://shahamat-english.com/index.php?option=com_content&view=article&id=12755:mujahideen-acquire-and-disclose-the-security-plans-for-the-upcoming-supposed-loyal-jirga[accessed November 15, 2011])).

SOME CONCLUDING THOUGHTS

It would be a naïve person who would argue that an opponent has not thought thoroughly about how to use information in order to develop intelligence, and how to use this insight to attack—whether that attack is to undermine national security, to defeat a military in whatever battle-space it might be fighting, or to dominate business enterprises throughout the world.

A counterintelligence officer needs to know what he or she is tasked to protect. The potential number of information items stored by an agency, the sources of this information, and the methods and final products produced through analysis, as well as the operations surrounding all of these considerations, are vast. As counterintelligence

resources are limited, the first task is to identify what is secret and what is not. This requires counterintelligence operatives to be skilled in analysis.*

* Dr. Petrus “Beer” Duvenage (State Security Agency, South Africa), personal communication, January 23, 2012.

Carl von Clausewitz once wrote: “So long as I have not overthrown my opponent I am bound to fear he may overthrow me. Thus I am not in control: he dictates to me as much as I dictate to him.”^[45] These are words of caution that should be heeded, as dominance in one area of the intelligence rubric does not mean dominance in all. There are without doubt some determined opponents in the world, and, until we find a way to wreck not only their ability to attack, but their *will* to attack, counterintelligence practitioners must stand vigilant against their persistent probing of information defenses. But as ruthless as these opponents might be, they are smart enough to evolve their methods and practices in response to each new innovation that counterintelligence theory and practice brings.

“The group known as Anonymous said Saturday it hacked into some 70 mostly rural law enforcement websites in the United States, a data breach that at least one local police chief said leaked sensitive information about an ongoing investigation. . . . Anonymous said it had stolen 10 gigabytes worth of data in retaliation for arrests of its sympathizers in the U.S. and Britain.”*

* Associated Press, “Group Hacks U.S. Law Enforcement Sites and Steals Data,” *Daily Technology News*, August 7, 2011,dailytechnologynews.org/group-hacks-u-s-law-enforcement-sites-and-steals-data/(accessed January 20, 2012).

There is a Latin proverb that states that a wise man learns from the mistakes of others, whereas a fool learns from his own.^[46] Although said in a different era, and no doubt in a different context, this saying seems

to have application for the challenges of counterintelligence today and certainly provides food for thought as we consider the fundamentals of counterintelligence.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Five-Eyes;
- MI6; and
- WikiLeaks affair; and
- Wilderness of mirrors.

STUDY QUESTIONS

1. Describe three challenges that counterintelligence professionals face in protecting classified information.
2. It could be argued that one of the weakest links in securing information is the human element. Taking this position, explain why this might be the case.
3. Using archived media reports, compile a list of five counterintelligence events that have taken place within the state or province in which you work or live (the time frame is not relevant). Distinguish whether the events were related to a national security, military, law enforcement, or private security/investigation event.
4. Describe the types of information that might be of interest to the opposition who might be: (a) a foreign political state; or (b) a business competitor.

LEARNING ACTIVITY

It has been claimed that the Internet is a form of “Wild Web,” where there is no cyberspace sheriff. This message (in one of the text boxes above) urges caution for those who post private information to the

World Wide Web. In an article that appeared in *The Times* (London), Defence Editor Michael Evans echoed this advice stating, “All members of the [British] Armed Forces are warned about Facebook and other social networking websites. Although they are not banned from the website, they have been told not to include details that could compromise their security. The same warning has been issued at MI5, MI6 and GCHQ, the Government’s eavesdropping center in Cheltenham.”^[47] So, as a learning exercise to demonstrate how such information could be complied by the opposition, use the Internet to assemble a dossier on *yourself*. Use only Internet-based information from the results of search engine queries—for example, media archives, social networking websites, other websites, and so forth.

NOTES

1. Jane Perlez, “US Seeks Release of Official in Pakistan,” *New York Times*, January 30, 2011, A4, New York edition. Matthew Teague, “Black Ops and Blood Money,” *Men’s Journal*, June 1, 2011. Compare these events with the successful intelligence operation that culminated with the assassination of an Iranian nuclear scientist in January 2012 by unknown covert operatives. See Rick Gladstone, “Iran Tightens Its Security for Scientists after Killing,” *New York Times*, January 18, 2012, A6, New York edition.
2. Matt Richtel, “Hewlett-Packard Settles Spy Case,” *New York Times*, February 14, 2008.
3. Brookes Barnes, “Pellicano and Lawyer Convicted in Wiretapping,” *New York Times*, August 30, 2008, C1, New York edition.
4. M. William Phelps, *Nathan Hale: The Life and Death of America’s First Spy* (New York: Thomas Dunne, 2008).
5. Neil Sheehan, Hedrick Smith, E. W. Kenworthy, and Fox Butterfield, *The Pentagon Papers as Published by the New York Times* (New York: Quadrangle, 1971).
6. Although the covering memo to the secretary of defense (through Mr. Paul C. Warnke and Dr. Morton H. Halperin), written by Dr. Leslie H. Gelb, chairman of the Office of the Secretary of Defense Task Force, stated that there were forty-three volumes, the notation on the index shows that there were forty-six volumes, plus the index volume, thus making the study a forty-seven-volume set. In June 2011 the entire study was declassified and made public except for eleven words, which remain classified.
7. In my book on intelligence analysis (*Handbook of Scientific Method of Inquiry for Intelligence Analysis* [Lanham, MD: Scarecrow Press, 2010]), I point out the value of archival data in relation to intelligence research. This secret history of the Vietnam War is a case in point, as no primary data in the form of interviews, surveys, or focus groups were sought, yet the goal of the classified research project was accomplished.

8. Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers* (New York: Viking, 2002).
9. G. Gordon Liddy, *Will: The Autobiography of G. Gordon Liddy* (London: Severn House Publishers, 1980), 170.
10. E. Howard Hunt wrote *The Sankov Confession*, as well as several other spy novels under the pseudonym of P. S. Donoghue. P. S. Donoghue, *The Sankov Confession* (New York: Donald I. Fine, 1988), 117.
11. Carl Bernstein and Bob Woodward, *All the President's Men* (New York: Simon and Schuster, 1974).
12. For instance, see Gerald Gold, ed., *The White House Transcripts* (New York: Viking, 1974).
13. Bob Woodward, *The Secret Man: The Story of Watergate's Deep Throat* (New York: Simon & Schuster, 2005).
14. Leonard Garment, *In Search of Deep Throat: The Greatest Political Mystery of Our Time* (New York: Basic, 2000).
15. Which in itself is a curious phenomenon—that is, a group of investigative journalists trying to expose the confidential source of another investigative journalist.
16. John W. Dean, *Unmasking Deep Throat: History's Most Elusive News Source* (San Francisco: Salon.com, 2002).
17. Bob Woodward, *Veil: The Secret Wars of the CIA, 1981–1987* (New York: Simon & Schuster, 1987), 264–65.
18. Julius Mader, *Who's Who in CIA: A Biographical Reference Work on 3,000 Officers of the Civil and Military Branches of Secret Services of the USA in 120 Countries* (Berlin, East Germany: Julius Mader, 1968).
19. Philip Agee, *On the Run* (Secaucus, NJ: Lyle Stuart, 1987), 130–34.
20. Woodward, *Veil*, 264–65.
21. Richard Helms, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003), 433–34.
22. Pete Earley, *Confessions of a Spy: The Real Story of Aldrich Ames* (New York: Putnam, 1997).
23. David Wise, *Night mover* (New York: HarperCollins, 1995).
24. David Wise, *Night mover*. But see also Tim Weiner, David Johnston, and Neil A Lewis, *Betrayal: The Story of Aldrich Ames, An American Spy* (New York: Random House, 1995); and Peter Maas, *Killer Spy: The Inside Story of the FBI's Pursuit and Capture of Aldrich Ames, America's Deadliest Spy* (New York: Warner, 1995).
25. David Wise, *Night mover*.
26. Select Committee on Intelligence, *Special Report, Committee Activities of the Select Committee on Intelligence, United States Senate, January 4, 1993, to December 1, 1994* (Washington, DC: U.S. Government Printer, 1995), 16.
27. Select Committee on Intelligence, *Special Report, Committee Activities of the Select Committee on Intelligence, United States Senate, January 4, 1993, to December 1, 1994*, 16.
28. Aldridge Ames reported in *New York Times*, April 29, 1994, A16:1
29. WikiLeaks, “About,” wikileaks.org/About.html (accessed July 5, 2011).

- [30.](#) Andrew Fowler, *The Most Dangerous Man in the World: How One Hacker Ended Corporate and Government Secrecy Forever* (New York: Skyhorse Publishing, 2011).
- [31.](#) Department of Defense, *DoD News Briefing with Secretary Gates and Admiral Mullen from the Pentagon* (Washington, DC: Office of the Assistant Secretary of Defense (Public Affairs), July 29, 2010). In support of this assertion, *Newsweek Magazine* published a story on August 1, 2010, alleging that some of the WikiLeaks documents contained names and villages of Afghans who were secretly cooperating with the American military. The news story said that, “just four days after the documents were published, death threats began arriving at the homes of key tribal elders in southern Afghanistan. And over the weekend one tribal elder, Khalifa Abdullah, who the Taliban believed had been in close contact with the Americans, was taken from his home in Monar village, in Kandahar province’s embattled Arghandab district, and executed by insurgent gunmen [i.e., Taliban insurgents].” See Ron Moreau and Sami Yousafzai, “Taliban Seeks Vengeance in Wake of WikiLeaks,” *Newsweek Magazine*, August 1, 2010. This story was preceded by others, such as the one that stated: “The Taliban yesterday threatened to decapitate informers revealed in uncensored intelligence documents published on the internet. In their first response since WikiLeaks placed thousands of secret documents online detailing names and locations of anti-Taliban informers, Afghan militants said ‘we know how to punish them’—a reference to beheading, the usual Taliban punishment reserved for ‘Traitors.’” David William, “Taliban Threatens to Behead Informers,” *The Advertiser*, Adelaide, Australia (July 31, 2010), 67.
- [32.](#) Fowler, *The Most Dangerous Man in the World*.
- [33.](#) Fowler, *The Most Dangerous Man in the World*.
- [34.](#) Department of Defense, *DoD News Briefing with Secretary Gates and Admiral Mullen from the Pentagon*.
- [35.](#) For example, as highlighted in Patrick F. Walsh, *Intelligence and Intelligence Analysis* (New York: Rutledge, 2011), 210–18.
- [36.](#) David Jolly and Raphael Minder, “3 Detained in Spain in PlayStation Attack,” *New York Times*, June 11, 2011, B1, New York edition.
- [37.](#) Valerie Plame Wilson, *Fair Game: My Life as a Spy, My Betrayal by the White House* (New York: Simon & Schuster, 2007), 347.
- [38.](#) Central Intelligence Agency, *Inspector General, Report of Investigation: Improper Handling of Classified Information by John M. Deutch* (Washington, DC: CIA, February 18, 2000).
- [39.](#) Sarah Lyall, “On Facebook, a Spy Revealed,” *New York Times*, July 6, 2009, A1, New York edition. Contrast this event with the news report that President Barack Obama, who used social media during his 2008 election campaign, refused to allow his two daughters to join his Facebook page, stating, “Why would we want to have a whole bunch of people who we don’t know knowing our business?” See David Jackson, “Obama: No Facebook for Malia, Sasha,” *USA Today*, December 14, 2011.
- [40.](#) See, for example, a description of this technique in Hank Prunkun, *Handbook of Scientific Method of Inquiry for Intelligence Analysis*, 65.
- [41.](#) John F. Burns, “Victim’s Family Appears amid Rage at Tabloids,” *New York Times*, July 13, 2011, A14, New York edition.

[**42.**](#) Sarah Lyall and Don Van Natta, Jr., “An Arrest and Scotland Yard Resignation Roil Britain,” *New York Times*, July 17, 2011, New York edition, A1; and Sarah Lyall and Ravi Somaiya, “Murdoch Company Settles with Dozens of Hacking Victims,” *New York Times*, January 20, 2012, New York edition, A4, as well as “Phone-Hacking Damages Claims Settled,” *Weekend Australian*, January 21, 2012, 10.

[**43.**](#) Islamic Emirate of Afghanistan, *Mujahideen Acquire and Disclose the Security Plans for the Upcoming Supposed Loya Jirga* (accessed November 15, 2011).

[**44.**](#) Islamic Emirate of Afghanistan, *Mujahideen Acquire and Disclose the Security Plans for the Upcoming Supposed Loya Jirga* (accessed November 15, 2011).

[**45.**](#) Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Oxford, England: Oxford University Press, 1976), 16.

[**46.**](#) A saying that seems to have its origin in an ancient Latin proverb and has been quoted in different forms, but with the same intent.

[**47.**](#) Michael Evans, “Wife of Sir John Sawers, the Future Head of MI6, in Facebook Security Alert,” *Times* (London), July 6, 2009.

Chapter 2

Fundamentals of Counterintelligence

Chapter 2 Fundamentals of Counterintelligence

This topic provides an introduction to the fundamentals of counterintelligence by examining the:

1. Intelligence quadrangle;
2. Role of security in intelligence;
3. Anatomy of counterintelligence;
4. Taxonomy of counterintelligence; and
5. Typology of counterintelligence.

INTELLIGENCE QUADRANGLE

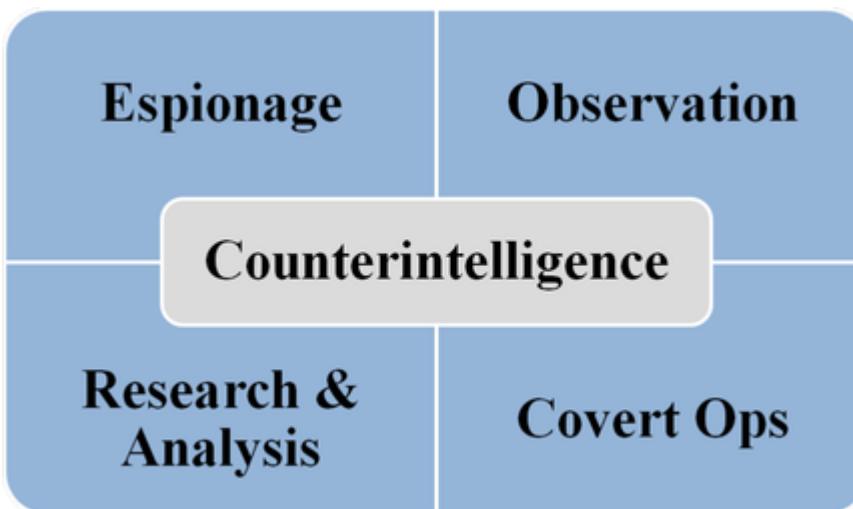
Individuals, corporations, the military, and entire nations owe their safety and well-being to counterintelligence. Without it the intelligence function in all its manifestations could not be as effective as it is. If espionage were a game of sport, those who practice the craft of counterintelligence would be considered the sport's goal keepers. Without these practitioners the opposition would have carte blanche to raid the open and unprotected goal and score endless points.

In order to understand counterintelligence, one needs first to understand intelligence. The term *intelligence* has a number of meanings, so it is important to offer a definition for each of the contexts in which the term is used. *Intelligence* can be defined in the following four contexts:

1. Actions or processes that are used to produce knowledge;
2. The body of knowledge produced as a result of processing;
3. Organizations that deal in knowledge (e.g., an intelligence agency); and
4. The reports and briefings that are the end result of the process or are produced by such an organization.

Sometimes raw data are referred to as *intelligence*, but this is not a correct use of the term. It can only be considered intelligence after it has been analyzed and meaning given to the results. Nevertheless, the common theme in all of these definitions is *knowledge*. In intelligence work, knowledge equates to *insight*. Or, stated another way, it is the ability to *reduce uncertainty*. Intelligence is important, as insight and certainty offer decision makers the ability to formulate policy, propose options, and take actions to better control “the unknown.”

Intelligence can be categorized into four broad functions—espionage, observation, research and analysis, and covert operations. Two of the quadrilateral’s quarters—espionage and observation—support a third quarter, which is research and analysis. In turn, the combination of these three quarters supports a fourth—covert ops. Counterintelligence, therefore, is the keystone that locks these pieces of intelligence mosaic to one another—it is common to all other functions (figure 2.1).



Intelligence quadrangle linked by the keystone of counterintelligence.

Courtesy of the author.

Espionage is seen as the archetypal method for gathering information. It dates back centuries with biblical references to it. For instance, in the fourth book of the Old Testament (Numbers), it states in chapter 13: “The Lord said to Moses, ‘Choose one of the leaders from each of the twelve tribes and send them as spies to explore the land of

Canaan.”^[1] “When Moses sent his spies out, he instructed them: ‘Find out what kind of country it is, how many people live there, and how strong they are. Find out whether the land is good or bad and whether the people live in open towns or fortified cities. Find out whether the soil is fertile and whether the land is wooded. And be sure to bring back some of the fruit that grows there.’”^[2]

This example demonstrates how agents were tasked to collect data about the issue under consideration so that this information could guide action. The word *espionage* is derived from the Old French, meaning *spy*; so it is understandable that it is sometimes simplified to *spying*. This biblical reference points out that espionage utilizes agents to go undercover to gather information. This is distinct from *observation*. So, the way the term “observation” is used here should not be confused with reconnaissance. Reconnaissance is scouting; although it is allied to observation, it has a different purpose. Observation in the context of this book is information gathering in the broadest sense.

An agent is someone who acts on behalf of another person or an agency (e.g., a private investigator, or a private inquiry *agent*). An agent is someone who an intelligence officer recruits to obtain secrets on behalf of the officer’s agency. In such situations, the recruiting officer is termed a *case officer*^[3] (or, in some instances, a recruiter or a *handler*^[4]). Those who perform operational duties are termed *operations officers* or *field officers* (field officers may even have specific role designations, such as *counterintelligence investigators* and the like). There are times when *dummy agents* are created for the purposes of deception. These dummy agents then perform invented activities, such as sending dummy messages or performing invented acts of espionage or sabotage, which form part of the deception plan. These activities give currency to the dummy agent’s “existence,” ultimately promoting carefully crafted disinformation to the opposition.

The role of agents is to place themselves in a position that allows them to obtain information—by viewing, overhearing, participating in discussions, or by other means so that the desired information can be obtained. In the biblical example, the tribal leaders that Moses is reported to have sent to Canaan were tasked with collecting certain data

items. However, with vast technological improvements, *observation* by technical surveillance and unobtrusive methods is a favored source over the use of human agents (though human sources should never be discounted).

“The techniques of secret operations are as old as the human race; they are by no means diabolical inventions . . . or symptoms of a human decline.”*

* Christopher Felix, *A Short Course in the Secret War* (New York: Dutton, 1963), 9.

Generally speaking, operatives are of two forms—those with some form of official cover and those without.^[5] *Cover* is best described as a plausible story about all facets of the operative’s life. If the operative is operating under official cover they can assume the role of a minor diplomat or other person in an embassy or consulate, thus giving them an excuse for being in certain places or undertaking certain activities. Those operating under non-official cover (NOC, pronounced *knock*), sometimes referred to as *commercial cover*, may work for a phantom company created and maintained by an intelligence agency. These operatives have no connection with their government. As has been pointed out by those in the trade, “the best way to protect your cover as a spy is to inhabit your cover identity as much as possible.”^[6]

NOC operatives have been described as the truest practitioners of espionage as they operate on their own at all times. They are afforded no protection from their government while overseas. If they are caught abroad, they may be tortured during interrogation and risk execution. If this happens, it is most unlikely that a media conference will be held and, therefore, no one will hear about the event. NOC operatives operate alone and die alone.

It could be said that espionage worked reasonably well during the Cold War years (1945–1991) when intelligence agencies faced actors that were states, as electronic and other technical means of data gathering were possible. But, since the al-Qaeda terrorist attacks of September 11,

2001, intelligence agencies have recognized the importance of having undercover officers and agents in place to gather information. This is because such groups are ill defined—there are no geographic borders to monitor, no specific land-based targets to reconnoiter, and no organized communities (whether military or social) to assess. Today's targets are bound by ideology and can live within the country of the agency or one of its allies.

During the Cold War, one reason for shifting to technically gathered data was the comparatively high cost of “running” human agents as well as improving the reliability of the data collected. For example, aerial and satellite photographs are not susceptible to an exaggeration of the truth as an agent might be. Technical data simply show what is there and what is not. Furthermore, technological advances have now made much of these data available in real time. As a case in point, take the May 2011 joint CIA and U.S. Navy SEAL operation that targeted Osama bin Laden in his safe house in Abbottabad, Pakistan. This secret operation was transmitted live into the White House Situation Room. However, the events of September 11 and the subsequent terrorist attacks in Madrid, London, and Bali showed that, despite the advantages of technically gathered data, these data may be of little value when faced with terrorist cells operating in a vastly different fashion to that of, say, a foreign government’s military.

Arguably, one of the rules of thumb of espionage is to never give away a piece of information—instead, sell it or trade it for information that is of equal or greater value.

Loosely structured groups related by an ideological bond and other nontraditional challenges to a state-centric paradigm have changed the nature of confrontations. Nations now face threats from weak and corrupt governments, rogue states, substate and transstate actors, as well as international organized criminal groups, radical ethnic and religious groups, and right- and left-wing political groups. All of these threats pose special data collection problems that defy a purely technical collection approach.

Observation

“Observation” refers to those methods for gathering information that center on *viewing*. It employs methods other than placing an agent in a position to obtain confidential information. Observation includes collecting data via technical means such as audio surveillance devices, radio frequency devices, and special photographic equipment, including space-based reconnaissance satellites. It is a catch-all category for a variety of methods other than espionage (as pointed out in the section on espionage above).

The use of technical means of observation through, say, remotely controlled drone aircraft can yield results no other method can. Examples of this can be seen in accounts of how U.S. unmanned aerial vehicles (UAV) were used to hunt down Taliban insurgents in Afghanistan throughout the first decade of the 2000s, and continued up until this book went to press.^[7] However, it is at the peril of an intelligence agency that it neglects data collection by human sources.

Moreover, observation is also concerned with collecting data that is in the public domain through what is termed *open-source* data collection. In some cases the collection of information from open sources can provide an intelligence analyst with an exponential gain in both the quantity and, under the right circumstances, the quality of the information gathered.^[8]

Research and Analysis

Research is sometimes seen as probing esoteric issues and obtaining findings, the applicability of which to real-world situations may at times be difficult to see. In academic disciplines this is termed *basic research* or *theoretical research*. Such research is concerned with discovery for its own sake—that is, when undertaken, it has no practical application. It is knowledge for the sake of knowing. The findings of such research can be used later in an applied setting, but, at the time of conducting the research, the goal was not to apply this knowledge to solving a particular problem.

In contrast, *applied research* has a practical purpose—to offer a basis for making a decision (i.e., to provide *insight*). Intelligence is in this sense applied research: it is the outcome of processing raw information that has been collected from a variety of sources—open sources, semi-open sources, official sources, clandestine sources, and/or covert sources. This function is sometimes termed *positive intelligence* or *positive collection* depending on the context. Once such information is made available to an intelligence analyst, it is evaluated and any irrelevant information discarded. The pieces of information pertinent to the matter under investigation are then analyzed, interpreted, and formed into a finished “product.”

This product can take the form of an oral briefing, a written briefing, a target profile, a tactical assessment, a strategic estimate, or any number of different types of reports. These products are then disseminated to the end users. In intelligence parlance, end users are called *customers*.^[9] The intelligence process can be summarized as analysis that leads to the production of deep, thorough, or meaningful understanding about a particular issue or topic.

Covert Operations

Covert operation lies in a somewhat gray area of intelligence work. Sometimes referred to as *special activities*,^[10] it uses various methods of information gathering including those of research and analysis, but incorporates advice and counsel, financial and material support, and technical assistance to individuals, groups, or businesses that are opposed to, or working in competition with, a target or adversary.

Covert ops, or *black ops* as they are sometimes referred to, are a function by which the perpetrator uses the information it collects through espionage, observation, and analysis to strengthen its allies and to weaken or destroy its opponents.^[11] The effectiveness of covert operations is contingent upon the perpetrator’s involvement remaining hidden, or deniable.

On one hand, if a “plausible denial”^[12] can be maintained, then the rewards of such ventures can be enormous. On the other hand, if the

perpetrator's involvement is discovered, the consequences of this activity can be catastrophic. For example, in 1985 the French government was concerned about protests by Greenpeace regarding nuclear testing on the Pacific atoll of Mururoa. So, on July 10, 1985, French intelligence operatives from the *Direction Générale de la Sécurité Extérieure* (or, in English, the Directorate-General for External Security) mined Greenpeace's *Rainbow Warrior* in Auckland Harbour, New Zealand, with an explosive charge. The vessel sank and the explosion killed one person on board.

New Zealand police mounted an investigation into the incident and two French operatives were arrested, tried, and found guilty. They were then sent to prison. The other French operatives involved in the black op managed to evade capture and escaped. The incident was not only an embarrassment to the French government, but carried political ramifications that affected the French government for many years. Had the operation been carried out successfully—that is, had the operatives managed to escape undetected—then the results of the op would have been much different.

THE ROLE OF SECURITY IN INTELLIGENCE

If one was to speculate about the origins of mankind's need for security, it is possible that it began with primitive man, who required a sanctuary, haven, or retreat from the threats of nature and the wilds. As man developed his security apparatus for the preservation of his life, it may further have developed to protect lands and chattels under his control, which, in turn, allowed him to project power and influence over others.

This early security is likely to have been defensive—employing tactics such as simple barriers, hiding places, natural camouflage, subterfuge, and evasion, along with others. It is likely that, once man started to organize into social groups, security took on more of an offensive role. For instance, feudal states (and their forerunners) formed armies to defend the clan's land from threats by neighbors. The strategy of striking at an external threat in order to prevent it from attacking (i.e., a preemptive attack) could be seen as the precursor to offensive security.

Applying this theory to intelligence, one can see that, in order to protect information that is vital to decision making from threats, some form of security is required. This is the role of counterintelligence.

ANATOMY OF COUNTERINTELLIGENCE

Just as the human anatomy comprises different parts, counterintelligence also comprises different components. But unlike intelligence—which is comprised of espionage, observation, research and analysis, and covert operations—counterintelligence is made up of two interrelated elements: counterintelligence and counterespionage.

Counterintelligence

Counterintelligence is concerned with deterrence and detection. It is a security-focused function, but it is not security. However, security is used defensively within counterintelligence. That is, the thrust of counterintelligence is to protect an agency (or its client) from infiltration by an adversary, to protect against inadvertent leakage of confidential information, and to make secure its installations and material against espionage, subversion, sabotage, terrorism, and other forms of politically motivated violence, and the transfer of key technologies and/or equipment. It is an active model that calls on defensive, as well as offensive, methods of security and uses research and analysis that is core to the intelligence function.

Even though there is a clear distinction between intelligence and counterintelligence, this demarcation line can be thin. That is, information discovered via the counterintelligence function concerning an adversary's attempts to penetrate one's own or partner agency can feed the intelligence side, revealing an opponent's information voids as well as highlighting their capabilities and possible intentions. So, counterintelligence can be seen as both an activity that is carried out and a product that is produced to inform decision makers.

Counterespionage

Counterespionage is concerned with detection, deception, and neutralizing the effectiveness of an adversary's intelligence activities. On the surface, counterespionage presents as a form of spying—collecting classified information through, say, a network of agents. And it is, but the difference is that it is the acquisition of data not from another nation's government or military, but from the opposition's intelligence service. It is in some ways related to counterintelligence, but differs in others. Counterintelligence could be seen as the defensive side of the craft, whereas counterespionage is the offensive side. An agency cannot have the latter without the former, so the two work in tandem.

Counterespionage is a precise function that is, arguably, the most subtle and sophisticated of all intelligence functions. It calls for the engineering of complex strategies that deliberately put one's agent(s) in contact with an opposition's intelligence personnel. This is done so that classified information can be obtained, or the adversary can be fed disinformation, which should lead to confusion, thus disrupting the adversary's operations, thus allowing the perpetrator to prosper. False information can also be planted, so, like a "barium meal," the route that this information travels within the opposition's intelligence apparatus can be traced in order to confirm penetration by a mole or expose other security leaks. It could be argued that counterespionage could not carry out its mission without the support of the methods and practices of counterintelligence.

If counterespionage were a religion, then case officers would be its high priests.*

* Adapted by the writer from a passage about Mossad that appeared in David Ignatius, *Agents of Innocence* (London: W. H. Allan, 1988), 337.

Security, Law Enforcement, or Intelligence

If viewed with a superficial eye, counterintelligence could easily be confused with the humble role of security. After all, it oversees many of

the methods for securing facilities, materiel, and personnel. But it also includes investigations where breaches of security are suspected or have taken place; so, does this make it a law enforcement role?

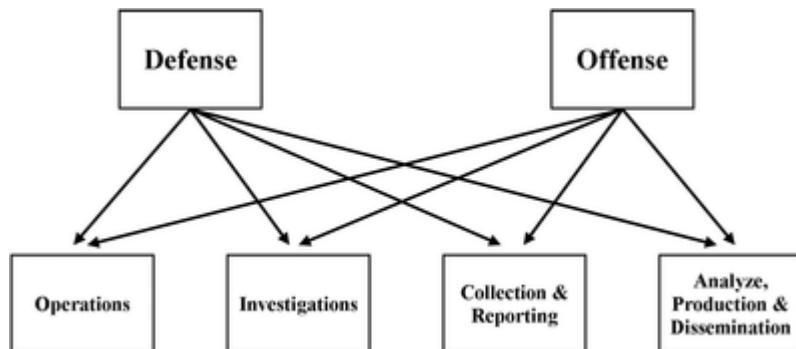
Counterintelligence also involves research and analysis; so does that make it an intelligence function?

In essence it is all of these—a fusion of security, law enforcement, and intelligence into a form uniquely termed *counterintelligence*. But because it is a composite of the three, no one function can be separated from the whole without leaving it incapacitated. In practice, this means that counterintelligence officers will liaise with their counterparts in the fields of security and police (including regulators and compliance), as well as intelligence. But unlike their counterparts, counterintelligence officers will have responsibilities that span all three fields.

TAXONOMY OF COUNTERINTELLIGENCE

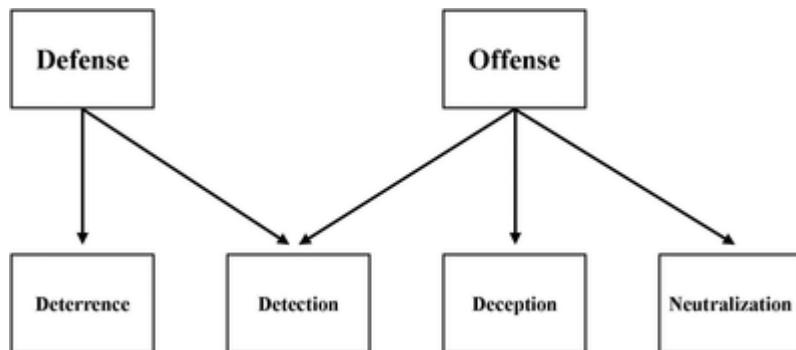
Although intelligence can be classified into three categories—operational, tactical, and strategic—counterintelligence’s taxonomic categories are those of *defense* and *offense*. Although these categories have been articulated in other ways by others in the intelligence community, viewing counterintelligence this way enables a more defined picture to emerge. For instance, the U.S. Marine Corps presents a taxonomy of counterintelligence along the lines of: “[1] operations; [2] investigations; [3] collection and reporting; and [4] analysis, production, and dissemination.”^[13]

Nevertheless, by viewing counterintelligence according to the two categories advocated here—defense and offense—we see that defensive counterintelligence gathers together those activities that contribute to deterrence and detection, whereas offensive counterintelligence is comprised of those activities that contribute to detection, deception, and neutralization. The reason detection has been included in both categories is because its role can be to provide a means that secures information and the facilities that hold that information, as well as “hunting” those who have breached those controls.



U.S. Marine Corps model with overlapping relationships that makes no real distinction.

Courtesy of the author.



The preferred defensive/offensive model for counterintelligence.

Courtesy of the author.

Figures 2.2 and 2.3 show the relationship between the two taxonomic models just described—figure 2.2 is the U.S. Marine Corps model and figure 2.3 is the preferred model. The reason the defensive/offensive model is preferred over the U.S. Marine Corps model is that each of the four functions described in the Marine Corps model can be part of both defensive and offensive, and hence the model makes no real distinction. As such, viewing it the way the Marine Corps has done raises the question as to how these functions are employed, as opposed to the clarity provided in the defensive/offensive model (figure 2.3). Under the defensive/offensive model, these four functions simply become *methods* of achieving the mission's objective—that is, to defend or go on the offensive. Arguably, this model is equally applicable to the five types of counterintelligence that are about to be

discussed—national security, military, law enforcement, business, and private.

TYPОLOGY OF COUNTERINTELLIGENCE

Introduction

One way to understand counterintelligence is by examining its typology. Counterintelligence types are based largely on the environment in which the agency operates. As such, there are five major counterintelligence types: national security, military, law enforcement, business, and private. However, having defined these types it is important to note there can be substantial overlap—for example, an investigation into the leaking of information regarding a troop deployment to a foreign country would be of interest to military intelligence units as well as agencies involved in national security, and perhaps some private security firms operating in the country. In addition to the typological overlap, the same functions—defensive and offensive—are used by each intelligence type.

Take for example the U.S. intelligence community. At the time of writing, the intelligence community was structured in an alliance that comprised seventeen agencies, all of which came under the control of the executive branch of government.^[14] Although these agencies worked individually on cases, they may work collaboratively in sharing resources, expertise, and information depending on the issue under investigation. While these agencies are intelligence focused, many have dedicated units devoted to counterintelligence or, at least, counterintelligence functions that are performed within the agency. In alphabetical order, these agencies are:

1. Air Force Intelligence;
2. Army Intelligence;
3. Central Intelligence Agency;
4. Coast Guard Intelligence;
5. Defense Intelligence Agency;

6. Department of Energy, Department of Intelligence and Counterintelligence;
7. Department of Homeland Security, Intelligence and Analysis;
8. Department of State, Intelligence and Research;
9. Department of the Treasury, Office of Intelligence and Analysis;
10. Drug Enforcement Administration;
11. Federal Bureau of Investigation;
12. Marine Corps Intelligence;
13. National Geospatial-Intelligence Agency;
14. National Reconnaissance Office;
15. National Security Agency;
16. Navy Intelligence; and
17. Office of the Director of National Intelligence.

Opposing Forces

If counterintelligence is generally concerned with identifying areas of weakness within an agency that could be exploited by those hostile to the agency (or its client), it warrants discussion as to who these persons or entities might be. A term commonly used in counterintelligence circles is *foreign intelligence service*, or FIS for short. Although the word *foreign* is used, it is synonymous for an *opposing force* (OPFOR) or the *opposition*, whoever or whatever that may be.

The opposition may be a country with regard to national security intelligence, or another nation's military in relation to military intelligence, and so on with regard to other types of intelligence. The opposition may be a traitor who works within the agency or a transnational group, such as a terrorist cell or a criminal enterprise. Opposition may also include an insurgent group that opposes government authority through criminal, paramilitary, or guerrilla methods.

Security Intelligence—Intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be

engaged in espionage, sabotage, subversion or terrorism.*

* U.S. Marine Corps, *MCWP 2-14, Counterintelligence*, G-20.

So, in this book the terms *foreign intelligence service*, *opposition*, and *perpetrator* will be used interchangeably, depending on the point being made, to denote the forces that are in conflict with the agency, or its client, that is trying to protect its secrets or secret operations. As pointed out in the section at the beginning of the book on the use of the “Key Concepts to Note,” the term *agency* will be used to denote the organization that is trying to keep its secrets safe.

National Security Counterintelligence

National security counterintelligence can be conducted by various branches of a nation’s armed forces, as well as its foreign diplomatic services. It can also be conducted by a law enforcement agency. Table 2.1 displays the national security agencies for the five-eyes intelligence alliance.

The Five-Eyes—National Security Counterintelligence Agencies

<i>Country</i>	<i>Selected Agency Examples</i>
Australia	Australian Security Intelligence Organisation (ASIO)
Britain	Security Service (MI5)
Canada	Canadian Security Intelligence Service (CSIS)
New Zealand	New Zealand Security Intelligence Service (NZSIS)
United States of America	Federal Bureau of Investigation (FBI), National Security Branch Department of Energy, Department of Intelligence and Counterintelligence Department of State, Intelligence and Research

Military Counterintelligence

Aside from the overlay between national security and military counterintelligence that was highlighted in the introduction to this section, by and large, military counterintelligence falls to units of the military itself. By way of example, table 2.2 shows two U.S. military agencies in order to demonstrate the types of units that have responsibility for counterintelligence. These are not exhaustive, but indicative, as there are numerous units that may have direct and indirect responsibility, or coordination/oversight of counterintelligence.

Selected US Military Counterintelligence Agencies

<i>Military Agency</i>	<i>Exemplar Counterintelligence Units</i>
U.S. Department of the Army	Office of the Deputy Chief of Staff for Intelligence (ODCSINT) Army Intelligence and Security Command (INSCOM) Army Tactical Counterintelligence Elements (e.g., at battalion level)
U.S. Department of the Navy	Naval Criminal Investigative Service (NCIS) Director of Intelligence, U.S. Marine Corps (DIRINT)

Law Enforcement Counterintelligence

Intelligence units involved in law enforcement intelligence are usually clear as their aims are typically well articulated—for instance, to increase the accuracy of decisions of operational commanders. In contrast, law enforcement counterintelligence units can be spread across several disjointed areas and not defined well at all, yet they still perform the function. For instance, a police force may use its detective bureau to conduct counterintelligence investigations on a case-by-case basis. That is, the matter is assigned to a detective for investigation like other alleged criminal offenses. Or the matter may fall to investigators assigned in the police force's internal investigations branch, or an external oversight body set up to make inquiries into alleged police and political corruption. So the form and role of counterintelligence may not be clearly defined, and this situation exists in the security role counterintelligence performs.

The role of securing facilities and information could be spread thin and wide in the law enforcement context. Take, for example, data security. A police force may share its computer network with other government agencies (especially at local government and state government levels). As such, data security may be the province of a data security manager who is an employee in the information technology department of government, not the police force. Building security may be the responsibility of a facilities manager who comes under the direction of not a police officer, but a supervisor in the resources branch (i.e., building management) of government. Vetting of personnel could be the role of a private sector firm contracted to carry out security and background checks, or they could be done by another law enforcement agency.

The exact configuration of a counterintelligence function within law enforcement is hard to describe as its role at the lower levels of government is commensurate with the risks posed, along with the resources management is willing and able to devote to maintaining security. However, at national levels of government, whole divisions or branches can be established—as is the case with the FBI—and these units are specifically labeled “counterintelligence.”

Business Counterintelligence

Business intelligence is concerned with the acquisition of trade-related information and commercial information that is held confidential from competing firms. It is also termed *competitor intelligence* (or *competitive intelligence*) and *corporate intelligence*.^[15] Therefore, business counterintelligence concerns itself with protecting trade information. Although the media has portrayed the unethical behavior of some business intelligence practitioners as “spying,” it is safe to say most information that is gathered in business intelligence is through open- and semi-open sources. So, by and large, the focus of intelligence activities is on monitoring what competitors are doing in the marketplace, whether that is local, regional, national, or international.

Therefore, business counterintelligence can involve units within commerce and industry that deal with issues as disparate as security, on one hand, or marketing, on the other. It can also include private investigation firms that specialize in protecting information or investigating breaches of trademarks, copyright, or trade secrets. Government intelligence agencies, both domestic and foreign, have units that monitor the transfer of information and technology. For example, the U.S. Department of Commerce's Office of Export Enforcement enforces export business regulations relating to prohibited dual-use items, such as hardware technology, software, [16] chemicals, and nuclear material.

"At what level ought company policy be decided [?] . . . At the topmost level, in other words, by the Chairman and the Board of Directors."*

* Peter Heims, *Countering Industrial Espionage* (Leatherhead, UK: 20th Century Security Education Ltd, 1982), 133.

Private Counterintelligence

Private counterintelligence can take a variety of forms, but, for the purposes of this book, it will be limited to those firms and private agents who offer their services for fee or reward. Although the term *private* implies an individual, there is some overlap in what constitutes private counterintelligence and what may be business counterintelligence, or even national security counterintelligence. The ultimate determinant is who is contracting the security agent. [17]

Private counterintelligence practitioners offer a range of specialist services that go beyond the bounds of what the average private investigator can provide. Although private investigators do feature largely, [18] often, however, the private counterintelligence practitioner comes from a background in law enforcement (including compliance or regulatory work), security, risk management, military intelligence,

military police, national security intelligence, or a country's diplomatic corps.

"Control Risks is an independent, global risk consultancy specializing in political, integrity and security risk. We help some of the most influential organizations in the world to understand and manage the risks and opportunities of operating in complex or hostile environments."^{*}

* As an example of a private counterintelligence agency, see the consulting group Control Risks. Control Risks, *About Us*, www.control-risks.com/SitePages/Home.aspx.html (accessed December 1, 2011).

Their specialties may be in fraud or background investigations, or countersurveillance and physical or information security. *Information security* should not be confused with *computer security*. Information security is used here in its widest context—that is, documents and papers, electronic data, software, knowledge, and artifacts. Practitioners may have extensive training in the use of state-of-the-art electronic audio surveillance equipment, so they are in a position to offer advice on *de-bugging* (i.e., electronic/audio countermeasure "sweeps," or *technical surveillance countermeasures*—TSCM).^[19]

They may also specialize in providing close personal protection (i.e., bodyguards) for important public figures or wealthy private persons. When Richard Nixon was president, the White House hired former New York City detective Tony Ulasewicz as a private investigator. Ulasewicz, who was a former operative in the New York Police Department's Bureau of Special Service and Investigation (BOSSI), wrote in detail about the operations he conducted on behalf of the presidency in a private capacity. This is an amazing arrangement given that the presidency had vast government investigation and intelligence resources at its disposal; nonetheless, the White House still relied on a private investigator who could be called on to conduct discreet inquiries, free of the fear of leaks.^[20]



An example of private counterintelligence (physical security)—devices that appear in circles are CCTV cameras, those in squares are floodlights, and those in diamonds are warning signs. Note also high wall and double-glazed windows with reflective foil treatment.

Courtesy of the author.

Private counterintelligence agencies could (arguably) include businesses that simply sell and install closed-circuit television (CCTV) equipment and other security hardware, but this may be too wide an interpretation. In the same vein, it could include businesses that sell or install alarms or access controls, or provide audit or similar services to track and account for pieces of information. But, again, this would a liberal interpretation. However, private counterintelligence could include practitioners who design integrated protection systems that incorporate several security functions.

Overall, private counterintelligence practitioners are viewed by some of their government counterparts as an important way to augment situations where resources are constrained by shrinking budgets. Such augmentation is done through outsourcing or contracts.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Agent;
- Applied research;
- Basic research;
- Black ops;
- Business counterintelligence;
- Case officer;
- Counterespionage;
- Counterintelligence;
- Cover;
- Covert operations;
- Customers;
- De-bugging;
- Defensive counterintelligence;
- Dummy agents;
- Espionage;
- Field officer;
- Handler;
- Intelligence;
- Law enforcement counterintelligence;
- Military counterintelligence;
- National security counterintelligence;
- Observation;
- Offensive counterintelligence;
- Open sources;
- Operations officer;
- Positive intelligence/positive collection;
- Private counterintelligence;
- Research and analysis;
- Spying;
- Sweeps; and
- Technical surveillance countermeasures.

STUDY QUESTIONS

1. Explain the role security plays in intelligence work and how it provides protection to the four intelligence types—espionage, observation, research and analysis, and covert operations.
2. Describe the difference between counterintelligence and counterespionage and explain how each element performs its mission separately, as well as how it supports the other.
3. Explain the differences between defensive counterintelligence and offensive counterintelligence. Give an example of each.
4. List the four types of counterintelligence, and then explain similarities and differences among them (perhaps use a table to facilitate this).

LEARNING ACTIVITY

Research the intelligence community at one of these levels in the jurisdiction where you live or work: local, state/province, or national. First, list the agencies and describe whether the entire agencies, or units within them, have responsibility for counterintelligence. Then, discuss whether these agencies work individually on cases or work collaboratively to share resources, expertise, and information. Finally, assess whether this structure could be improved by advancing a hypothetical structure, with explanations as to why this might provide improvements, and in what ways.

NOTES

1. United Bible Societies, *Good News Bible: Today's English Version* (London: The British Foreign and Bible Society, 1978), 142–43.
2. United Bible Societies, *Good News Bible: Today's English Version*, 143.
3. Case officers are also known as *operations officers*.
4. Though the role and skills of a recruiter and a handler can be quite different. See, Melissa Boyle Mahle, *Denial and Deception: An Insider's View of the CIA from Iran-Contra to 9/11* (New York: Nation Books, 2004), 134–35.
5. Generally, the role of a non-official cover officer is to identify people who can potentially provide information to the agency. In doing so, the assessment would include determining whether they

are willing to do so. Once these details are established, the actual recruitment is handed over to an officer with official cover. The reasoning for this is that by definition NOC officers have no connection to their government. If they were to make such an approach they would “break cover” and expose their true affiliation. See Laura Rozen, “Becoming a NOC,” in the Afterword to Valerie Plame Wilson, *Fair Game: My Life as a Spy, My Betrayal by the White House* (New York: Simon & Schuster, 2007).

6. Rozen, “Becoming a NOC,” 327.

7. For instance, in June 2011 it was reported that the CIA planned to deploy armed drones in Yemen to hunt down and kill al-Qaeda militants as part of its strategy to combat the threat posed by this organization (Siobhan Gorman and Adam Entous, “CIA Palms Yemen Drone Strikes,” *Wall Street Journal*, June 14, 2011. Also see Joby Warwick, *The Triple Agent* (New York: Doubleday, 2011) for a more detailed discussion of the uses and the targets of intelligence-driven drone attacks. Also, accounts of how certain environmental activists have used drone aircraft as part of their intelligence-gathering activities have been reported in the world’s press. See for instance “Donated Drone in Hunt for Whalers,” *The Advertiser*, Adelaide, Australia, December 26, 2011, 34.

8. By way of example, CIA analysts employed in the CIA’s Open Source Center (formerly the Foreign Broadcast Information Service) are reported to monitor an estimated five million social media postings a day in an attempt to gain an understanding of public sentiment in places like the Middle East, North Africa, and various parts of Asia, as well as other intelligence requirements. See Kimberly Dozier, “CIA Following Twitter, Facebook,” November 4, 2011, retrieved from: news.yahoo.com/ap-exclusive-cia-following-twitter-facebook-081055316.html, December, 24 2011.

9. For example, if the president or the prime minister of a country were the audience for an intelligence report, they would be referred to as the *first customer*.

10. William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: University of Kentucky Press, 2004), 13–15, and note seven at 228.

11. See, for instance, Dennis Fiery, *Out of Business: Force a Company, Business or Store to Close Its Doors . . . For Good* (Port Townsend, WA: Loompanics Unlimited, 1999)

12. Peter Grabosky and Michael Stohl, *Crime and Terrorism* (London: Sage, 2010), 53 and 64. See also Richard A. Best, Jr. and Andrew Feicket, *CRS Report for Congress: Special Operations Forces (SOF) and CIA Paramilitary Operations: Issues for Congress* (Washington, DC: Congressional Research Service, Library of Congress, December 6, 2006), 5.

13. U.S. Marine Corps, *MCWP 2-14, Counterintelligence* (Washington, DC: Department of the Navy, September 2000), 2-1.

14. Office of the Director of National Intelligence, *About the Intelligence Community*, www.intelligence.gov/about-the-intelligence-community/ (accessed November 16, 2011).

15. Leonard M. Fuld, *Competitor Intelligence: How to Get It—How to Use It* (New York: Wiley, 1985); and Richard Eells and Peter Nehemkis, *Corporate Intelligence and Espionage: A Blue Print of Corporate Decision Making* (New York: Macmillan, 1984), 78.

16. For a discussion of how certain commercial software programs and various pieces of standard computing hardware can be used as cyber weapons, see Hank Prunckun, “Bogies in the Wire: Is There a Need for Legislative Control of Cyber Weapons,” *Global Crime* 9, no. 3 (2008): 262–72.

17. In the private sector there are private intelligence agencies, so it follows that there are private agencies and persons that perform counterintelligence functions. See, for example, Eells and Nehemkis, *Corporate Intelligence and Espionage*, 57–60.

18. For instance, the British Broadcasting Corporation (BBC) was reported to have spent £310,000 hiring private investigators on more than two hundred occasions during a six-year period starting around 2006. See the *Times* (London), “BBC spent \$459,000 on Private Detectives,” *Australian*, January 25, 2012, 10.

19. The term *countermeasures* refers to control, and control in the context of counterintelligence is the ability to implement plans or actions that will mitigate risk. *Risk*, of course, is likelihood and consequence.

20. Tony Ulasewicz with Stuart A. McKeever, *The President’s Private Eye: The Journey of Detective Tony U. from N.Y.P.D. to the White House* (Westport, CT: MACSAM Publishing Company, 1990).

Chapter 3

Counterintelligence Theory

Chapter 3 3 Counterintelligence Theory

This topic examines the theory of counterintelligence by examining and discussing the following:

1. Introduction;
2. Background;
3. Rationale for developing a theory;
4. Context of the theory;
5. Method of development;
6. A grounded theory; and
7. Conclusions.

INTRODUCTION

In the realm of financial investment the concept of *risk* is used as a means of understanding *yield*. That is, if an investment has low risk, its return on investment is likely to be low as well. But this does not stop investors from longing to eliminate risk yet achieve high yields. If this metaphor is applied to intelligence work, one can see how operatives and analysts might yearn for a low-risk operation to, say, obtain information, yet still be able to yield high-grade intelligence.

“A secret is something you haven’t told yet.” —Anonymous

Unfortunately, reality suggests that the factors of low risk and high yield are not destined to meet in either finance or intelligence. Nevertheless, risk can be mitigated and in intelligence work this falls to the role of counterintelligence—to keep safe methods and operations while engaging in the activities that will ultimately produce a focused intelligence product.

But in order to reduce the risks that are characteristic of intelligence work there needs to be a theoretical base on which the practice of counterintelligence can rest. Without a theoretical foundation an efficient and effective counterintelligence program is less likely to be achieved. It follows that, if this cannot be accomplished, risk management is also not likely to be realized. So, the aim of this chapter is to put forward a theory of counterintelligence.^[1]

BACKGROUND

In the previous chapter it was pointed out that entities, whether they are individuals, corporations, the military, or even entire nations, have their safety and well-being enhanced by the protection afforded by counterintelligence. This is because counterintelligence supports the intelligence function in all its manifestations, and, in turn, intelligence supports the development of sound, rational policy.^[2] If espionage were a game, those who practice the craft of counterintelligence could be considered the game's "goal keepers." Without these practitioners the opposition would have carte blanche to raid the unprotected goal and score endless points. Without counterintelligence, the intelligence goal would be wide open to such raiders.

Given this analogy, it is not difficult to see why the role of counterintelligence is commonly thought of as *security*. In fact, Johnson pointed this out well over twenty years ago when stating, "People like to confuse counterintelligence with security."^[3] The role of counterintelligence likely has been misunderstood because there is little if any formally articulated theory of counterintelligence to guide practice.^[4] Practitioners are therefore left to formulate what they do and how they do it based on need and not on an understanding of its theoretical principles. Though there is nothing inherently wrong with a necessity-based experience approach, it does however make for a less efficient and, hence, less effective practice.

What makes intelligence work different from the research and analytic functions found in industry and commerce (which includes collecting information) is, arguably, the fact that some aspect of the

endeavor is secret.^[5] Secrecy is therefore a primary objective of counterintelligence. Johnson put it bluntly when he stated: “[counterintelligence] is aimed against intelligence, against active, hostile intelligence, against enemy spies.”^[6]

The confusion between security and counterintelligence—and also between counterintelligence and other intelligence functions, such as counterespionage—is understandable. This is perhaps why counterintelligence practitioners may have become lost in their own *wilderness of mirrors*, as James Angleton famously put it using T. S.

Eliot’s quote.^[7] But, despite recognizing this confusion, Angleton did not himself advance a theory on which counterintelligence could be based when questioned before the *Select Committee to Study Governmental Operations with respect to Intelligence Activities* (i.e., the Church Committee).^[8] Whether by design or because of the genuine absence of such a theory, Angleton missed an important opportunity to provide a matchless description. As a result, at best, we are left with a number of cobbled-together definitions that, over time, have appeared in various academic journals, professional manuals, and military field manuals, as well as in media accounts about what counterintelligence does.

RATIONALE FOR DEVELOPING A THEORY

Three recent attempts to formulate a theory of counterintelligence are those by John Ehrman,^[9] Miron Varouhaskis,^[10] and Vincent H. Bridgeman.^[11] Ehrman’s treatment resulted in not so much a theory but an essay on the importance of developing a theory, and this was acknowledged by that author: “as a foundation for theoretical work it remains incomplete.”^[12] The Varouhaskis treatment was an attempt “to provide a framework by which counterintelligence officers will be able to ultimately understand, explain, and predict the intelligence-gathering behaviors of intelligence agencies domestically and abroad, as well as the employee behavior at those agencies”^[13]—or, in other words, it was an examination of organizational behavior with counterintelligence as its focus. Bridgeman’s treatment however does make a genuine attempt to structure a theory around what he describes as three advantages

areas, or modes—denial, insight, and manipulation.^[14] Nevertheless, even this could be argued as less than a comprehensive theory. But having drawn attention to the limitations of these studies does not detract from their importance; on the contrary, these are studies of vital importance and their contribution to the literature needs to be applauded. In fact, the work of these scholars underscores the need to develop a theory: “I hope others will contribute to the development of counterintelligence theory and help further develop what this article attempts to begin.”^[15]

One could argue that there is already a considerable base of evidence within the subject literature that explains such aspects as why intelligence practitioners collect data and how these data are used to support intelligence products, and the like. There is no doubt that there has evolved a rich stockpile of information on intelligence and intelligence analysis. Likewise there is ample information on counterintelligence practice and the need for improvement.^[16] This is not in dispute. What observers like Ehrman point out, however, is the lack of a systemic presentation of these practices via a theory that explains why they are performed and how each principle relates to the other.^[17] Ehrman underscored this issue when he wrote: “Almost from the start, scholars have called for a theory of intelligence. None has been advanced. Although some authors entitle sections of their work ‘theories of intelligence,’ to my knowledge no one has proposed concepts that can be tested.”^[18] Although he wrote of intelligence in general, it applies equally to counterintelligence, and to the five types of counterintelligence discussed in chapter two—national security, military, law enforcement, business, and private.

There are likely to be tens of thousands of personnel practicing the craft of counterintelligence worldwide (in one form or another), so it is reasonable to assume that these practitioners know what to do instinctively—through practice—as there is no theoretical base reflected in the subject literature. The absence of an articulated theory, therefore, forms the rationale for this chapter—that is, what is the theoretical base that underscores counterintelligence?

CONTEXT OF THE THEORY

There are many definitions of counterintelligence and Ehrman^[19] lists a number of these in his study. Without debating the finer points of these and no doubt other definitions, it is reasonable to view counterintelligence definitions as being context specific. For instance, the definitions cited by Ehrman appear to treat counterintelligence as if it only applies to foreign policy intelligence or national security issues. However, experience has shown that, when a nation deals with, for example, a non-state actor or a transnational criminal organization, there is little demarcation between what might constitute a national security issue and, say, a law enforcement problem. Perpetrators, or targets of interest, that fall into these types of categories as “threat-agents” traverse the “radar screens” of a number of functional agencies.

William R. Johnson’s definition of counterintelligence as an activity that is “aimed against intelligence, against active, hostile intelligence, against enemy spies,”^[20] is probably as close to the mark as one could get. However, if his definition is truncated to “an activity aimed at protecting an agency’s intelligence program against an opposition’s intelligence service,” it might be closer to being what could be considered a universal definition. This is because the term “agency” could be used to mean any organization or even a nation-state. The term “opposition” could be used to mean any person or group (including a nation-state) with hostile intent. Such a definition could then be applied equally to issues that affect national security, the military, law enforcement, or even corporate and private affairs. This wide approach to defining counterintelligence is the approach taken in this book.

METHOD OF DEVELOPMENT

Although David C. Bell stated that “creating theory is an art,”^[21] it does require structured thinking. It is through structure that transparency and replicability of the methods used to conduct the research can be established. Transparency and replicability are at the core of the scientific method of inquiry,^[22] thus making it not only an art, but a science.

The research method that is widely used for developing theory is that of *grounded theory*.^[23] Grounded theory usually finds its home with qualitative researchers, as it is a method for theorizing by *grounding* the theory being developed in observation or, in other words, practice.^[24] Grounded theory method is simple but it is an iterative process. The iterative process requires the identification of themes, followed by the use of inductive logic to assign meaning to those themes.^[25] The process is equally applicable to primary or secondary data.

As there is no shortage of secondary information that either explains or discusses the counterintelligence practice, secondary data were deemed an appropriate source in developing a theory, offering both depth and breadth of information and a practical way to obtain the required information (i.e., through library research as opposed to the unrealistic approach of trying to arrange personal interviews or focus groups). Even more appealing was that these data included practitioners who wrote about their experiences, as well as academics who have studied the craft of counterintelligence. In brief, the subject literature ranged from accounts by private investigators and security operatives through to those at the highest levels of national security. The tactical issues covered in these texts ranged from the commonplace to the most complex operational issues to face counterintelligence.

Data were therefore collected from secondary sources that were in the public domain; these included scholarly journal articles and textbooks of various descriptions but mainly pertaining to counterintelligence, intelligence, investigation, and security. Military field manuals and training texts that had been used by in-service practitioners were also reviewed, as were government reports and publications and memoirs of former intelligence operatives and agency chiefs.

The question, “What constitutes the principles of counterintelligence?” was posed and then qualitative data from the sources just described were collected. From these data items key themes (or concepts) relating to counterintelligence principles were distilled. Then, connections between the themes were hypothesized, thus yielding

a set of counterintelligence principles—or, in other words, the theory of counterintelligence.

The thematic counterintelligence principles were collated and connected using the technique known as *mind mapping*.^[26] The themes were then organized into a logical structure, or model, that then formed the theory presented in the findings section below. In short, a simple step-wise process was used that was based on the original grounded theory method espoused by Barney Glaser and Anselm Strauss,^[27] which involved:

1. observation—by collecting data through empirical means;
2. theme notation—through content analysis, then identifying and recording key themes; and
3. meaning formulation—based on inductive reasoning, assigning meaning to the observed themes.

A GROUNDED THEORY

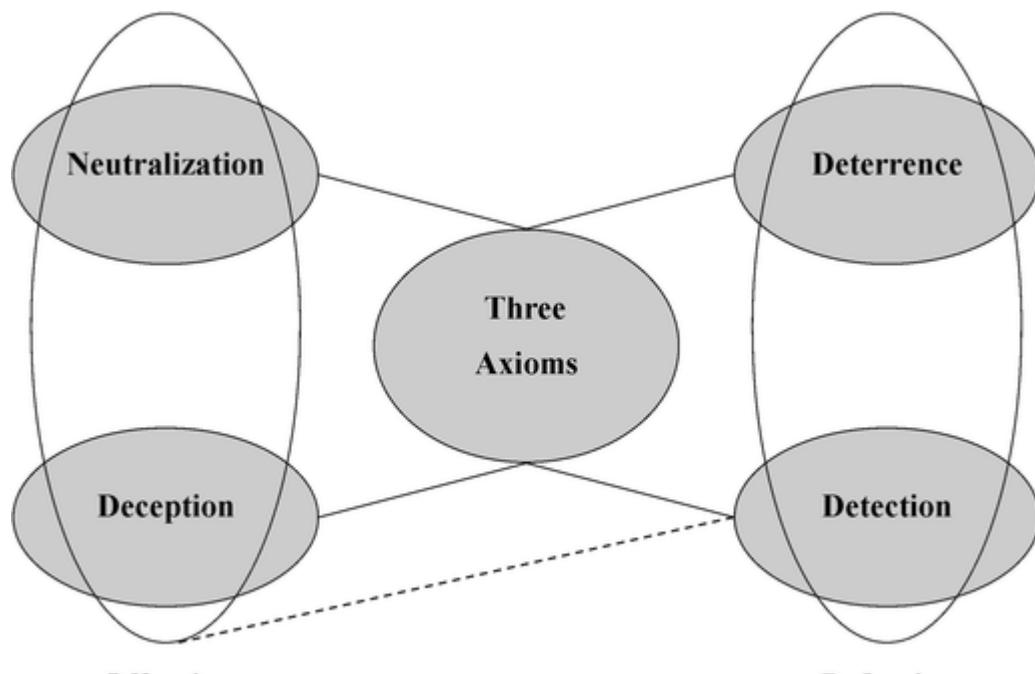
Summary of the Theoretical Model

Prima facie, the principles of counterintelligence are well established but only in practice. In fact, this theory may appear to some to be without surprise because these principles are so ubiquitous. However, they appear to have been overlooked in the same way that one “cannot see the trees for the forest.” Therefore, by using a grounded theory approach to observe practice, a theory emerges. As with all theories, it can then be tested empirically. Findings of empirical studies —ones based on valid and reliable data—can then guide good practice.

At its core, the theory of counterintelligence states that there are four principles—to deter, detect, deceive, and neutralize^[28] the opposition’s efforts to collect information, regardless of why these data are collected—whether for intelligence, subversion, sabotage, terrorism, weapons proliferation, or competitive advantage. In this sense, intelligence can include planning for any number of purposes—criminal,

national security, military, business, and private. Subversion can include such acts as rebellion, treason, and insurrection. Sabotage is damage, disruption, and incapacitation of services and process of a variety of descriptions. Terrorism can include the violent acts themselves and the means by which politically or ideologically motivated groups express their violent messages. There may be others, but for illustrative purposes this list is sufficiently wide.

These four principles have two foci—passive defense and offensive defense or, stated another way, defensive counterintelligence and offensive counterintelligence. This theory is shown in a logical model in figure 3.1. Defensive counterintelligence comprises the principles of deterrence and detection, and offensive counterintelligence encompasses the principles of deception and neutralization. Offensive counterintelligence to some degree shares the principle of detection (hence the broken line between the two foci). The model shows that there are three underpinning axioms. These axioms are essentially self-evident propositions on which the theory-dependant principles rest.



A logical model of counterintelligence.
Courtesy of the author.

Axioms

The four counterintelligence principles are contingent upon three axioms that are, in effect, statements of condition: they are deemed to be true and must exist for the theory to stand.^[29] The three axioms are now considered in turn.

Axiom of Surprise: The first axiom is that the purpose of counterintelligence is to support other intelligence functions so these functions can achieve operational surprise. It does this by establishing and maintaining secrecy. Surprise may take many forms; in the military sense it might be an attack, or in a national security sense the ability to call the bluff of a foreign leader regarding a geopolitical issue. Law enforcers may translate surprise into a scenario where they are able to provide the community with safety by being able to execute search warrants against gangs for illegal firearms. Businesses may be able to use surprise in developing and launching a new range of services or products ahead of their competitors.^[30]

Axiom of Data Collection: The second axiom is that an opposition will use various means to collect data on an agency's operations. An opposition that does not intend to collect data on the agency, by this fact itself, does not warrant a counterintelligence program. This axiom also considers that the means employed by an opposition will include *all* available avenues to collect data—ethical and unethical; legal and illegal.^[31] By grounding this axiom in this most dangerous possible attack vector, the theory therefore provides counterintelligence practitioners with the ability to formulate a number of possible solutions.

By assuming the worst case, such strategies allow analysts to identify the resources they need to deal with a range of possibilities, from the most minor situation up to and including the catastrophic.^[32] If reasoning such as this did not form part of this proposition, the possibilities would be limited, thus providing inadequate countermeasures for all risks. By incorporating a worst-case premise into this axiom it allows analysts to formulate a number of contingency plans. Should the countermeasures be circumvented by the opposition,

it also allows for analysts to estimate what resources will be needed to mitigate the effects of a successful attack, and recover from that attack.

Axiom of Targeting: An opposition will direct its data collection efforts toward obtaining information that will lay bare an agency and how it operates (as well as the entities the agency serves to protect). That is, the target of a hostile information collection operation will focus on data that will expose an agency's structure (legal and constitutional, as well as its chain of command and personnel), its sphere of operations and influence (e.g., geographic, economic, and political/social), its current capabilities (in all regards), and its future intentions. Moreover, it will target the factors that limit the agency's operations and its administrative, managerial, and functional vulnerabilities.

"As the shield is a practical response to the spear, so counterintelligence is to intelligence."*

* Frank Santi Russell, *Information Gathering in Classical Greece* (Ann Arbor: University of Michigan Press, 1999), 190.

The reason why these areas are targeted is that it allows an opposition to concentrate its efforts on vectors that will offer surprise, allows it to inflict the most damage (however defined), or allows it to leverage the most advantage in order to neutralize the agency's operations to protect itself and its clients (if any).

Principles of Defensive Counterintelligence

Principle of Deterrence: Deterrence is the ability to prevent an opposition from gaining access to information. Deterrence in this context can be both the ability to discourage an opposition from attempting to conduct a penetration operation or to deny an opposition's data collection operation once a penetration operation has been launched and is underway.

Underlying deterrence are three premises that must be met or else it will fail. The first premise is that of *unacceptable damage*. An organization must be able to deliver some form of harm upon its opposition in order for that opponent to be deterred. Deterrence in the

counterintelligence sense is different from that used in the context of, say, international foreign relations, where it is used to, for instance, contain the aggressive behavior of an opponent state through the threat of retaliation. In a counterintelligence context, deterrence is simply an agency's ability to persuade its opposing force (OPFOR) that the costs or the risks of mounting an information collection operation outweigh the benefits (in a sense, this could be construed as a form of "retaliation").

The second premise is that the threat has to be *perceived* by an opposition. If an agency wants an opposition to cease unethical or illegal data collection, then the opposition must realize that such a threat has in fact been made; it is of no value if the threat is not communicated.

The third premise is that of *credibility*—the threat must be credible to succeed. Credibility, in turn, comprises two elements, the first that the organization making the threat is *capable* of delivering the "unacceptable harm," and second that it has the *will* to do so.

Deterrence forms the bulk of what comprises defensive counterintelligence, and it mainly takes the form of physical security, information security,^[33] personnel security, and communications security. Security is the bedrock on which this principle relies. Although security does not act as an absolute deterrent, it is the keystone.

Principle of Detection: Detection is the act of noticing that an event has taken place and that the event is somehow associated with a breach or potential breach of confidential information. There are five premises that comprise the principle of detection and these are:

1. Identifying an event of concern;
2. Identifying the persons who were involved in the event;
3. Identifying the organizational association of the person(s) of interest;
4. Identifying the current location of the person(s) of interest;
and
5. Gathering the facts that indicate that the person(s) committed the event.

An *event of concern* is used here as a generic term that could be anything that could be at the center of a hostile information collection

operation. For instance, it could be the temporary removal of documents from an office for copying. It could be the passing of information from an employee to an opposition organization. Or it could be the unauthorized observation of classified information. The examples are endless, but suffice to say that the event of concern is, in law enforcement terms, the “alleged breach.” With regard to counterintelligence, it is the event that has given cause for concern.

To be able to identify such events, counterintelligence officers need to have in place systems that will bring these events to their attention. Systems might include the observations of a person in the office who has been trained to report issues of this nature; or they might be technical systems, like alarms or digital image recordings of people’s activities within the office. Regardless, without systems in place detection is diminished—the event may go unnoticed, which is after all what the hostile information collection operation is anticipating.

If an event is detected, then the perpetrator needs to also be identified. Without this, the ability of assessing the damage caused by the breach is lessened. For example, a counterintelligence officer could not conclude with confidence who was interested in the data, how it was to be used, and what ramifications this “lost” information could result in for the agency. Counterintelligence officers could nonetheless estimate the damage and the intended purpose, but this would not be as valuable as knowing the identity of the person and the details surrounding the breach.

Closely associated with detecting the person involved is identifying the person’s association with any organization (opposition or otherwise). It would be hard to envisage an individual acting solely on their own without any association with anyone else or with any other organization. Spies collect data and, in the normal course of their employ, pass it onto intelligence analysts in a headquarters setting who then analyze and synthesize this information and produce intelligence reports. Even in the case of small operations in, say, the business community, where a competitor is seeking insight into a competitor’s service or product, the data is handed from the information collector to someone who will (formally or informally) process this information and use it for planning.

Unless the case involves a private individual who has unilaterally embarked on a personal mission to, for instance, “expose” some dealings of the agency (or its client), then it is hard to conceive of a situation where no one else is involved. But even in a situation of such a “man-on-a-mission” case, they would presumably hand over the information they collect to some legal authority or the news media as a way of exposing the disagreeable behavior at the core of their mental disquiet. [34]

Regardless, it is important that the person’s association with others is identified for two reasons. It allows the counterintelligence officer to understand what needs to be done in terms of damage control, and it also helps detection and evidence gathering—given that motivation is key to many a successful counterintelligence investigation. Knowing whom one is looking for, by name and other identifying traits, increases the likelihood that the person will be located.

Finally, the ability to gather facts that directly or indirectly indicate a person’s complicity in an event of concern concludes the principle of detection. With the facts of the events in hand, the counterintelligence officer has the full picture of the event—who, what, where, when, why, and how (the five Ws and H of information gathering). Generally termed *criminalistics* or *forensics*, this includes the use of science and scientifically based techniques to locate, collect, and preserve evidence of the event. However, unlike a pure criminal investigation, the end purpose of collecting evidence in a counterintelligence investigation may not be prosecution in a court of law, but instead to mount a counteroperation (see offensive counterintelligence below) in order to obscure, confuse, or deceive the opposition.

So, with any event of concern, the ability to detect and identify the perpetrators would cause an opposition to be less inclined to attempt a hostile operation to target an agency’s information. If it does not, and the opposition is still inclined, it forces them to become far more sophisticated, which may place them beyond their technical capability, or it places them at such risk that the consequences outweigh the benefits. If the opposition does carry out a more sophisticated operation, then it makes the counterintelligence officer’s job harder, but,

paradoxically, the counterintelligence officer can deduce the likely identity of the perpetrator, and by doing so contribute to the first principle of counterintelligence theory—deterrence.

Principles of Offensive Counterintelligence

Principle of Deception: Deception involves misleading an opposition's decision makers about some aspect of the agency's operations, capabilities, or intentions (or those of its client), or concealing *who* is perpetrating an operation. The end state is to have the opposition form a view that makes them take action (or not act) so that these actions prove futile. Or deception operations may be aimed at causing confusion, thus delaying an opposition's ability to react effectively, or projecting a false understanding that sends the opposition down a path that wastes its time and resources, thus placing the agency in a far stronger position than before.^[35] Double-agent operations are classic in regards to the latter,^[36] and so is the use of dummy agents, who form a part of campaigns to sow disinformation or to project false pictures of what is truly occurring.

Legendary examples of counterintelligence deception are the various operations carried out in the lead-up to the Allied invasion of Nazi-occupied Europe during World War II. One was Operation Bodyguard. This operation was designed to convince German leadership and decision makers that the Allies' invasion would be timed later than it actually was, and that the invasion would be at locations other than the true objective of Normandy. For instance, Allied forces were well aware that the Nazis were collecting information on the preparations they were making for invasion with the view to determine the landing sites.^[37] With such intelligence, the Nazis could have mounted a formidable defense that repelled the attack, as they did in 1940 when British, French, and Belgian troops were forced to evacuate Europe from a beachhead at Dunkirk, France (i.e., Operation Dynamo).^[38]

Other examples of deception are discussed in chapter twelve (Offensive Counterintelligence: Deception) and include decoys, camouflage, and pretexts and ruses.

Principle of Neutralization: The blocking of an opposition's intelligence collection operation can be done through the method of *neutralization*. This principle is based on the concept of "defeat"—that is, collapse, failure, rout, or ruin.

The ability of an opposition to be successful with its intelligence collection operation is predicated upon the premise that it will be successful. So, this counterintelligence principle suggests that hostile operations can be thwarted by either destruction or paralysis. It can also be achieved by causing a loss of interest or enthusiasm in carrying out the operation (or continuing to carry out an operation), or by inflicting a loss of confidence in an opposition that in turn will be unable to achieve its objective (in whole or part).

Destruction in the military sense is easy to visualize—say, the destruction of forward observation posts, whether they are manned or electronic, or the killing of reconnaissance forces sent forward to reconnoiter. However, in other intelligence operations it might be the arrest of a spy cell or the transfer of a suspected spy to a remote office or location where they have no access to classified data (e.g., where not all the elements of *detection* have been established).

Although neutralization by paralysis is not as dramatic as destruction, it can be as effective. With paralysis an agency must be able to cause an opposition to halt any actions that might lead it to gain access to classified or sensitive information (or further access if already underway). Unlike destruction, where "demolition" of the operation is the goal, paralysis is concerned only with inflicting a temporary disruption of, say, a key process or a temporary disruption to communications so that direction, leadership, coordination, or command is lost, thus dooming the operation to failure. The intent is to cause the abandonment of the operation and the dismantling of, perhaps, a spy ring, by the opposition to avoid detection. Paralysis can be actions that are initiated by an agency as a preemptive measure to flush out an opposition operative or as part of a counterintelligence investigation.

It could be argued that destruction and paralysis are defensive counterintelligence strategies, whereas loss of interest and loss of confidence could be classified as offensive. For instance, loss of interest

is predicated on the notion that, if an agency can project the belief that the financial, political, or other costs of collecting the information are greater than the benefits of collecting the information by legal or ethical means, it will cause an opposition to lose interest in the operation. Another approach to causing a loss of interest is if the agency can project the belief that the value of the information is so low that it is not worth collecting, or by presenting a more tempting alternative, which might also form part of a deception strategy.

Causing a loss of confidence is a more esoteric method. It involves an organization being able to inflict upon an opposition's operative an event or set of events that cause that operative (or his master controller) to become dysfunctional to the point that he is either detected or is paralyzed to the point that he is ineffective. Take, for example, two business competitors aggressively vying for the same market. If an agency can erode the opposition's faith in their operative's ability to succeed, defeat will occur.

Methods for neutralization are numerous but the standout is the one made classic in the fictional spy genre of counterespionage. Counterespionage "calls for the engineering of complex strategies that deliberately put one's agent(s) in contact with an adversary's intelligence personnel. This is done so that an adversary can be fed with disinformation which should lead to confusion, thus disrupting the adversary and allowing the perpetrator to prosper."^[39] Accordingly, "counterespionage is like putting a virus into the bloodstream of the enemy."^[40]

CONCLUSIONS

If we return to the analogy of financial investment, one could argue that anyone promoting the notion of a low-risk but high-yield investment is akin to the alchemist peddling the idea he can turn lead into gold. Extending the financial analogy to intelligence work, one would be hard pressed to argue that running an intelligence operation, or conducting a secret research project, could be performed without the need to mitigate risk.

In order to provide utility to the support of sound counterintelligence practices, this study sought to formulate a theory of counterintelligence that was grounded in empirical observation. The study used secondary data from the subject literature as the basis for its observations.

What can be concluded from these findings? First and foremost is the fact that counterintelligence is more than a security function. It has at its core analysis. The craft of counterintelligence could not function efficiently or effectively without producing policy options that are based on fact and reason. Reasoned argument is, in essence, analysis. So, counterintelligence practice needs to be based on analytic output. This may in turn join together with the research function of positive intelligence, and perhaps it should as a matter of course, as the two could work hand in glove to achieve the same overall objective.

As for the practice aspects that counterintelligence analytics informs, these too are more than traditional security. The theory states that defensive measures constitute only half of the practice—deterrence and detection. However, these principles of counterintelligence are also more than simply “blunting the opposition’s ability to,” as the saying goes. These defensive functions need to dovetail with the offensive side of the craft—to deceive and to neutralize.

With regard to offensive counterintelligence, the theory highlights the active role it plays in misleading an opposition’s decision makers through deception and in destroying or paralyzing the opposition’s ability to continue with its intelligence operation. Neither of these functions can be effectively performed without considering the defensive functions interaction. Without such a theoretical understanding, a successful agency counterintelligence program would be hamstrung.

Nevertheless, by viewing counterintelligence according to the two foci put forward here—defense and offense—we see that defensive counterintelligence gathers together those activities that contribute to deterrence and detection, whereas offensive counterintelligence is comprised of those activities that contribute to deception and neutralization. But, having said that, detection may also be included as part of offensive counterintelligence. The reason detection can be included in both categories is because its role can be to provide a means

that secures information and the facilities that holds these data, as well as “hunting” those who have breached those controls.

In sum, this theory of counterintelligence is not one that could be described as being conceptually dense but nonetheless it is one that clearly articulates the four principles that explain why counterintelligence practice is performed as it is or, arguably, as it should be. It also presents the three axioms that lay the conditions on which these principles rely. Therefore, an understanding of the relationship between theory and practice can be used not only to improve a counterintelligence program’s performance but to help avoid catastrophic security failures (or penetrations).

Theory can do this by providing scholars with the ability to formulate hypotheses that can be tested: for example, *a purely defensive approach to protecting information is less effective than one that incorporates offensive measures*. Because this is a universal theory of counterintelligence, it allows the context to be varied so it too can be tested: for instance, *a purely defensive approach to protecting national security information is less effective than one that incorporates offensive measures, but, in a business context, incorporating an offensive role will be counterproductive*. Using such hypotheses, scholars can then define variables and operationalize them. Take the first hypothesis above as an example: *offensive measures* could be operationalized into, say, double-agents, agents provocateurs, “sleepers,” walk-ins, or any number of other manifestations of the concept.

Finally, having a basis to explain why and how counterintelligence practitioners carry out their craft in a testable form also gives rise to the possibility

of exploring metrics that could be used to measure counterintelligence processes, outputs, and outcomes.

“Intelligence is . . . not a form of clairvoyance used to predict the future but an exact science based on sound quantitative and qualitative research methods. Intelligence enables analysts to present solutions or options to decision makers based on defensible conclusions.”^[41] The same is true for counterintelligence. With what is advanced here the

profession may continue to refine the theoretical base that underpins the craft. All being well, one would anticipate that, in the fullness of time, this and other yet to be articulated counterintelligence theories will spawn better policy options. These policy options will therefore be based on defensible conclusions that are grounded in empirical research.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Deception;
- Detection;
- Deterrence;
- Event of concern; and
- Neutralization.

STUDY QUESTIONS

1. List the three underlying assumptions that support counterintelligence theory.
2. List the four parts that comprise the theory of counterintelligence.
3. List the three premises that comprise the theory of deterrence.
4. List the five premises that comprise the theory of detection.

LEARNING ACTIVITY

Consider the concept of an *event of concern*. Using either your current workplace or a notional one, brainstorm at least five (5) situations that could be considered as events of concern. List the event and next to it the reasoning for it being of concern. Rank them in terms of risk (i.e., likelihood and consequence) from highest at the top to lowest at the bottom. Select the highest ranking event and a system that will bring

this type of event to the attention of a counterintelligence officer. If there is already such a system in place for this, evaluate it in terms of whether it could be improved from the point of view of effectiveness and/or efficiency.

NOTES

1. This chapter is based on my study: Hank Prunckun, "A Grounded Theory of Counterintelligence," *American Intelligence Journal* 29, no. 2 (2011): 6–15.
2. Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* (Washington, DC: Brassey's, 1995).
3. William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer* (Bethesda, MD: Stone Trail Press, 1987), 1; and William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer* (Washington, DC: Georgetown University Press, 2009), 1.
4. John Ehrman, "Toward a Theory of Counterintelligence: What Are We Talking About When We Talk About Counterintelligence?" *Studies in Intelligence* 53, no. 2 (2009): 18.
5. Patrick F. Walsh, *Intelligence and Intelligence Analysis* (New York: Routledge, 2011).
6. Johnson, *Thwarting Enemies at Home and Abroad* (1987), 2; and Johnson, *Thwarting Enemies at Home and Abroad* (2009), 2.
7. Michael Holzman, *James Jesus Angleton, the CIA, and the Craft of Counterintelligence* (Amherst: University of Massachusetts Press, 2008), 3.
8. Holzman, *James Jesus Angleton, the CIA, and the Craft of Counterintelligence*, 3.
9. Ehrman, "Toward a Theory of Counterintelligence."
10. Miron Varouhakis, "An Institutional-Level Theoretical Approach for Counterintelligence," *International Journal of Intelligence and Counterintelligence* 24, no. 3 (2011).
11. Vincent H. Bridgeman, "Defense Counterintelligence, Reconceptualization," Jennifer E. Sims and Burton Gerber, editors, *Vaults, Mirrors and Masks: Rediscovering U.S. Counterintelligence* (Washington, DC: Georgetown University Press, 2009).
12. Ehrman, "Toward a Theory of Counterintelligence," 18.
13. Varouhakis, "An Institutional-Level Theoretical Approach for Counterintelligence," 498.
14. Bridgeman, "Defense Counterintelligence, Reconceptualization," 128.
15. Ehrman, "Toward a Theory of Counterintelligence," 18.
16. Frederick L. Wetterling, "Counterintelligence: The Broken Triad," *International Journal of Intelligence and Counterintelligence* 13, no. 3 (2000).
17. Although there have been scholarly attempts that have achieved some levels of success in advancing work toward a theory, these have not achieved what could be considered full success. See, for instance, Michelle K. Van Cleave, *Counterintelligence and National Security* (Washington, DC: National Defense University Press, 2007). Nevertheless, this is a praiseworthy piece of research.

- [18.](#) Ehrman, “Toward a Theory of Counterintelligence.” See, for instance, the critical appraisal of some existing models of intelligence and whether these accommodate a clear understanding of counterintelligence, by Petrus “Beer” Duvenage and Michael Hough, “The Conceptual Structuring of the Intelligence and the Counterintelligence Processes: Enduring Holy Grails or Crumbling Axioms—Quo Vadis?,” *Strategic Review for Southern Africa* 33, no. 1 (May 2011): 29–77.
- [19.](#) David Kahn, “An Historical Theory of Intelligence,” *Intelligence and National Security* 16, no. 3 (2001): 79.
- [20.](#) Johnson, *Thwarting Enemies at Home and Abroad* (1987), 2; and Johnson, *Thwarting Enemies at Home and Abroad* (2009), 2.
- [21.](#) David C. Bell, *Constructing Social Theory* (Lanham, MD: Rowman & Littlefield, 2009), 61.
- [22.](#) Hank Prunckun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis* (Lanham, MD: Scarecrow Press, 2010).
- [23.](#) Anselm Strauss and Juliet Corbin, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques* (Newbury Park, CA: Sage, 1990).
- [24.](#) Earl Babbie, *The Practice of Social Research*, 9th ed. (Belmont, CA: Wadsworth, 2001).
- [25.](#) Bell, *Constructing Social Theory*.
- [26.](#) Tony Buzan, *How to Mind Map* (London: Thorsons, 2002).
- [27.](#) Barney Glaser and Anselm Strauss, *The Discovery of Grounded Theory* (Chicago: Aldine, 1967).
- [28.](#) As this is an examination into a universal theory of counterintelligence, these four terms have been adapted. Scholars may find synonyms for these terms in other counterintelligence contexts, such as military, national security, law enforcement, and business contexts. For instance, the term *detection* may equate to *identification*, and so forth. The temptation is to resist debate that might draw one down to terminology, so that the discussion remains at a high level, focused on the overall theory.
- [29.](#) John Hospers, *An Introduction to Philosophical Analysis*, 2nd ed. (London: Routledge and Kegan Paul, 1973).
- [30.](#) Alain Franqu, “The Use of Counterintelligence, Security and Countermeasures,” in *Managing Frontiers in Competitive Intelligence*, ed. Craig Fleisher and David Blenkhorn (Westport CT: Greenwood, 2001).
- [31.](#) Robin W. Winks, *Cloak and Gown: Scholars in the Secret War* (New York: Morrow, 1987), 328.
- [32.](#) Godson, *Dirty Tricks or Trump Cards*, 231.
- [33.](#) *Information security* should not be confused with *computer security*. Information security is used in this book in its widest form; that is, documents and papers, electronic data, software, knowledge, and artifacts.
- [34.](#) See, for example, Andrew Fowler, *The Most Dangerous Man in the World: How One Hacker Ended Corporate and Government Secrecy Forever* (New York: Skyhorse Publishing, 2011).
- [35.](#) For in-depth examples and case studies involving deception, see, for instance, Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (London: Phoenix, 2005), and Jon Latimer, *Deception in War* (Woodstock, NY: The Overlook Press, 2001). See also Melrose M. Bryant, *Deception in Warfare: Selected References from Air University Library Collection, Special Bibliography No. 275* (Maxwell Air Force Base, AL: U.S. Air Force, 1985).

36. Winks, *Cloak and Gown*, 342–43.
37. William Stevenson, *A Man Called Intrepid: The Secret War 1939–1945* (London: Book Club Associates, 1976).
38. W. J. R. Gardner, ed., *The Evacuation from Dunkirk: “Operation Dynamo,” 26 May–4 June 1940* (London: Frank Cass Publishers, 2000).
39. Prunckun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, 10.
40. Winks, *Cloak and Gown*, 422.
41. Prunckun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, 2.

Chapter 4

Defensive Counterintelligence Planning

Chapter 4 4 Defensive Counterintelligence Planning

This topic discusses the analytic techniques that apply to defensive counterintelligence planning:

1. Rationale for planning;
2. Threat analysis;
3. Vulnerability analysis;
4. Risk analysis; and
5. Prevention, preparation, response, and recovery planning.

RATIONALE FOR PLANNING

The foundation of any plan rests on the cogitative process to produce a strategy that leads to the achievement of a goal. It also includes the mechanical process of producing some form of document that records this thinking. In terms of a defensive counterintelligence plan, the goal is to make secure information available to only those with a need to know.

Why plan? Without a plan it is difficult to apply the limited resources at the disposal of the counterintelligence coordinator across the spectrum of information that lies within the agency that may require protection, and to do this across all the weeks of a year. In this sense a plan is a document that logically and progressively takes the reader from the general to the specific and explains why and how the conclusions drawn have been reached. The term *transparency* is used in this context—the reader can see and understand the rationale and logic used to do what is being suggested. Plans contain a number of elements, or sections, and each is designed to step the reader through the thinking of the planner.

With regard to developing a plan for an agency's defensive counterintelligence needs, the first step is to conduct a threat analysis. This is the first of three integrated phases. The two subsequent phases are vulnerability analysis and risk analysis. The results of these three pieces of analytic work lay the groundwork for crafting a plan that addresses *prevention, preparation, response, and recovery* (PPRR). In other words, all of the methods contained within this chapter are intrinsically linked and act as building blocks to a comprehensive way to develop a plan. Without a plan, an agency's

resources may be allocated to areas of low risk and/or low impact, leaving high-risk and/or high-impact areas exposed.

The steps in developing a counterintelligence plan are:

1. Identify and locate sensitive information that requires protection;
2. Identify the threat-agent(s);
3. Explore vulnerabilities to the threat(s);
4. Gauge the likelihood that the threat(s) will eventuate;
5. Assess the consequence the threat(s) will have; and
6. Construct a PPRR plan.

Consider the following example of how these steps are applied in practice:

1. Classification—Identify all sensitive information and assign a classification level to these data;
2. Threat—interception of signals at an overseas embassy in an unfriendly country;
3. Vulnerability—the agency's wireless communications located within the embassy;
4. Likelihood—greater than 90 percent probability;
5. Consequence—moderate to severe compromise of classified data; and
6. PPRR—develop a plan that does four things: attempts to prevent such an interception (prevention); prepares the agency for such an interception if prevention measures fail (preparedness); guides the agency in the actions it needs to take to respond to an interception that is underway or has occurred (response); and suggests what needs to be done to aid the agency's client in recovering once the interception incident has passed (recovery). Recovery could be thought of also as a business continuity plan, but with information; this will be in the vein of a "damage control" plan too.

Although discussed here as a packaged approach to counterintelligence, any one of these analyses can be carried out on its own, or applied to problems other than protecting secrets. For instance, a risk assessment could be conducted in relation to a person or group acting criminally.

IDENTIFY SENSITIVE INFORMATION

One of the most important considerations in developing a defensive counterintelligence plan is identifying the information that needs protecting along with the places these data are held. In chapter eight the classification process is discussed, as are the types of information that require protecting and the levels of security that can be assigned to each data item. A reading of chapter eight is recommended to understand the concerns involved in this issue.

Nevertheless, guarding sensitive information is at the heart of the defensive planning process, and the ability to apply countermeasures (or risk treatment options), which will be discussed later in this chapter, requires that all sensitive information be identified in the first instance. This simple argument sums up the situation: (1) if data are not identified and classified, treatment options cannot be applied to protect them; and (2) if sensitive data are unprotected, the information is as good as in the hands of the opposition.

THREAT ANALYSIS

In some agencies the term *threat* has been used loosely to mean *risk* or *hazard*, so some clarification is needed. Essentially, a threat is one person's resolve to inflict harm on another. Threats can be made (by a *threat-agent*) against most entities—people, organizations, and nations. The potential harm can be in many forms and can be suffered either physically or emotionally/mentally. A threat-agent does not have to openly declare its resolve to cause harm in order to constitute a threat, though explicit words or actions make it easier for field operatives to identify the threat-agent and for analysts to assess the threat.

So, it is clear that threats are projected by threat-agents, whereas *risks* are the function of likelihood and consequence, and a *hazard* is a nature-induced event or naturally occurring danger. Risk and hazards will be discussed further on in this chapter, but it is important to note the difference and not be tempted to blend the terms as if they were synonymous.

Threat analysis acknowledges two key factors—that there needs to be a threat-agent (which could be anything from a physical substance to a person or a body corporate/organization) and an object of the threat (i.e., the target, which does not have to be a material target—such as a shopping mall or an individual—but can be an intangible such as a threat to national security or the security of a particular jurisdiction or an event). Stated another way, a threat-agent who has intent and capability must be able to harm something. By way of example, a threat-agent could be an employee who is intent on and capable of

passing on classified trade information to a business competitor. Or like the group of ten Russian sleepers who were expelled from the United States in 2010 for spying—it was determined that they had intent and capability to obtain sensitive information about matters of strategic interest to their nation.^[1] And so on.

Identifying Levels of Threat-Agents

Listed below are three broadband sources of threat-agents. This list is intended to present an illustrative hierarchy of typical threat-agents that an agency may confront in the course of conducting its “business.” Steps taken to thwart intelligence collection from, for example, a Level II threat-agent would be sufficient to guard against any attempt by the inferior Level III threat-agent, but not the reverse. This is an important factor to remember. It is critical for agencies to determine where their threat vectors originate before deciding on the range and depth of countermeasures (i.e., risk treatment options) they will require. Furthermore, an agency’s threat-agent level may change from time to time due to the dynamics of its operations. Consequently, an agency’s security needs will also need to either escalate or abate in response to these changing conditions.

- **Level I Threat-Agent.** Surveillance by a foreign government’s security or intelligence agency, or surveillance by an investigation company staffed by former law enforcement or intelligence personnel.
- **Level II Threat-Agent.** Surveillance by an organized criminal group, a well-financed terrorist or extremist group, a foreign or domestic business competitor employing a “spy-for-hire,” a private investigator acting on behalf of a party interested in the affairs of the agency, or other professional fact finders such as an investigative journalist.
- **Level III Threat-Agent.** Nonprofessional surveillance by, for example, an employee, a business associate or competitor, or another interested individual or group acting on their own with no formal training in investigation or information gathering, or an unsophisticated criminal.

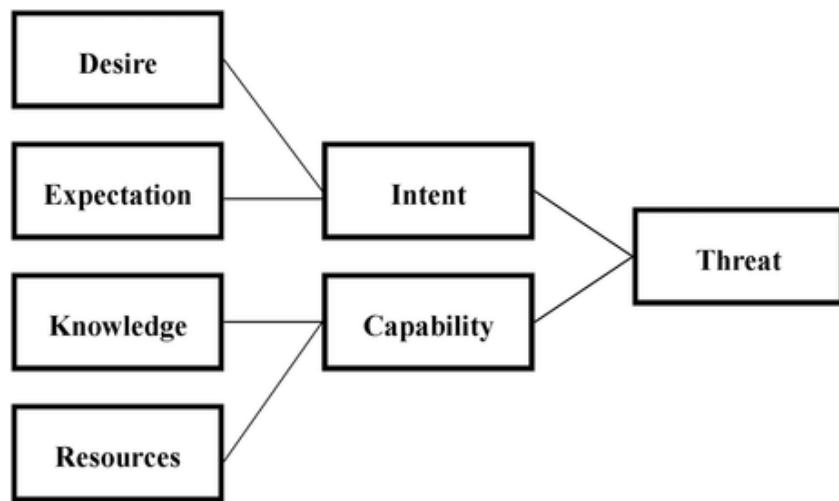
Logical Model for Threat

When counterintelligence coordinators assess a threat-agent, they are gauging whether the agent has *intent* and *capability* to harm a target. To determine whether the threat-agent has intent and capability, analysts need to

establish two elements for each of these factors: *desire* and *expectation* (or *ability*) for intent, and *knowledge* and *resources* for capability. These considerations are shown diagrammatically in a logical model in figure 4.1 below. Threat can also be expressed as an equation in the form of:

$$\text{threat} = (\text{desire} + \text{expectation}) + (\text{knowledge} + \text{resources}).$$

It is important to note that threats can only originate from a threat-agent acting in an offensive role—that is, humans (but can include organizations in the broad sense of the term as these entities are controlled and directed by humans—e.g., nation-states, armed forces, corporations, etc.). Threats, by definition, cannot originate from a nonhuman source, such as fire, flood, storm, wind, earthquake, and other forms of nature-induced events, as well as events caused by accident, mishap, misfortune, coincidence, and chance. These are *hazards*. Hazards need to be considered as part of any counterintelligence plan, but this is done at the risk assessment phase.



Logical Model for Threat.

Courtesy of the author.

Turning to intent and capability in detail, desire can be described as the threat-agent's enthusiasm to cause harm in pursuit of his or her goal. Expectation is the confidence the threat-agent has that they will achieve their goal if their plan is carried out. Knowledge is having information that will allow the threat-agent to use or construct devices, or carry out processes, that are necessary for achieving their goal. Resources include skills (or experience) and materials needed to action their plan.

The actual carrying out of a threat analysis will vary from agency to agency as the context of each agency's mission will be different. Nevertheless, a step-by-step process might look something like this:

1. Identify the categories from which threats may manifest. These can be called *threat communities* and this concept is discussed later in this chapter. Examples of possible threat communities could be along these lines: internal and external, with each of these categories being broken down into subcategories—internal may be permanent employees, contract agents, ancillary staff, temporary staff, and others. The same can be done for the external category. The best way to create such a list is to either brainstorm using a small group of knowledgeable people or, if working alone, by using a mind map.
2. Collate the categories and subcategories into a list using headings and subheadings for ease of handling.
3. The lowest level of headings in the collated list (in the above example, it would be subheading) will be the areas that the threat assessment will need to examine. If the subheading of *temporary staff* is selected as a starting point, the counterintelligence investigator would then take each of the four criteria (desire, expectation, knowledge, and resources) and gauge whether that subcategory, as a whole, contains evidence of any of these four factors. If the answer is yes, but only to one or two factors, then the subcategory can be said not to pose a threat. If the assessment shows evidence that three factors are present, then it might be placed on a “watch list” in case the situation changes. If all four factors are present, then by definition it poses a threat and a closer look is warranted. But having said that it is a threat does not mean it actually is. The assessment is merely an analytical method for helping counterintelligence investigators focus their efforts, and their agency's resources, where they are most beneficial and, hence, the next step.
4. Inquiries will need to be conducted to gather information as to whether each of the four factors is of such a magnitude that a reasonable person would draw this conclusion. It is important that all information is weighted in this process and not “cherry-picked” to include only information to support a particular point of view—this is both unethical and operationally dangerous. A balanced view needs to be formed so that the correct conclusion can be drawn. If, on balance, the evidence does not lead one to draw such a conclusion, a watching brief may be raised. Sources of information can be both primary and secondary, and they can

be from either the public domain, private sector, or confidential/classified. An appropriate information collection plan and research method for analyzing these data needs to be crafted as per any intelligence project. A good text for guiding the counterintelligence investigator through this research process is my book entitled *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*.^[2]

Once the formal assessment process is complete, a summary can be created using a simple table that shows the results. This is a handy way for displaying the results so decision makers can understand the outcome of the assessment without burdening them with large amounts of narrative. A model for calculating threats might look something like table 4.1.

**Example of a Threat Summary: Threat
Community Summary for
Former Employees of Manly Pharmaceutical
Corporation**

Scale	Scores	Tally
	<i>Desire</i>	
Negligible	1	
Minimum	2	2
Medium	3	
High	4	
Acute	5	
	<i>Expectation</i>	
Negligible	1	
Minimum	2	
Medium	3	
High	4	
Acute	5	
Total Intent		3
	<i>Knowledge</i>	
Negligible	1	

Minimum	2	
Medium	3	
High	4	4
Acute	5	
<i>Resources</i>		
Negligible	1	
Minimum	2	
Medium	3	
High	4	4
Acute	5	
Total Capability		8
Threat Coefficient		11

Although models do not eliminate subjectivity, using a model forces counterintelligence investigators to be transparent about how they calculate threat and, in doing so, positions them to defend their conclusions. You will note that there are no conditions assigned to what constitutes a high level of intent. That is because this needs to be developed in the analytic process that leads to the assignment of the coefficient. Ideally, some form of conditioning statement would be attached to each of these categories so that the decision maker knows what is meant by high intent, low intent, and so forth. An example of how such a conditioning statement scale could be constructed is shown in table 4.5 later in the chapter.

In addition, models do not eliminate miscalculations because of inadvertent skewing. Note in table 4.1 that intent is calculated by adding desire with expectation, and, in turn, this sum is added to the sum of knowledge and resources (and will range from a low of 4 to a maximum of 20). The process of adding limits the spread of values, whereas the process of multiplying any of these scores would increase the values. For instance, if all scores were multiplied—that is, substituting multiplication for addition—as per the equation, the range would be spread from 1 to 625.

The precision of this wide range of values diminishes the counterintelligence investigator's ability to accurately determine either intent or capability. Therefore, it is suggested that adding all values rather than multiplying them will reduce the spread and, therefore, maintain the threat coefficient as an *indicator*, rather than promote it as a reflection of its absolute

condition. (Even if the counterintelligence investigator multiplied desire and expectation, and knowledge and resources, but added the resulting sums, it would still yield a very wide spread—from 2 to 50; as would the opposite, that is, multiplying the sums that comprise intent and capability—from 4 to 100.)

Having said that, two additional issues need to be noted: (1) there is still a need to provide conditioning statements so that the reader of the assessment understands what is meant by a medium threat intent and capability (e.g., along the lines of table 4.5); and (2) “unknowns” are not accommodated in this model.

The threat coefficient obtained from this analysis is then compared against a reference table to gauge where it sits on a continuum of danger. The scale suggested below in table 4.2 can be varied with additional qualifiers or it can be collapsed if the number is deemed too many. Likewise, how the incremental breakdown of coefficients is determined will depend on whether the agency is willing to accept the risk that a threat-agent may slip under its gaze by raising the categories of negligible and minimum. In the end, their number and their descriptors need to make sense in the context of the asset being protected. That is, each of the descriptors needs to have a conditioning statement attached to it to define what is meant by negligible, minimum, medium, high, and acute. See table 4.5 as an example.

Example of a Threat Coefficient Scale

<i>Threat Level</i>	<i>Coefficient</i>
Negligible	4–6
Minimum	7–10
Medium	11–15
High	16–18
Acute	19–20

Threats are context dependent, and what forms a threat in a business setting does not necessarily form a threat in a military or national security setting (though the opposite may be true). Bearing this in mind, an example from national security will be discussed to illustrate the threat analysis method.

In a military situation, say, a low-intensity conflict, threats can range from spontaneous street demonstrations by the local population, at one end, through to terrorist bombing and confrontations with insurgent or guerrilla

units at the other end. The techniques for assessing the elements of a threat can vary depending on the issue under investigation and the counterintelligence investigator's personal preference or the agency's policy.

Nevertheless, the approach is to weight each element using some verifiable means that is open to third-party scrutiny. For instance, an analyst may use a force field analysis to judge whether there are threats in Country Q associated with a low-intensity campaign being prosecuted by friendly military units. Likewise, the nominal group technique could be employed not only to assess the four elements of a threat (i.e., desire, expectation, knowledge, and resources), but to generate a list of possible threat-agents (i.e., belligerents) to compare the elements against each other. Participants for such a group could be drawn from subject experts or operational specialists, or a mixture of both. Some of the other analytic techniques discussed in chapter ten of my handbook of intelligence analysis^[3] can also be used, but there is no firm rule on how this analysis should be done.

One way of considering the context for threats is to conceptualize it as *threat communities*. Some examples of threat communities in the realm of malicious human threats include:

External

- competitors;
- common thieves;
- criminals and criminal groups;
- international or transnational terrorists;
- domestic terrorists;
- insurgents and guerrillas;
- anarchists;
- cyber-criminals and cyber-vandals;
- rights campaigners;
- spies-for-hire (i.e., former law enforcement, security, or intelligence personal who have turned private operatives); and
- foreign government intelligence services.

Internal

- principals of the business or agency;
- associates;
- current employees;

- former employees;
- temporary staff; and
- contractors.

These threat communities can be subdivided into more distinct groups if there is a need—for instance, rights campaigners can be classified into political activists, religious activists, and single-issue activists (anti-taxation, antiwhaling, animal rights, antiabortion, etc.). But bear in mind that membership in one threat community (or subcommunity) does not exclude that person from being a member of another, or several other, threat communities.

When compiling a threat profile, targets can and should be considered in terms of their criticality, cost (either as a direct loss, or an indirect or consequential loss due to disruption), and sensitivity (e.g., compromised information). This is because targets that do not possess any of these attributes may not be considered by threat-agents with the same weight.

To better understand the “who” that comprise a threat community, counterintelligence investigators need to compile a *threat profile*. The profile needs to be adequate (perfection is rarely, if ever, obtainable) to understand the threat environment, which aids the next phase in the analytic process—that is, vulnerability analysis. In the meantime, consider the threat profile shown in table 4.3 as an example that demonstrates the important aspects of a fictitious threat-agent (the order can be rearranged to suit the counterintelligence investigator’s research project and other factors can be added if these are deemed inadequate to communicate the message).

Threat Profile for the Omen Martyrs Faction

<i>Summary Type</i>	<i>Observations</i>
Organization	
Organization	Well organized but not hierachal.
Affiliation	Autonomous.
Recruitment	Ethnic population centers.
Financing	Extortion and kidnapping the wealthy.

International connections	Training and ideological support.
Behavioral	
Motivation	Radical religious ideology.
Intent	Extensive destruction.
Tolerance to risk	High.
Self-sacrifice	Very accepting.
Willingness to inflict collateral harm	Extreme.
Operational	
Planning	Based on target acquisition intelligence through fixed and mobile surveillance, informants and open-source data.
Targets	Objects that represent Western values or people who do not ascribe to their interpretation of their faith (including other believers).
Target characteristics	Symbolic and iconic objects that afford high visibility and hence high media coverage.*
Tactics	Targets mass gathering, critical infrastructure, communications, mass transport, and distribution chains.
Weapons	Improvised explosives and small arms.
Resource Summary	
Skills and Knowledge	Attack vector dependent: Computer-based—low; Electronic/communications—moderate; Small arms—high; and Explosives—high.

* Regarding this factor, see Stratfor, *How to Look for Trouble: A Stratfor Guide to Protective Intelligence* (Austin, TX: Stratfor, 2010), 127–31.

VULNERABILITY ANALYSIS

In short, *vulnerability* is a weakness in an *asset* that can be exploited by a threat-agent. The term *asset* is being used in this context to denote a resource that requires protection and can be places and objects as well as people. But in the context of counterintelligence we are talking about information resources that require protection. So, viewed another way, vulnerability can be described as an asset's capability to withstand harm inflicted on it by a threat. Harm can

be anything from experiencing a minor nuisance event to a situation that is catastrophic.

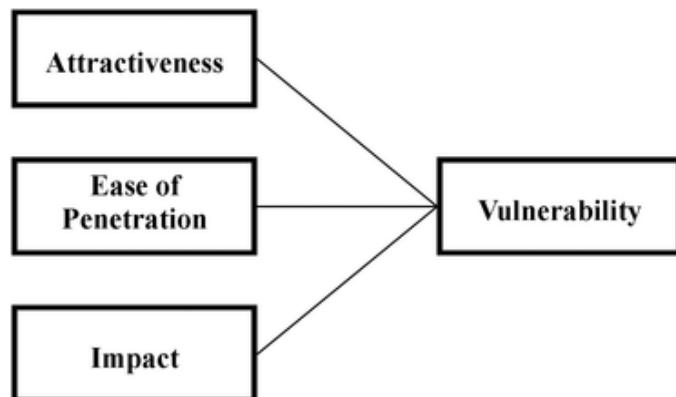
Vulnerability is a function of several factors—attractiveness of the targeted information, feasibility of carrying out a penetration, and potential impact if released. This model is shown diagrammatically in figure 4.2. Usually, these factors entail such considerations as: status of the targeted information, potential for the penetration to succeed, potential for the threat-agent to get away with the penetration, and potential to inflict loss (i.e., capitalize on the information obtained). These factors can be weighed against measures to mitigate loss and to deter or prevent penetration of an asset (e.g., through a force field analysis).

Formulae-based analyses are popular amongst law enforcement and security agencies engaged in information protection, and, although these vary from agency to agency, they all follow a basic stepwise formula:

1. Define what constitutes an information asset (corporate website, research reports, servers holding classified data, along with others);
2. Sort these assets into categories;
3. Assign a grade or level of importance to each asset; and
4. Identify potential impact on the asset if it suffers harm (i.e., unauthorized access/dissemination).

As there is no one single criterion for calculating vulnerability because each class of information asset may require special considerations to be taken into account (and there may also be agency protocols that take precedence), one general approach is to use a model such as:

$$\text{vulnerability} = \text{target information attractiveness} + \text{ease of penetration} + \text{impact}$$



Logical Model for Vulnerability.

Courtesy of the author.

To operationalize the variable *attractiveness*, the counterintelligence investigator could ask questions along the following lines and tabulate the results to insert into the model:

- Could the obtaining of the target information cause harm and therefore be of value—symbolic, monetary, or strategic? For instance, when the former Soviet Union paraded the CIA's U2 pilot Gary Francis Powers, who was shot down while conducting a reconnaissance mission in 1961, before the world's media, this was of great symbolic importance (as well as having other strategic advantages). This was because obtaining proof that the United States was conducting surveillance of the Soviet Union brought that program to an end (though it was simply displaced by satellite reconnaissance, which the Soviets engaged in also).
- Is the target information readily obtainable? Rather than answer this question in a dichotomous way (i.e., using nominal data—yes/no), ordinal data could be used to give greater precision to the overall vulnerability indictor. For example, is the information obtainable via the World Wide Web; or are the data obtainable through library research but only held in special collections in a handful of libraries; or are these data held in security containers with physical security measures?^[4] These ordinal type indictors can also be applied to the concept of harm discussed directly above.

Attractiveness needs to be placed in context with the threat-agent. For instance, a business competitor of a pharmaceutical company may see the scientific papers published by the company's scientists as very attractive.

To operationalize the concept *ease of penetration*, the analyst could ask these types of questions:

- How difficult would it be for the threat-agent to gain access to the target information? A scale from certain (as in the case of published data) to very difficult (in the case of data contained and protected by armed guards) could be constructed as in the examples cited with regard to attractiveness, above.
- Are there security measures in place (e.g., calculated on a scale of low to high deterrence, or low to high prevention)?

Vulnerability of Company's Scientific Research Expertise

Scale	Scores	Tally
<i>Attractiveness</i>		
Negligible	1	
Minimum	2	
Medium	3	
High	4	4
Acute	5	
<i>Ease of Penetration</i>		
Negligible	1	
Minimum	2	
Medium	3	
High	4	4
Acute	5	
<i>Impact</i>		
Negligible	1	
Minimum	2	
Medium	3	
High	4	4
Acute	5	
Vulnerability Coefficient		12

Questions that probe the existence and extent of controls (or lack thereof) can also be asked to gauge ease of penetration. On one hand, if there is a high degree of control effectiveness, this will usually reduce ease. On the other hand, if there is a low level of control effectiveness, it will increase ease. Counterintelligence investigators should be mindful that, with some sensitive information, even a small reduction in control effectiveness can result in a disproportionate increase in ease of penetration.

Impact could be operationalized by questions like:

- What is the basis of harm which could result as a consequence of disclosure? This is akin to attractiveness. It may be context specific, as well as graded as to the person(s) or opposition agency that the information is made available. Again, a scale for context and degree of harm could be constructed.
- In dollar terms, what would the financial impact of an unauthorized disclosure be if the information was simply obtained, but not used by the person (e.g., if the person was apprehended shortly after obtaining the data but before they were able to pass it onto others), through to a complete handover of the information and debriefing? Or it could be put in terms of days/weeks of having to reengineer business practices or operational plans because of the disclosure, or lost units of production, and the like.

Impact should not be predicated on an assumption that all penetrations are designed to result in immediate or visible harm. This may be true of an organization such as WikiLeaks, which publicly stated that its intention was to bring “important news and information to the public [via] . . . an innovative, secure and anonymous way for sources to leak information.”^[5] But it would not be true of an opposition that wants to use the information, say, in its own counterintelligence program. A template for calculating vulnerability might look something like that shown in table 4.4.

The vulnerability coefficient derived from this analysis is then compared against a reference table to gauge where it sits on the continuum of exposure or susceptibility to penetration. The scale can be increased with additional qualifiers or it could be collapsed if the number is deemed too many. In the end, the number and their descriptors need to make sense in the context of the information being protected (the left-hand and center columns of table 4.5). Qualitative descriptors (i.e., conditioning statements) can be added for each category as shown in the right-hand column of table 4.5.

Note that *consequence* is not a factor that is considered in a threat assessment. It is, however, considered in a risk assessment (see below).

Examples of Vulnerability Coefficients

Vulnerability	Coefficient	Qualifier
Negligible	1–3	<ul style="list-style-type: none"> • Can only be penetrated successfully if the threat-agent has an acute threat coefficient; or

		<ul style="list-style-type: none"> Has little or no importance; or The range of security measures makes penetration very difficult; or If penetrated, the information has little utility to cause harm.
Minimum	4–6	<ul style="list-style-type: none"> Can only be penetrated successfully if the threat-agent has a high coefficient (or greater); or Has limited importance; or The range of security measures makes penetration difficult; or If penetrated, the information has only some utility to cause harm.
Medium	7–9	<ul style="list-style-type: none"> Can only be successfully penetrated if the threat-agent has a medium coefficient (or greater); or Has reasonable amount of importance associated with it; or The range of security measures makes penetration moderately difficult; or If penetrated, the information has a moderate level of utility to cause harm.
High	10–12	<ul style="list-style-type: none"> Can only be successfully penetrated if threat-agent has a minimum threat coefficient (or greater); or Has a sizeable amount of importance associated with it; or The range of security measures makes penetration undemanding; or If penetrated, the information has a high degree of utility to cause harm.
Acute	13–15	<ul style="list-style-type: none"> Can only be successful penetrated if threat-agent has a low threat coefficient (or greater); or Has a very high level of importance associated with it; or The range of security measures is nonexistent; or If penetrated, the information will cause immediate and/or extreme harm.

RISK ANALYSIS

Risk is a function of two factors: *likelihood* and *consequence*. In some agencies the term *probability* is sometimes used instead of *likelihood*, and both are acceptable. A risk assessment can be carried out in relation to almost any

situation; it is not just for issues of grave concern. Nor is risk management solely for counterintelligence; risk analysis techniques can be applied to situations or targets that are not associated with sensitive information—for instance, counterterrorism. Nevertheless, analyzing risk allows counterintelligence investigators to recommend measures that will provide decision makers with the ability to:

- accept the risk as is; or
- treat the risk (which includes such decisions as to avoid the risk altogether, mitigate the risk, or defer the risk for another person or agency to deal with).

In counterintelligence, investigators can focus on a wide range of risks. These can vary from the minor—say, the release of noncritical information to the public—to risks that are faced by liberal democratic nations from penetrations by the likes of corrupt governments, rogue states as well as organized criminals, and radical ethnic, racial, and religious groups, including ultra-right-wing political groups.

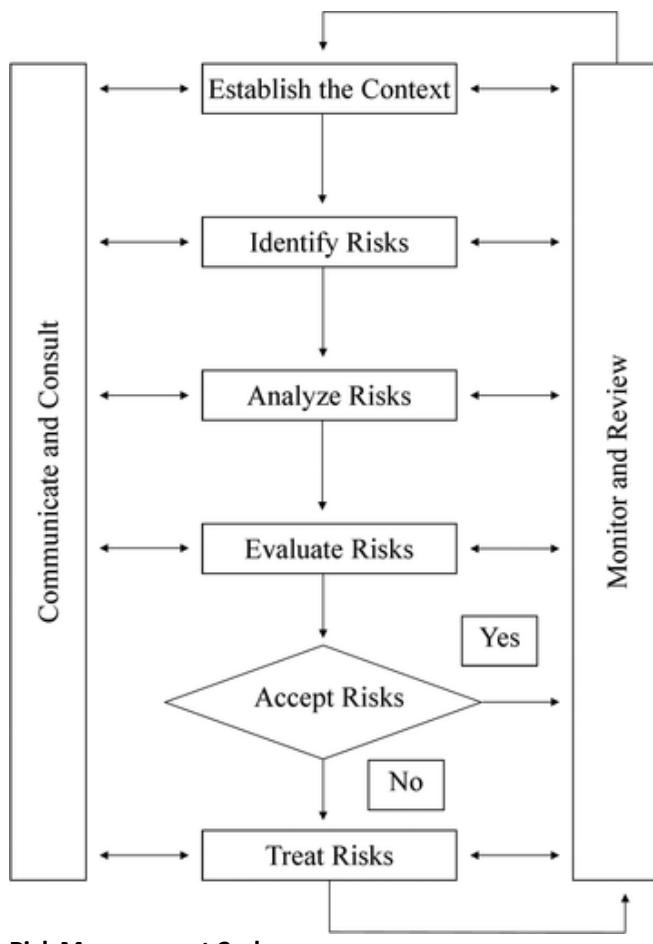
Internationally, risk analysis is the subject of a standard. The Swiss-based International Organization for Standardization (ISO) has published a document that puts forward a common approach for dealing with risk by providing generic guidelines in relation to the principles for how risk is managed.^[6] In Australia, as well as in New Zealand, uniformity in risk management is specified by AS/NZS 31000:2009. This document is published through a joint venture by these two organizations: Standards Australia and Standards New Zealand. AS/NZS ISO 31000:2009 can be applied to a number of activities, decisions, or operations in the private and public sectors, as well as the military. They can also be applied by nonprofit organizations, community groups, and individuals.

Some of the key terms in risk management include the technique that is considered here—*risk analysis*—as well as *risk*, *risk assessment*, and *risk management*. According to ISO 31000:2009, risk is “the effect of uncertainty on objectives.”^[7] Risk assessment is the “overall process of risk identification, risk analysis and risk evaluation,”^[8] and risk management is the “coordinated activities to direct and control an organization with regard to risk.”^[9]

Understanding these terms helps distinguish the process of managing risk from the analytic process of assessing risk using the equation:

$$\text{risk} = \text{likelihood} + \text{consequence}$$

Likelihood refers to the probability of “a specific event or outcome, measured by a ratio of specific events or outcomes to the total number of possible events or outcomes.” *Consequence* is defined as the “outcome of an event affecting objects.”^[10] Likelihood and consequence are evaluated in the analysis phase of the risk management cycle. This analytic cycle comprises five phases shown diagrammatically in figure 4.3.^[11]



Risk Management Cycle.

Source: International Organization for Standardization, *ISO 31000: Risk Management—Guidelines on Principles and Implementation of Risk Management* (Geneva: ISO, 2009), 14.

Step by step, the three analytic phases of the risk management cycle comprise:

1. The use of two analytic techniques—in the form of scales—to evaluate the information target’s risk rating (e.g., a database on a particular server). These two scales consist of a likelihood scale (table 4.6) and the consequences scale (table 4.7).

2. The results of these two assessments are then injected into a risk-rating matrix (table 4.8) that returns a risk-rating coefficient.
3. Finally, the counterintelligence investigator looks up the risk rating coefficient on the risk evaluation scale (table 4.9) in order to determine what actions (if any) are required.

In addition to the descriptors listed in the tables below, there may be a need to include a set of conditioning statements, along the lines of those contained in table 4.5. This also applies to the descriptors contained in table 4.7.

Examples of low-risk events include:

- An event that would occur rarely and would result in insignificant consequences (reflected in table 4.8 as E1); or
- An event that is unlikely to occur and would result in minor consequences (reflected in table 4.8 as D2).

Examples of high-risk situations include:

- An event that would occur rarely but result in catastrophic consequences (reflected in table 4.8 as E5); or
- An event that is likely to occur and have minor consequences (reflected in table 4.8 as B2).

Treating Risks

Once each risk is assessed in this way, they can be positioned on the risk-rating matrix (table 4.8) so they can be compared with each other in order to prioritize treatment options—these can sometimes be termed *countermeasures*. Take for instance the following events considered by troops stationed in Country Q.

- The risk posed by a local citizen employed to remove rubbish around a forward command post, and who hence gained access to sensitive operational information, was assessed at C5 (possible with catastrophic consequences and, therefore, an extreme risk); or
- Harm as a result of inadequate shredding of some routine sensitive documents could be located at B4 (likely with moderate consequences, so the risk is high).

Typical Example of a Likelihood Scale

<i>Rank</i>	<i>Likelihood</i>	<i>Descriptors</i>
A	Almost Certain	The situation is expected to happen
B	Likely	The situation will probably occur
C	Possible	The situation should occur at some time
D	Unlikely	The situation could occur at some time
E	Rare	The situation would only occur under exceptional circumstances

Typical Example of a Consequences Scale

<i>Rank</i>	<i>Consequence</i>	<i>Descriptors</i>
1	Insignificant	Will only have a small impact
2	Minor	Will have a minor level of impact
3	Moderate	Will cause considerable impact
4	Major	Will cause noticeable impact
5	Catastrophic	Will cause systems and/or operations to fail with high impact

Typical example of a risk rating matrix

			<i>Consequences</i>		
	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
A Almost Certain	Moderate	High	Extreme	Extreme	Extreme
B Likely	Moderate	High	High	Extreme	Extreme
C Possible	Low	Moderate	High	Extreme	Extreme
D Unlikely	Low	Low	Moderate	High	Extreme

E Rare	Low	Low	Moderate	High	High
-----------	-----	-----	----------	------	------

Typical Example of a Risk Evaluation Scale

<i>Risk Rating and Suggested Actions for Treatment</i>	
Low Risk	Manage using standard operating procedures.
Moderate Risk	Outline specific management actions that need to be taken.
High Risk	Create a business contiguity plan and a response plan (test annually).
Extreme Risk	Urgent actions are necessary (in addition to those per high risk).

The scale provided in the risk-rating table (table 4.9) is useful for judging whether the counterintelligence investigator recommends accepting the risk or treating the risk (and, if so, to what extent). Without the risk assessment process the recommendations of the investigator could be called into question as an overreaction or, equally, deemed an underestimate of the seriousness of the situation. These models curb subjectivity to some extent by providing transparency about how counterintelligence investigators make their calculations.

Although the risk rating (table 4.9) shows what is a generally accepted distribution of risk levels,^[12] counterintelligence investigators will need to make their own judgments as to where these transition points occur. Many times this will be a topic for discussion with the employing agency or a matter set by policy. But, by using a systematic approach to risk management, investigators can reduce the likelihood, and lessen consequences, through the application of technology, science, or personal or collective effort.

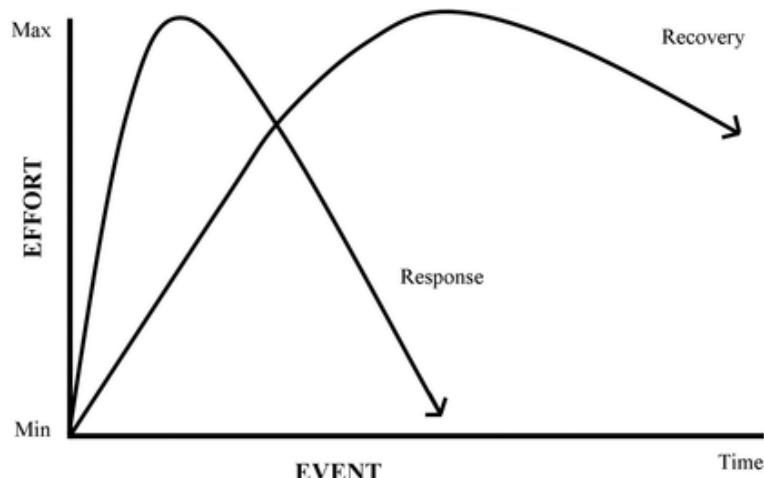
According to Emergency Management Australia (EMA), some treatment options include: awareness and vigilance, communication and consultation, engineering options, monitoring and review, resource management, security and surveillance, and community capability and self-reliance.* Although these treatment approaches are discussed in relation to critical infrastructure, they could be adapted for use in treating risks in relation to sensitive information.

* Emergency Management Australia, *Critical Infrastructure Emergency Risk Management and Assurance*, 2nd ed. (Canberra: Attorney-General's Department,

2004), 43.

PPRR Planning

There are four elements to PPRR policy development—prevention, preparation, response, and recovery. Prevention considers the risk and tries to implement ways that could prevent it from happening. Preparedness acknowledges that, despite preventative measures, the event may still occur, and asks how one can prepare for it. If it does occur, response is that part of the plan that deals with how agencies will mobilize and take action (and what type of action, etc.). The final element provides guidance for how a recovery operation will take place. This anticipates the worst-case scenario; that is, preventative measures have failed, preparation measures may have mitigated the impact to some degree, but it still occurred; response has contained and brought the event to an end, but it is now time to recover from the event's effects.



Comparisons of Response and Recovery Efforts.

Courtesy of the author.

Even though this chapter addresses PPRR from a counterintelligence point of view, it should be borne in mind that, when planning for one type of event, it is prudent to consider actions to cover what is termed *all hazards*.

For instance, if a counterintelligence investigator is considering the impact of, say, a penetration by an opposition agent, then why not consider the same (or like) event occurring as a result of inadvertent leakage or by chance or accident?

When compiling a defensive counterintelligence PPRR plan, try to avoid constructing the plan in such a way that each element forms either a conceptual or real barrier between them—there is usually no clear delineation between the elements though they may be expressed in these terms. Also, bear in mind that each element will not necessarily carry the same weight of importance—the four elements may not be equal. In fact, some elements may not have any strategies or treatments, or few, or minimal.

Further, although the elements are cited in a sequence—PPRR—they may be accomplished at the same time; for instance, response and recovery can (and should) start at the same time as they are inextricably linked (see figure 4.4).

Finally, though the language appears to contain action-oriented terms, the treatment options do not have to be physically based options. Options involving social dimensions are also needed as, arguably, people are often the means by which the opposition will gain access to sensitive information.

Counterintelligence investigators should try and keep their thinking about treatments broad and innovative. The Australian Institute of Criminology has suggested a 5Is model for solving crime-related issues, and this model could be adapted to countermeasure for defensive counterintelligence.

This involves the gathering and analysis of information on the specific crime problem (*intelligence*), selection of the full potential repertoire of responses to address proximate and distal causes of the problem in question (*intervention*); action to convert interventions into practical methods (*implementation*); mobilization of key stakeholders and agency participants (*involvement*); and evaluation of outcomes (*impact*). [\[13\]](#)

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- All hazards;
- Attractiveness;
- Capability;
- Coefficient;
- Consequence;
- Desire;
- Ease of penetration;
- Expectation;

- Impact;
- Intent;
- Knowledge;
- Likelihood;
- PPRR;
- Resources;
- Risk;
- Threat;
- Threat-agent;
- Threat communities;
- Threat profile;
- Treatment; and
- Vulnerability.

STUDY QUESTIONS

1. What are the elements that comprise a threat analysis? Describe each and explain why each is important to understanding a threat.
2. What are the elements that comprise a vulnerability analysis? Describe each and explain why each is important to understanding the concept of vulnerability.
3. What are the elements that comprise a risk analysis? Describe each and explain why each is important to the understanding of risk.
4. What are the elements that comprise a PPRR plan? Describe each and explain why each is important to defensive counterintelligence planning.

LEARNING ACTIVITY

Suppose that you are asked to conduct a threat assessment for a business that is researching a new vaccine. The information relating to the new vaccine is currently in the form of a research proposal and the document is located in the company's safe within the office of the chief researcher. Conduct a threat assessment and a vulnerability assessment regarding that piece of data using the processes discussed in this chapter.

NOTES

1. Associated Press, "Irish Expel Russia Envoy over ID Theft for Spying" *New York Times*, February 1, 2011, A9, New York ed.

2. Hank Prunckun, *Handbook of Scientific Method of Inquiry for Intelligence Analysis* (Lanham, MD: Scarecrow Press, 2010)
3. Prunckun, *Handbook of Scientific Method of Inquiry for Intelligence Analysis*, 2010.
4. These are only a small set of categories that could populate a scale-like arrangement of options from open and accessible in minutes to well-protected arrangements using state-of-the-art techniques and equipment.
5. WikiLeaks, *About*, wikileaks.org/About.html (accessed July 5, 2011).
6. International Organization for Standardization, *ISO 31000: Risk Management—Guidelines on Principles and Implementation of Risk Management* (Geneva, Switzerland: ISO, 2009).
7. International Organization for Standardization, 2009, 1.
8. International Organization for Standardization, 2009, 4.
9. International Organization for Standardization, 2009, 2.
10. International Organization for Standardization, 2009, 5.
11. International Organization for Standardization, 2009, 14.
12. Queensland Government and Local Government Association, *Local Government Counter-Terrorism Risk Management Kit* (Brisbane: Queensland Government and Local Government Association, 2004), 16.
13. Adrian Cherney, "Problem Solving for Crime Prevention," *Trends and Issues in Criminal Justice* (Canberra: Australian Government, May 2006), 2.

Chapter 5

Tenets of Defensive Counterintelligence

Chapter 5 5 Tenets of Defensive Counterintelligence

This topic describes the essentials of defensive counterintelligence by examining:

1. Initial considerations; and
2. Tenets of defensive counterintelligence.

INITIAL CONSIDERATIONS

Defensive counterintelligence is concerned with *deterrence* and *detection*. Translating these concepts into actions within an agency is termed *countermeasures*. But the concept of countermeasures is applied in this context with a somewhat narrower connotation than is common in the mainstream intelligence studies literature. In its application here, countermeasures can be seen as an umbrella term for measures ranging from passive defensive to active offensive. This chapter provides a discussion of the seventeen tenets of defensive counterintelligence.^[1] These tenets should therefore form the basis for considering specific issues in the counterintelligence planning process.

TENETS OF DEFENSIVE COUNTERINTELLIGENCE

Tenet 1—Executive responsibility. Of the tenets of defensive counterintelligence, the highest order tenet is that of executive governance. Although it might seem to some as somewhat self-evident, it is worth stating this tenet for clarity. The responsibility for security in all its forms rests with the head of the agency. Although the agency head will rarely be involved in any of the day-to-day security issues, he or she has responsibility for creating and maintaining a security program to guard the agency's confidential information and secret operations. To this end, this functional responsibility is therefore delegated to

subordinates (or a committee), and, depending on the size of the agency, there may be several such delegations flowing down the chain of command. Nevertheless, the point is that the ultimate responsibility for orchestrating these activities rests with the agency head, and the importance placed on security within the agency is driven by the commitment of that person.

Tenet 2—Executive support. For security to be effective the agency head must be willing to promote security so that all employees understand and accept it in the most favorable light. The image of security within the agency must be positive. Staff's attitudes must be cultivated to respect its purpose and, as a consequence, accept its associated policies and practices.

The main hazard to information is complacency regarding its security.

Tenet 3—Ethical symmetry. One of the key issues in acceptance is that staff view the security regime as one that is in harmony with the prevailing social norms—that is, it does not seek to recreate the model of a dictatorial state to deal with procedural compliance. Nor should it implement countermeasures that are illegal or unethical; for example, barriers that are electrified to a lethal level, or air-locks that fill with poisonous gas.

Tenet 4—Need to be there. The rationale for allowing people to access an area where sensitive information is being processed, analyzed, or stored needs to be established. Although the doctrine's relation to access to information—known as the *need to know*^[2]—is discussed in more detail in tenet five below and in chapter eight (Defensive Counterintelligence: Information Security), it is important to illustrate the basis for this tenet. Known as *friendly access*, this is a means where the opposition attempts to gain access by deception rather than force. Therefore, access to an agency's offices should be limited to employees and visitors who are known or have appointments. All other visitors should be carefully screened and their identities verified prior to entry. People making deliveries, including mail deliveries and maintenance

workers, should be handled in the same manner. Access to all areas of the agency should be on a restricted *need-to-be-there basis*. If an agency's visitor/staff traffic is heavy, a system of custom-designed identity cards worn on employees' outer clothing can be an efficient method of quickly establishing *friend or foe*.

Tenet 5—Need to know. Much of what is considered in here in defensive counterintelligence could be redundant if the opposition was never aware that sensitive information existed. This means that the first breach of security occurs when the opposition becomes aware that information worthy of targeting exists. If one uses the metaphor of a genie, it is at the point when the opposition knows about the information that the proverbial genie has been let out of the bottle and there is no way of returning it. All that can be done at that juncture is intensify the defensive counterintelligence measures and/or conduct an offensive counterintelligence operation. So, if information holds some degree of sensitivity, its existence needs to be kept confidential to all but those with a need to know.

Tenet 6—Counterreconnaissance. This tenet is associated with tenet five—not allowing the opposition to know of the information or operation in the first place. This tenet seeks to prevent *reconnaissance*. [3] In this sense, it is more than preventing a reconnoitering of a physical target, as the case would be for the location of a piece of critical infrastructure. It is preventing *environmental scanning*—that is, hunting for leads that could indicate the agency is inactive in perusing certain developments. For instance, strategic intelligence analysts use a method known as environmental scanning to investigate issues of value. It seeks to obtain data at the macrolevel. If in analyzing these data the analysts conclude that there are indicators that the opposition may be involved in activities that they would like to know about, the proverbial genie has been let out of the bottle.

Tenet 7—Realistic policies and procedures. Countermeasures need to be flexible and need to correspond to the risk. They should not become a rigid set of policies and procedures. Rather, they need to be fluid and adaptable to changes in the agency's requirements for security. No doubt practitioners will need to consider many factors before

implementing countermeasures. Nevertheless, important issues need to be weighed when establishing, or improving, a defensive counterintelligence program. These include, but are not limited to, financial constraints and the willingness of staff to follow proposed procedures. For instance, in the business and private sectors, there is little sense in spending large sums of money on a safe and intruder detection systems if the utility is not justified, or it pushes the budget toward insolvency. Likewise, staff may be tempted to bypass security procedures if they are seen as overly complicated or time consuming.^[4]

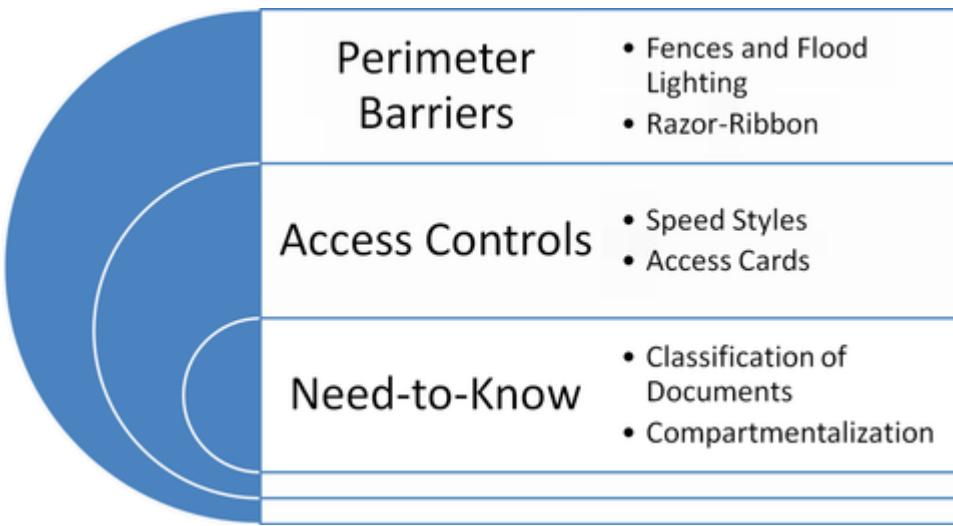
Tenet 8—Synergistic approach. Countermeasures should be seen as modular, that is, able to be adapted either in whole or in part, depending on the results of the counterintelligence planning process that was described in the previous chapter (chapter four, Counterintelligence Planning). The important issue is that the tenets of defensive counterintelligence are observed and that periodic inspections are carried out to check on the standard of security practiced. Countermeasures can therefore be seen in a synergistic way—the combination totalling more than the sum of the individual components.

Tenet 9—Early detection. Break-ins and burglaries are not an uncommon occurrence for government agencies or businesses to experience. However, in June 1972 the Watergate affair brought home the reality that break-ins are not only a method for acquiring cash and valuable physical assets, but they are also a technique for information gathering.^[5] In intelligence work this technique is referred to as a *black bag operation*.^[6] Surreptitious entries are used to plant surveillance devices or to carry out other covert intelligence-gathering activities. Short of creating a minifortress, there is nothing that will make an office 100 percent burglar-proof—even Buckingham Palace has had its intruder. Ideally, this tenet dictates that an alert is sent to the counterintelligence officer that a penetration has occurred at the time it took place. This facilitates several things: an immediate notification shortens the time the perpetrator has to access information, as well as places the perpetrator under pressure, thus increasing the chance of errors. Errors could also result in trace evidence being left behind. If it is not possible to design an immediate alert facility, then the time between penetration

and detection needs to be as short as possible. Detection also increases the deterrent effect of the system.

Tenet 10—Defense in depth. The tenet of early detection (tenet nine) is integral to this tenet—that of delay. Namely, once detected, countermeasures should be directed to delaying the perpetrator so that security guards or police can arrive and apprehend the offender. This requires a system of barriers to be installed. Barriers can be any device that separates two spaces. They can range from reinforced walls and doors to transparent glass partitions. Barriers also act as a means to cause the perpetrator to leave behind evidence of how they tried to penetrate the barrier, thus providing a rich source of forensic evidence for counterintelligence investigators. In this regard, the barrier system needs to consist of several barriers to form a set of layers—termed *defense in depth*. The theory behind defense in depth is that the perpetrator will lose momentum as they encounter each barrier. If there was one single defense, although difficult to penetrate, once breached, the target data is immediately vulnerable. The strongest barrier in a defense-in-depth system needs to be located closest to the targeted data.

Allied to the tenet of defense in depth is the central pillar of personnel security (see chapter seven). This pillar states that, in order to ensure that staff who work for the agency do not inadvertently disclose secrets, some form of “protection” needs to be in place. Although not a physical barrier as such, the protection afforded is a barrier nonetheless. This protection takes the form of background investigations. For instance, to guard against persons who may seek to intentionally reveal classified information and those who may be so indiscreet that they may unintentionally reveal secrets if employed, a vetting process needs to take place.



Diagrammatic representation of the tenet of defense in depth.

Courtesy of the author.

Another set of pillars that is associated with the tenet of defense in depth are the three pillars of information security (see chapter eight). These pillars include confidentiality, integrity, and availability. Confidentiality is concerned with the prevention of unauthorized disclosure; integrity is concerned with being able to detect if and when information is modified; and availability is concerned with ensuring that the data is able to be accessed by those with a need to know when required.

Tenet 11—Unpredictability. If the agency's barrier defense system could incorporate a feature that causes the perpetrator to be startled or confused as they encounter each barrier, this will add to the overall robustness of the barrier system. A barrier that is predictable can be overcome more easily than one that has several possible outcomes when trying to breach it. Again, early detection and time delay are the overall goals of these related tenets.

Tenet 12—Core hardening. Following on from the tenet of defense in depth (tenet ten), the target data needs to have the strongest barrier around it in the immediate vicinity. And the risk associated with protecting these target data also needs to be reduced to the smallest possible physical profile. Spreading the risk over a large area (say a floor of an agency's building) weakens the countermeasures established to protect it. But, having said that, a security plan needs to avoid placing

the target data in a position that makes it susceptible to a single vulnerability. It is therefore important that the system that is set up to protect the data in the core location of the defense-in-depth plan is not only small in profile, but is itself protected. Examples of this type of self-protection system can be seen in physical protection measures that prevent intruder alarms from being tampered with, or an automatic logging system that occurs when users log on to a computer system.

Tenet 13—Delineate and prioritize. It follows that, if a defensive counterintelligence program needs to harden the protection it has for sensitive information items, then an agency must first identify what these items are. This is of pivotal importance—there is an undeniable need to delineate and prioritize those bodies of information that warrant counterintelligence protection. Concomitantly, the systems, processes, institutions, and individuals in which such information resides need to be prioritized also.^[7] Kenneth DeGraffenreid once stated: “A country must first know what it is trying to protect. What are those values, secrets and institutions that it needs to protect? In a free society there are lots of them. Given the finite nature of its counterintelligence resources, what are its most precious secrets? This requires analysis and decision.”^[8]

Tenet 14—Quality over quantity. As in many of life’s endeavors, quality is more important than the quantity and this is the same when it comes to defense in depth. This is particularly demonstrated when it comes to those elements of the system that involve people. Security guards come to mind in this regard. A small cadre of well-trained and motivated security guards is far more valuable than abundant but poorly trained and lackluster sentinels. It took only one observant and responsive security guard to expose the illegal intelligence operation that was eventually traced back to the Nixon White House,^[9] with the ultimate result of Richard M. Nixon resigning as president of the United States of America (see figure 5.2).

LEFT	RETURNED	6-16-72	LEFT	Returned	6-17-72
		Door cracked open left clear but door was left open after investigation	5:30 AM	6:20 AM	Aut De Reg Secured all B1-B2-B3 several
5:00 AM	5:30 AM	All doors and windows locked up but also left unlocked checked out cells off duty found key hole glass intact.	6:55 AM	6:55 AM	unlocked trash pool several B1-B2-B3 secured
5:45 AM	6:00 AM		7:00 AM	7:00 AM	several B1-B2-B3 secured made return + now informed about the break in deck floors of return cells to Dist. 855 AM;
6:00 AM	6:30 AM		8:00 AM	9:00	
7:00 AM	7:30 AM				
12:00	12:00				
12:05	12:05	Will go Party 12:00 PM			
		Return to a several office buildings also office bath + care also the door on each type coffee etc other words the with paper and the door open outside off office bldg will be open			return care back investigate down two bldgs. Will be fully investigating inc car shuffle, etc paul keeper.
			1:00 PM	made	Security check made on all the floors it will soon
			2:00 PM	make	floor first
			2:15 PM	check	floor for damage everything ok
			2:30 PM	check	B-1 B-2 B-3 floor obscene
			3:00 PM		By place + D.E.T. coming
			2:00 PM	make	work on 11 floor + at lowest
				floor every thing under control	
				Police are here they making check all so	
				Reported here I had been deepest	
				house down most keep it down	
			4:00 PM	long	check all floor front like this
				long	the largest corner checked out
				long	1:00 Office statement on duty

Security guard the late Frank Wills's log showing his entry relating to his discovery of the break-in during the night of June 17, 1972, at the Democratic National Committee's offices at the Watergate office complex, Washington, DC.

Courtesy of the U.S. National Archives and Records Administration.

Tenet 15—Cooperation. As security is usually agency specific, this tenet states that there is a need for cooperation between counterintelligence personnel and external law enforcement agencies. This involves liaising with police and neighboring firms with crime prevention strategies, as well as a formal reliance on law enforcement agencies to effect arrests^[10] and to prosecute cases through the courts.

Tenets 16 and 17—Reduction and complicity. Finally, there are two integral tenets that, although complementary upon first examination, can also be seen as mutually exclusive. Tenet sixteen is that the security strategies need to be able to reduce the list of suspected perpetrators to the smallest possible pool. The ability to do this serves as a deterrent, as well as signals that there will be detection. However, if the security countermeasures can be designed to ensure that no single person can breach the safeguards, then this will ensure that more than one person will be involved in any attempt to acquire sensitive data. Tenet seventeen could be called the tenet of complicity. Complicity

ensures that, in order to penetrate the security arrangements, it will require two or more people. Having multiple perpetrators ensures that errors will be made. The intent here is that the perpetrators' security arrangements will be compromised. It also creates a potential trail of link evidence for counterintelligence investigators. If a perpetrator is forced by security arrangements to enter into a complicit arrangement, it acts as a deterrent and provides valuable leads of detection.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Black bag operations;
- Defense in depth;
- Detection;
- Deterrence;
- Environmental scanning;
- Friendly access;
- Friend or foe; and
- Reconnaissance.

STUDY QUESTIONS

1. 1. List the seventeen tenets of defensive counterintelligence.
2. Describe how the opposition might use *reconnaissance* to gain an awareness of, say, an agency's headquarters' critical infrastructure and then contrast this to how it might conduct an *environmental scan* to detect the existence of desired information. Although they are different, are there also similarities? If so, explain what the similarities are.
3. Describe the purpose of tenet ten, defense in depth. Give an example of how this tenet could be applied to an office area in which you have recently worked.

4. In relation to tenet eleven, devise a barrier system that could provide some degree of unpredictability, thus affording delay to any penetration attempt. As this is a notional example, you can use any barrier to demonstrate your unpredictable system enhancement.

LEARNING ACTIVITY

Consider the tenets of reduced pool of perpetrators (tenet sixteen) and complicity (tenet seventeen). Using either your current workplace or a notional one, think of a small collection of sensitive data. These data can be hardcopy documents or electronically stored files. Now brainstorm three (3) strategies that would enable counterintelligence investigators to reduce the list of suspects who have attempted to obtain these data to the smallest possible pool. Finally, think of a countermeasure that could complement each of the three (3) strategies so that it ensures that no single person would be able to breach the strategy to protect the sensitive data.

NOTES

1. Many of these tenets are adaptations of security-related considerations espoused by Hamilton (1979) but have been specifically crafted to help explain and underpin the principles of defensive counterintelligence. See Peter Hamilton, *Espionage, Terrorism and Subversion in an Industrial Society* (Surrey, UK: Peter Heims Ltd., 1979), 164–74.
2. There are two principles relating to access to information—*need to know* and *right to know*. Closely tied to the need-to-know principle is that of *need to share* as well as the *responsibility to provide*.
3. In this sense, the term *reconnaissance* is used in a way slightly different from the usual meaning—that is, scouting ahead of a main force. But *environmental scanning* is in a way related as the person scanning is seeking information about the issues under investigation ahead of the main research effort.
4. Government agencies, or contractors who do work for government agencies, may have a legislative requirement to employ certain levels of security, or certain classes of security devices, or use certain procedures, and these may not be able to be varied.
5. In the case of Watergate, this could be considered as private political espionage as the operation was conducted outside the Constitutional functions of the Executive Office of the President.

6. See, for example, Carl Roper, *Agent's Handbook of Black Bag Operations* (Cornville, AZ: Desert Publications, 1978).
7. This tenet stems from discussions with Dr Petrus "Beer" Duvenage (State Security Agency, South Africa), personal communication, January 23, 2012.
8. Kenneth DeGraffenreid, "Counterintelligence," in Roy Godson (ed.), *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence and Covert Action* (Lexington, MA: Lexington Books, 1989), 151.
9. See chapter one in Richard Helms with William Hood, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003).
10. It is worth recalling that in some jurisdictions all citizens have the power of arrest, not only police officers. But this is usually predicated on the requirement that the person making the arrest has observed firsthand the commission of a felony (in some jurisdictions a *felony* is termed an *indictable offense*) or it may be a summary offense (i.e., a misdemeanor), but these are usually related to property damage or offenses against a person. Laws that allow for a *citizen's arrest* also usually stipulate that the arresting person can use coercive force to apprehend the alleged offender, but once restrained the arrestee must be delivered to the police without delay. For example, in Australia section 3Z of the federal government's *Crimes Act, 1914* gives every citizen the power to arrest for an indictable offense. And, under South Australian state law, every South Australian citizen has the power to make an arrest for indictable offenses as well as summary offenses relating to property and crimes against the person under the provisions of section 271 of the *Criminal Law Consolidation Act, 1935*. Note that these are only examples as this is an academic discussion; it should not be taken as legal advice.

Chapter 6

Defensive Counterintelligence: Physical Security

Chapter 6 6 Defensive Counterintelligence: Physical Security

This topic describes the essentials of defensive counterintelligence by examining:

1. Physical protection of secrets;
2. Barrier controls;
3. Doors;
4. Entry and exit controls;
5. Windows;
6. Secure containment;
7. Security lighting;
8. Closed-circuit television;
9. Intruder detection systems;
10. Computer physical security; and
11. Guarding services.

PHYSICAL PROTECTION OF SECRETS

If defensive counterintelligence is concerned with *deterrence* and *detection*, then physical security is the bedrock on which the approach relies. Though physical security cannot act as an absolute deterrent, the tenets of defensive counterintelligence rely on it. This chapter presents the most key physical security countermeasures and their tactical application. Although these countermeasures are described in terms of their potential application, it should be noted that some government agencies, or contractors who do work for government agencies, may have legislative requirements to provide a certain level of security and/or to comply with certain security standards. Offering lower levels of security, or opting out of certain security procedures, may not be

negotiable. For instance, in Australia the *Protective Security Manual* “facilitates and promotes a consistent approach to security across all Australian Government agencies. . . . It is also the minimum security standard for State and Territory Government agencies which access Australian Government [classified] resources.”^[1]

BARRIER CONTROLS

Perimeter Fencing

A perimeter fence serves several purposes. It first stands as a symbolic division between an area where one is allowed to be and an area where access is controlled. Its physical presence signals to those contemplating crossing that such an act will bring consequences. The important aspect of a perimeter fence is that it can actually make crossing difficult. Note that it needs to be difficult, as attempting to make it impenetrable may be wishful thinking. Even the Maginot Line failed to keep the Nazis from invading France during World War II. What a perimeter barrier will do is declare a “no-go-zone,” provide warning if breached, and cause delay if entry is attempted.

Having a declared area that is off limits gives security guards the ability to detain and question personnel found within the area. A delayed entry will give security officers time to detect and respond.

The configuration of a perimeter fence can vary greatly, and, even though the term *fence* is used here, the barrier can be a wall, a series of bollards, moat, or other construction design. Barriers are often viewed as physical obstructions, but barriers can be devices, such as passwords, security clearances (e.g., secret or top secret), or classifications placed on documents, and so forth.

In contrast, ram-raid or cash protection barriers are not contemplated in the context of perimeter fencing. These types of barriers are designed to absorb high levels of energy—such as that from a vehicle driven into the barrier. Perimeter-fencing standards are usually specified in terms of time to breach the barrier. Features that increase delay include barbed wire or razor ribbon (see figure 6.1), or electrification. Some installations feature two or more sets of fencing

with cleared areas in between to further cause delay, as well as other variations such as vertically stacked coils of razor ribbon or pyramid-stacked arrays, or other configurations. Perimeter barriers can also be augmented by dog patrols and/or CCTV monitoring or motion detection alarms.



An example of a barrier fortified with a combination of two strands of barbed wire and an overlay of interlocking circles of razor ribbon.

Courtesy of the author.



An example of “barrier spikes” on top of a gate. Such spikes can also be a feature of walls and other obstacles. Note the use of electrification on the opposite side of the chain-link (a close-up of this feature is shown in figure 6.3).

Courtesy of the author.



A close-up of how electrification can be incorporated into a chain-link barrier.

Courtesy of the author.

Some issues that should be considered in designing new perimeter barriers, or for assessing the adequacy of existing barriers, are listed below. Although this is not an exhaustive list, the questions are indicative of the types of issues that should be considered.

- Is the height of the barrier in relation to the surrounding space appropriate?
- If chain link, is the gauge of the wire and construction of the pole supports adequate?
- Is there barbed wire or razor ribbon at the top of the fence?
- Is the perimeter fence adequately united with any building or structure that might form part of the perimeter (e.g., by increasing the height of the fence where it joins a building)?

- Is the clear space on either side of the barrier sufficient to notice any attempt to breach the barrier?
- Is the area on either side of the barrier a car parking area or used to store material that could be used in an attempt to breach the barrier?
- Are there any utility tunnels or sewer or water channels that run under the perimeter, and, if so, are they secure?
- Are the number and location of gates along the barrier adequate for access, including the need for evacuation in case of an emergency or to allow emergency services to enter?
- Are the locking devices used commensurate with the strength of the barrier they are installed in?
- Is there a system of key control for the gates and other secured penetrations in the barrier (e.g., manholes)?
- Is the barrier posted with “no trespassing” signs at regular intervals?
- Is the barrier’s perimeter checked by patrols, dogs, or CCTV to detect attempts to breach the barrier and to act as a deterrent?

Tangle-Foot Wire

This is either barbed wire or razor ribbon that is used to construct an obstruction to tangle intruders’ feet. It can be constructed outside a facility’s perimeter fence or in the area formed between a set of double fences. In the latter case, it adds greatly to the deterrent effect. The barbed wire or razor ribbon is usually supported by short, metal stakes driven into the ground and secured at irregular intervals. The height of these support stakes should be less than the height of the wire coils so intruders cannot use them as balance points. If the barbed wire or razor ribbon is laid in a cross pattern it adds to the obstacle’s overall effectiveness by making the pattern more complex to negotiate.

Perimeter Beams

If the outermost defensive measure is the perimeter fence, then an additional fortification is an electronic “trip wire” known as a *perimeter*

beam. These devices are usually mounted to a structure inside the fences to help reduce defeat by tampering. Although intruders are able to see these devices, the difficulty of avoiding triggering them is not trivial. As such, their use presents a high level of deterrence. However, in terms of detection, they are known to present false positives—that is, they can be prone to triggering by wind-blown vegetation, debris, the movement of animals, and even spider webs. Certain zones will need to be deactivated during the time of any patrols or if dogs are used, and then reset.

Perimeter Towers

Observation towers offer security personnel a way of increasing the viewing range for large or spreading facilities for which they are responsible. If the area under observation is illuminated with floodlights, towers can be used at night as well as during daylight hours. It is important that, if more than one tower is required to cover the area under guard, the towers are placed so that the field of view from each tower has some common area of overlap. Inclement weather may adversely affect the advantages of towers, in which case foot patrols or CCTV may need to be considered as backup measures. It is essential that a primary and secondary method of communication is incorporated in tower design along with a system of sounding an alarm (visual as well as audible). Temporary or mobile towers may also be used for special projects or occasions.

DOORS

External Doors

External doors are not only a symbol of strength but one of great practical application. It is the physical barrier that separates the opposition's agents from the areas they seek to access. External doors should be solidly constructed and have three hinges per door. The installation of the additional third hinge contributes greatly to the door's resistance against forced entry. Hardwood doors are better than

those constructed of softwood, and solid doors are stronger than ones containing panels. However, wood-panelled doors are more secure than doors containing glazed panels.

It is equally important to have strong door frames to prevent failure during attack. Door frames should be securely fixed to the wall by appropriate bolts. Furthermore, double-cylinder deadlocks should be installed on all external doors. The double-cylinder deadlock needs a key to open it from either inside or outside and, when in use, it prevents an intruder from using the door as an exit after intrusion. The deadlock system also offers a medium to high degree of protection against *lock picking*. There are also multilocking systems that incorporate vertical bolts and rods designed to reinforce the door in conjunction with the deadlock option.

External doors can be fortified by the addition of security grilles or an outer set of security doors that feature a mesh or grille construction. Such a feature adds both deterrence and delay for those determined to breach the barrier. A fortified external door is shown in figure 6.4. The sizable amount of force need to break down this door can be seen in this photograph. The noise generated in the breach would no doubt give alarm to the occupants, thus providing time to destroy any confidential information that might be sought by those searching.



U.S. soldiers breaching external door in Buhriz, Iraq, November 30, 2010.

Photograph by Air Force Staff Sergeant Stacy L. Pearsall. Courtesy of the U.S. Army.

Flush bolts are used to secure the inactive half of a set of double-leaf doors. These bolts are fitted to the top and bottom of the inactive door as close as practicable to the leading edge in order to gain strength to resist forced entry. The length of the bolt and the gauge of the bolt itself is key in determining the strength the bolt can withstand in an attack. Generally, the longer and wider the bolt, the more strength it has. Balance needs to be applied in fitting flush bolts to ensure the aesthetics of the architectural design of the doors is maintained. If this proves inadequate, the design of the doors may have to be revisited with the architect to design a door system that provides both security and a pleasing visual look.

Internal Doors

Depending on the application, internal doors can be as plain as a solid panel or as stylistic as architectural design glass sliding doors. Steel doors that are common features in banks can also be employed as

internal doors. The room in which one of these would be hung would not hold cash or securities, but information or communications equipment carrying classified message traffic.

The main function of internal doors is to define areas that require approved access and to cause delay if a breach is attempted. Digital card readers, swipe card readers, keys, or other means of accessing these areas are the standard. More sophisticated biometric access controls can be used, but this equipment is costly and perhaps warranted for information that is classified at the highest levels of secrecy.

ENTRY AND EXIT CONTROL

Speed Styles

Access control to an agency's building, or within areas of the building, can be controlled by *speed styles*. These are not intended as outright barriers, as would be the case with reinforced doors, but a convenient way of triage—that is, separating those with approved clearance to enter and those without. They allow large numbers of staff to enter or exit with convenience and do not slow entry or departure, but facilitate control and will alarm security guards to any attempted breach, whether intentional or by error. Access is usually by electronically coded cards. By coding these cards centrally, security staff can reactivate cards without the staffer presenting the card. In practice this means that, if a person is transferred on short notice to a special project in another area, his or her access can be approved via the computerized coding system, thus allowing them their new accesses. Likewise, when they complete their posting in certain areas, their accesses can be removed and new ones assigned. Being computerized also allows for a log to be generated, which could be used to help counterintelligence investigators in any inquiry relating to breaches.

Electronic Security Access Cards

Security access cards provide a convenient way to triage staffer movements through controlled areas of buildings, car parks, and other

zones controlled by the agency. They can be electronically programmed for access, as well as to arm or disarm alarms within designated areas. The more common use is with speed styles (see description in the section above) and to provide an audit trail via the electronic log generated each time the card is used. The physical size and design of the cards can vary depending on the agency, but usually they are the size of a credit card or driver's license. For instance, they can be combined with a photographic ID and can also contain color-coded security classifications.

Technological Improvements in Access Control

The post-9/11 security environment has seen the rapid development of new technologies for screening people for access to public facilities. The first example that springs to mind is access to airports and other transport hubs. The need to triage people with a need to enter these facilities is combined with the need to identify persons of interest so that their location, movements, and associations can be used for intelligence analysis. These same technologies can also be used for defensive counterintelligence purposes—to screen those with a need to access a location, and hence the information or people there, and those who need to be directed elsewhere. The technologies that were in use at the time of writing included a number of biometrics—facial recognition, fingerprints, iris or retinal scan, voice prints, odor, and DNA.^[2]

Although these technologies may give the impression that they afford an ironclad system of identification, there are some limitations and, as such, no single biometric device is able to provide 100 percent effectiveness. Some form of triangulation may be needed to ensure authentication.

When planning biometric installation, considerations include: whether the access control is fully automated (i.e., not attended by a security guard) or semiautomated (i.e., staffed by a guard); whether the environment is friendly (e.g., the building is located in the agency's home country) or unfriendly (e.g., a remote or hostile country); and

whether the subjects who are providing their biometric data are comfortable with the collections methods in relation to their societal, cultural, and religious norms, as well as the ethical standards associated with providing such biometric data, and the hygienic conditions when doing so.^[3] These factors are, of course, predicated on the level of risk and the security level of the information being protected.

WINDOWS

All windows should be protected by a suitable locking device. Keyed window locks provide a high level of security because an intending intruder can cut or smash the glass to reach and open any nonkeyed device. Keyed locks also prevent windows from being opened for use as an exit by a successful intruder. Other window security devices include bars and grilles. These are a must for air vents, fan openings, and skylights. Reflective window tinting is another effective countermeasure. Although not intended to prevent entry, reflective tinting provides a high level of protection for staff, equipment, and processes contained within. By denying intruders knowledge of what is inside a building, an agency can increase its level of physical security. An alternative to window tinting is the use of translucent glass.

Window Glazing Types and Indicative Security Ratings

<i>Glazing Type</i>	<i>Indicative Level of Security</i>
Plate glass (also known as <i>monolithic glass</i>)	Provides negligible resistance to attack.
Wired glass	Provides a marginal improvement over plate glass, but still in the negligible range.
Laminated glass	The layers of glass that are bonded together provide some resistance to attack.
Shatter resistance film	Used to increase the level of resistance from attack for standard glass types such as plate glass and wired glass. Its effectiveness depends on the product used and how it is applied, but generally only offers a small increase in protection.

Polycarbonate	Offers resistance to attack and is a commonly used type of glazing for security.
Bullet resistant glass	This type of glass offers a very high level of resistance from attack, including resistance to ballistic attack. Categories of bullet resistant panel and elements range from 9mm military parabellum through to rifle rounds such as 5.56mm and 7.62mm, as well as shotgun rounds using full choke and single slugs.
Shielding glass	Not intended to protect from physical attack but from “attack” by an electronic eavesdropper—uses radio frequency shielding to reduce emissions that could be intercepted outside the classified area.



Another way to strengthen windows against attack is to use bars, grilles or grates.

Courtesy of the author.

Glass-Break Detectors

These are devices that activate when glass panes are broken. These devices employ sensors, which are essentially microphones that are designed to trigger an alarm once a frequency of noise or vibration within the range emitted by the breaking of glass is detected. These devices are commonly mounted directly on the glass panes of doors and glass wall partitions. Other variants include thin strips of aluminum adhered to the outer edges of the glass panes; if the glass is broken, it

cuts the circuit created by the metal foil, thus activating an alarm. Or seismic sensors that detect the vibrations generated in the breaking of the glass may be used.

Curtains and Reflective Film

In situations where the content of an agency's offices can be viewed from public areas or from adjunct buildings, the use of curtains, blinds, or reflective film should be considered. Protection from onlookers is especially important during the hours of darkness as the interior of offices are brighter than the ambient outside.

SECURE CONTAINMENT

Strong Rooms and Keeps

A *strong room* is an area within a building that has been constructed to hold items of value. In the business and financial world, these items can include cash, jewelry, precious metals and stones, artworks, guns, pharmaceuticals, and so on. In the world of defensive counterintelligence, it is information contained in documents and digital records that are the concern, although artifacts may fall into this consideration from time to time.

Strong rooms are also known by the terms *keeps* and *vaults*. In medieval Europe, a *keep* was a place with a castle fortress that was heavily defended. As such, these areas held the castle's food and water, as well as the armory; the reason for this was to provide an area to retreat to during sustained attack or siege, thus increasing the inhabitants' chances of survival.^[4] Nevertheless, whatever the term used, their intent is the same—to protect the items placed within from unauthorized access and theft. Strong rooms differ from safes in that strong rooms are purposely built into the design of the building, whereas safes are smaller, independent storage devices that can be moved if the need arises.

Safes

Safes are intended to offer varying levels of protection for documents and other classified items, for instance, classified electronic devices such as secure two-way radio equipment and secure cell telephones. Safes are generally constructed with an inner and outer casing of hardened steel plate, with the cavity between the two layers filled with steel-reinforced concrete (and other refractory materials to aid the maintenance of physical strength in intense heat). The level of protection from attack is categorized in different ways, but the level designation indicates the amount of force required to breach the safe and/or the time required to effect the breach. For instance, a safe holding a low security level may be breached with hand tools such as hammers, punches, and chisels, by hydraulic prying, or with pressure tools. A safe of a higher security level may require the use of an oxyacetylene cutting torch, a high-speed drill, a diamond-grinding wheel, or explosives. The time frames required to resist attack could range from, say, fifteen minutes to thirty minutes.

Key Control

A system of key control is essential for preventing unauthorized personnel from obtaining or duplicating keys. All existing keys and their corresponding locks should be catalogued. Keys currently issued should be signed for and they should be collected when employees terminate their employment. If a key is lost, the lock or its cylinder should be replaced. It is important not to label keys with their purpose; if necessary, use a color code. The control of keys for an agency's document containers should follow these guidelines.

Illegal Entry

If an agency discovers that its offices have been broken into, the head of counterintelligence is usually called in the first instance, as it is that person who has responsibility for the subsequent reporting and

investigation.^[5] The agency's policy on security will advise whether the investigation is handled within the agency or by an external law enforcement agency. In any case, notification should happen at once. It is important to secure the area and not disturb evidence that may assist the investigation. A guideline for dealing with instances where information has been compromised is outlined in chapter eight (Defensive Countermeasures: Information Security).

SECURITY LIGHTING

A lighting system is more than just providing adequate illumination to conduct business; it acts to provide deterrence and detection. Without lighting, the countermeasures taken to establish barriers are placed under increased risk of penetration. A good lighting system should be designed to perform four essential functions:

- provide sufficient illumination to deter entry and make detection certain;
- provide redundancy in case of failure of any one of the many single light sources that might otherwise leave a dark area in the coverage area (this assumes there is an auxiliary power source for the installation being protected);
- eliminate heavily shadowed areas; and
- withstand efforts directed at its intentional destruction.

Sensor Lighting

Some Positives and Negatives of Motion Sensor Light Switches

Benefits	Drawbacks
Movement activated, thus providing surprise	Their installation is known to intruders
Can form part of a wider alarm or CCTV installation	False trigger by animals and wind-driven debris
Can save power costs as lights are only switched on when required	Require regular checking for proper operation

Motion sensors can be wired into the power circuit of a lighting system to surprise intruders through immediate illumination of an area. Although the sensors are visible to intruders, the sudden illumination provided by the sensor switches can place the intruder in a position that subjects them to time pressure to react. It is in the immediacy of the reaction that errors can be made in exiting the area, and, if CCTV recording is used in conjunction with the sensor lights, there is evidence for counterintelligence investigators. Motion sensors can be switched to operate either manually or automatically, or switched to the off position. They are suitable for *floodlighting* (illumination over a large area) or spot lighting (direct light onto a specific location or item).



Floodlighting at a building's pedestrian gate entrance.

Courtesy of the author.

CLOSED CIRCUIT TELEVISION

Over the years there has been steady growth in the development of technologies relating to closed-circuit television (CCTV). The use of CCTV cameras in crime prevention is well documented in the security literature, and these cameras can now be seen in public places of all

descriptions—shopping and business districts of cities and towns; train, tram, and subway systems; retail stores; public buildings; and parking lots.

Research shows that offenders understand that CCTV images can be used to identify them and can be used in the prosecution of cases before the courts. This research indicates that, if an offender understands that the visual evidence from a CCTV system will be used to identify and capture them, they perceive these systems as a credible threat, and they, thus, act as a deterrent. [6]

Because of the range of equipment available commercially and the ways that the components can be configured, it is not possible to review them here. Nevertheless, the key aspects of a good system are: visual coverage; quality of the recorded images; monitoring (including remote, delayed, and real-time) and storage of the digital images; export of the images; and flexibility so that authorized third parties can easily view the images. System design should be site specific, and the degree to which the key aspects just cited are incorporated into the system will be based on the level of protection required. That is, the level will be in line with the classification of the data being protected.

Whether a CCTV system is installed inside the agency or outside, the quality and placement of the cameras and their associated components need to be considered carefully. Assume that all video images will be used as evidence in legal proceedings; therefore, the system needs to be of a high standard and installed so that positive identification can be made and recorded. Procedures for handling, copying, or duplicating the video images, and the safe storage of the tapes or disks also need to be considered as any court of law will want to be assured that others did not inadvertently alter the images. This is known as the *chain of evidence* or *chain of custody* and is an important concept in counterintelligence investigations (see appendix D).

There are a number of factors that influence an agency's ability to capture high-quality video images that can be used to prosecute a matter in court. First is the quality of the CCTV camera itself—it must be at the upper end of devices that are on the market. Inexpensive equipment may not be robust enough to perform to legal standards.

Images for use in courts need to provide recognition, detection, and movement monitoring and be of high quality.



An example of a ceiling-mounted CCTV camera in a reception area of a building. Housed in a protective dome, this camera has pan, tilt, and zoom features.

Courtesy of the author.

Recognition

The camera should be installed so that it will provide an image of a suspicious person's head and shoulders. This is usually done as the person enters the restricted area. If a height marker is placed in the entrance way of the restricted area so that it too is recorded in the video frame, this will provide counterintelligence investigators with height, along with identity. The location of CCTV cameras is categorized by purpose; that is, to observe, to detect, to recognize, or to identify. Not all cameras would be likely to have the enhancement image resolution to identify, as some cameras may be needed simply to observe the pattern of entry or exit or the movements within an area. Another camera could provide identification.

Purposes of CCTV Surveillance

<i>Purpose</i>	<i>Image Size</i>
Observe	The target person or vehicle should appear as an image at about 5 percent of the viewing height of the CCTV monitor.
Detect	The target person or vehicle should appear as an image at about 10

	percent of the viewing height of the CCTV monitor.
Recognize	The target person or vehicle should appear as an image at about 50 percent of the viewing height of the CCTV monitor.
Identify	The target person or vehicle should appear as an image at about 120 percent of the viewing height of the CCTV monitor. At this resolution the image of the target should be of a quality that will permit counterintelligence investigators to identify the target individual or provide confirmatory details to the level of a vehicle's license plate number.

Detection

Cameras can provide an image of the person as they move in or around a restricted area and will provide counterintelligence investigators with evidence that the person of interest was within the location of interest (e.g., a safe or filing cabinet, computer workstation, etc.). The position of the cameras in these areas should show the person's presence in the restricted area with a clear images of his or her face as a court will want to satisfy itself that it is the same person that entered the agency's restricted area. Even if these images are not used in a court of law, counterintelligence investigators planning an offensive operation, rather than a criminal prosecution, will need to assure themselves of the same.

Monitoring

If the agency's restricted zones are large areas, such as entrance areas, lobbies, car parks, and queuing lines, cameras that cover these areas need to provide evidence of a person's movements in, out, and around. For instance, if an agency was considering CCTV for its employee car parking area, then cameras should be installed that can monitor the approach to the car park, its entrance, and the parking bays on the lot. These cameras would show vehicles as they entered and exited. Other cameras should then be placed so that they record the license plate numbers of the vehicles and, if possible, the driver's face behind the steering wheel.

Image Quality

The clarity provided by CCTV cameras is as important as its mounting location. A dirty lens will distort the images. An out-of-focus lens will also produce image degradation, so maintenance is important. Ensuring the camera is not pointed into floodlights or the sun is critical in order to avoid the iris of the lens closing down and making the images dark and indistinguishable. Likewise, pointing the camera into dark areas without adequate lighting will produce equally poor results. A constant, yet adequate lighting source is important to image quality.

Signage

To further enhance the deterrent effect of CCTV, the agency should display signs at the entrances of restricted areas indicating that the area is under CCTV surveillance.



Illustration of CCTV surveillance camera signage.

Courtesy of the author.

Placebo CCTV Cameras

If the agency has assessed the need for CCTV cameras, then it is viewed as false economy, and false utility, to install *placebo cameras* (these are also referred to as *decoy cameras* or *dummy cameras*). A view shared by security contractors is that the extra money associated with

installing fully operational cameras is worth more than the marginal advantage, if any, of a decoy camera. Research shows that there may be some deterrence effect, but that it is reasonable for a well-prepared intruder to differentiate between a real camera and a decoy.^[7] If this happens, the deterrent effect afforded by CCTV could be lost and the agency may become an attractive target as it is clear that it has less protection than what is being projected.^[8]

INTRUDER DETECTION SYSTEMS

Intruder alarms will not prevent the physical entry of the opposition's agent; however, installation of a system could add an exponential level of deterrence. But the concern here is not the protection of tangible assets, such as cash, precious metals, artworks, or goods that could easily be converted to cash, but rather the protection of information. Protection of tangible assets may require an alarm system configured differently.

By installing an intruder detection system, the intention is to achieve a level of security in line with the level of sensitivity of the information being protected, not absolute security. It should be kept in mind that the opposition's agent will gain a greater advantage by obtaining the targeted information without the agency's knowledge. It is therefore less likely that entry into an area or document storage container protected by an alarm would be attempted as it would alert the agency to the fact that sensitive information has been compromised. Nevertheless, it is possible that the opposition's agent could disguise such a penetration as a simple burglary targeting property, or even an act of vandalism, hoping to throw any subsequent investigation off the track.

Not all areas of an agency's offices must have a high level of physical security in order to protect their sensitive documentary information. A particular office or meeting room can be designated as *the* area in which the most sensitive information is held and other offices can retain lower-level documents used routinely. In this example, only the secure room would need to be considered for an intruder alarm system.

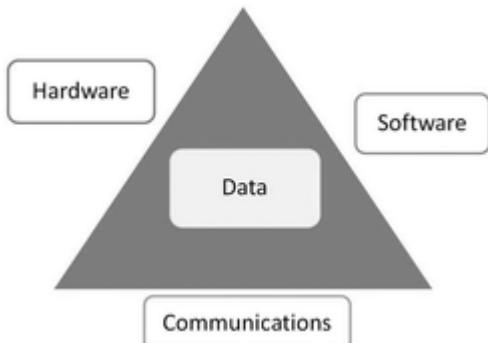
This same principle applies to electronic eavesdropping. A particular office or meeting room can be reserved for confidential discussions. Likewise, only that room would need to be fitted with an intruder detection system (and possibly soundproof insulation). If the agency is small and on a restricted budget, such a secure room may be used for both sensitive meetings and the storage of confidential documents (but not labeled or identified confidential for obvious reasons).

Type of Detection Sensors

There are two basic types of intruder detection devices; the *passive infrared* (PIR) and the combination passive infrared and microwave (*dual technology* or DT). PIR devices are designed to detect temperature variations and, in the case of intruders, this would be from the thermal radiation emitted by their body. DT devices can detect both temperature variations and movement. Older versions of these sensors were subject to false positives because of changes in temperatures—heating and cooling. But the DT sensors monitor temperature variations, as well as movement, through the transmission of microwaves. The microwave component operates on the Doppler principle, similar to radar. In order to activate the alarm, both of these sensor elements are required to be triggered; thus the combination acts as failsafe.

COMPUTER PHYSICAL SECURITY

Computer security is a complex issue. It is comprised of a number of areas of concern, from the physical security of the hardware and their installations to the way the software applications run on these systems and the way data is sent to and received from remote computers and other networks. But, here, defensive counterintelligence is concerned with making the nodes, or access points, to these electronic systems and, hence, data they hold secure from unauthorized access by the opposition. This three-sided relationship is shown diagrammatically in figure 6.9.



Computer Security's Three Main Areas of Concern—Hardware, Software, and Communications.

Courtesy of the author.

As there are numerous hardware configurations based on a wide range of manufacturer models and industry standards, it is not possible to canvass these in detail here. Nonetheless, it is possible to talk in general terms about the essential countermeasures that will provide high levels of computer physical security. Here is what could be argued to be the top eleven countermeasures:

1. Lock the computer base unit to the workstation or, if it is a server, lock the server room. This applies to the most important network devices such as the switches, hubs, and routers, as well as the modems, gateways, and firewalls. The cases for many desktop computers come with quick-release fasteners to aid technicians making repairs, but these will also allow quick access to the computer hard disk drive by unauthorized persons. Cases should be locked closed.
2. Mount all computer and communications devices within the server room in racks. This adds an additional layer of security, especially if the cabinets are themselves locked and the devices mounted in the racks are bolted to the frames rather than fastened with quick-release hardware.
3. Require a log-in for desktop computer terminals and log entry into and exit from server rooms. If the computer terminal is in a public location like a reception area, require card access or biometric log-on, in addition to password protection. Position computer monitor screens in a way to prevent viewing from

windows, doorways, or glass partitions, as well as by any nonauthorized persons in, say, a reception or waiting area.

4. Install CCTV surveillance in the server room so that it digitally records images of all who enter and leave, in addition to their movements within the room.
5. Disable computers that are not in use. Equip computers that must remain in open areas, sometimes out of view of employees, with smartcard or biometric readers so that it is more difficult for unauthorized persons to log on.
6. To limit the possibility of staff copying data to removable media such as CDs, DVDs, or USB drives, disable these drives and ports. There are commercial products that will physically disable these drives and ports and there are software solutions to do the same.
7. Portable computers, such as notebooks and netbooks, present particular concerns, as these devices are taken away from the security of an agency's buildings where, under the tenet of defense in depth (tenet ten of defensive counterintelligence), physical security is high, and into the field where hostile threats exist. For instance, the portable computer can be stolen along with all the data it holds. If the computer is programmed for agency network access, these data will be stolen also. Therefore, the hard disk drive needs to be protected with a high level of encryption so that access would require years to decrypt the partitions, the operating, programs, and data. This is known as *full disk encryption*. Handheld devices need secure storage in safes when not in use. They present the same problems as portable computers and more as they can be inadvertently left by the user in, say, a café, bar, or restaurant.
8. Allow only trusted and qualified technical personnel to service or make modifications to a computer system.
9. Conduct electronic countermeasure sweeps at irregular intervals for "bugs" or wiretaps.
10. Shield cables leaving the server room in metal conduit to prevent electromagnetic radiation, which could be intercepted, and to deter illegal tapping.

11. When disposing of old hard disk drives, use a commercial disk cleaning software package that writes zeros over the entire disk surface. This will leave the disk useable but no data will be recoverable. If the aim is to destroy the disk, then, after using a software cleaner, drill four holes (e.g., at twelve o'clock, three o'clock, six o'clock, and nine o'clock) through the unit so that each hole punctures the magnetic platter.

Finally, the security measures that an intelligence unit adopts to protect its computer systems should not be discussed with anyone outside of the agency. It is acceptable, however, to acknowledge that measures to combat espionage and sabotage are in place, but the specific techniques and procedures should never be confirmed.

Video Display Units

To a large extent, flat screen technology has eliminated the problem that once existed with cathode ray tube (CRT) computer monitors. That is, the older video display units (VDUs) were prone to image *burn-in*. This phenomenon became evident when images of the data being displayed were electronically etched into the phosphor on the inside of the unit's screen during use. Therefore, these older VDUs needed to be inspected for signs of burn-in prior to disposal, resale, or transfer to other more open areas of an agency's office, such as a reception area. If an agency still uses CRT monitors, sound security advice would be to immediately replace these with flat screen technology.

GUARDING SERVICES

General Considerations

A *security guard* is usually a person employed to provide protection services for people, property, and valuables. They are sometimes called *security officers*, but, whatever the term used, they should not be confused with *bodyguards*, who are employed specifically to protect a

person from direct violence. Although security guards may have as part of their duty statement the protection of people, such function is usually discharged by alerting them to the need to evacuate in case of fire, providing first aid, or observing and reporting to a law enforcement agency threats posed by people acting criminally.

Guards are usually in uniform and can be hired by the agency itself or by a third party that provides the guards' service to the agency under contract. Their presence is, in the main, to provide deterrence. They also provide compliance with policy, practice, and procedures by detecting breaches and reporting. But, more important, they can and should act to help educate agency employees by providing polite and helpful instruction with regard to how best to adhere to the agency's security policies.

Although a security guard's function is to observe and report breaches to police, security guards in many jurisdictions that have a legal framework based on common law can make arrests under the doctrine of what is known as a citizen's arrest. Moreover, some jurisdictions have passed legislation that grants all citizens the power of arrest.^[9] In some jurisdictions, security officers can be deputized as sheriff's officers or special constables (or other functional titles) in order to act as agents for law enforcement agencies. This is usually done in a limited capacity within the building's precinct, including the grounds immediately adjacent to the building (i.e., land owned or controlled by the agency).

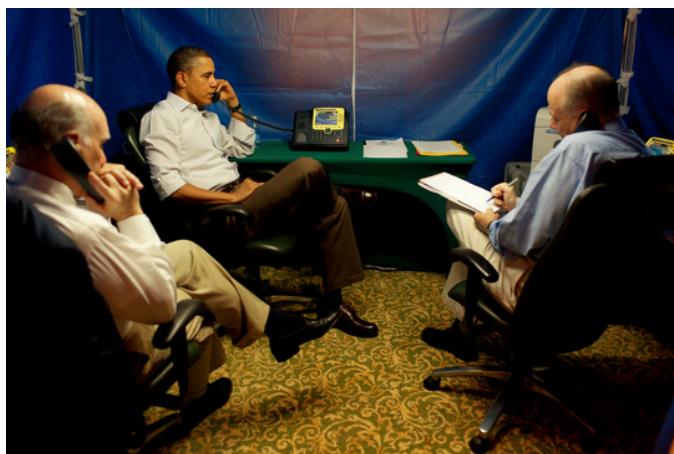
Security guards prevent breaches to a large degree by their presence. They provide observation via static observation, as well as patrols inside and outside of the agency's buildings. The advantages of guard service are many, but the chief reason is that it places a rational person at a site of high vulnerability or risk who is able to assess, and respond appropriately to, a particular situation.

SENSITIVE COMPARTMENTED INFORMATION FACILITY

A sensitive compartmented information facility (SCIF, pronounced *skiff*) is an area, or a room, or an installation where sensitive information can be stored, used, discussed, or processed. A SCIF can be a permanent

working area or a temporary working space. In either case, the specifications, its construction, those who can access the area, and the procedures for its operation are set out in directives, policy, or technical manuals.

From a counterintelligence point of view, one of the key aspects of its construction, as well as its access, is the attenuation to sound and electromagnetic radiation from the work area. The SCIF is essentially a safe haven where classified work is carried out, so the facility, whether permanent or temporary, needs to be proofed against the inadvertent overhearing by unauthorized persons. The techniques for acoustical protection and sound masking can be simple or elaborate and will vary with each installation. The important consideration is that the acoustical countermeasures are in line with the risk assessment for the users and the level of information being used.^[10]



President Barack Obama is pictured here in a temporary SCIF that was set up in a Rio de Janeiro, Brazil, hotel room. Here the president is seen being briefed on the revolution in Libya, March 20, 2011. Chief of Staff Bill Daley is pictured on the left and National Security Advisor Tom Donilon is on the right.

Photograph by Pete Souza. Courtesy of the Executive Office of the President of the United States.

SAFE HOUSES

A safe house is a building that is controlled by the agency. It offers agents and intelligence officers a secure place to meet and stay that is out of harm's way by the opposition. Recall the second underpinning of the theory of counterintelligence—the *axiom of data collection*—which

states that the opposition will use various means to collect data on an agency's operations. The safe house is therefore a means for providing a venue that hides operatives and the meetings they have, including pre- and post-covert operational activities.

Safe houses have been used throughout history—from biblical times to the present—to protect participants who were involved in secret operations. Take, for instance, the hiding of the late dictator of Iraq, Saddam Hussein. He was harbored in various safe houses while Coalition Forces searched for him. Finally, he was located on December 13, 2003, hiding in a secret underground “spider hole” (i.e., a one-man, foxhole-like hide) at a farmhouse in the village of ad-Dawr, which is near Tikrit, Iraq.

At first thought, a spider hole may seem to have been an odd place to consider as a safe house as it employed none of the physical security measures discussed in this chapter—fortified doors, locks, barbed wire, CCTV, and others. But it is the absence of these obvious security treatments that make a safe house safe. That is, the theory of safe houses is that, if the facility blends in with its surrounds and calls no attention to itself, then it is unlikely that anyone viewing the facility will notice it. *Hide in plain sight* is a phrase often used to describe this technique. The key determinant for a facility to be considered a safe house is secrecy.

Although secrecy may seem an easy requirement to meet, in practice it is not. For instance, if a safe house is being established for the first time, then there will be people who will wonder what the facility is being used for. For example, real estate sales or rental agents will be asking what the buyer or renter has in mind for the property. And this is only the beginning. Think of all the utility companies that will need to be contacted to organize light, power, water, and gas. With each contact come questions and the production of identification, and so forth. Each contact raises the risk of a breach of secrecy. Accordingly, a well-developed cover story is essential. If the agency has a large budget, safe house establishment and maintenance can be done by dedicated staff whose job is to plan and carry out these counterintelligence support operations.

Sometimes commercial businesses are used as cover for safe house activities. Take, for example, a business that owns a warehouse; this facility could be used to store equipment as the comings and goings of trucks and personnel would look no different from normal trade or commerce. A private bed-and-breakfast (B&B) could be used as a safe house as “guests” come and go regularly. Operatives could use the B&B as a place to conduct meetings or as a staging point for pre- or post-operations, and so forth, as no other guests would be using the B&B, as its sole function is to serve the agency.

But maintaining secrecy of a safe house, even if a commercial cover is established, is also difficult as operatives may be followed to the safe house or the safe house may come under surveillance. As such, consideration needs to be given to countermeasures, which would include policies and procedures for dealing with suspected cases of surveillance and guard against the inadvertent drawing of attention to the safe house. Once the safe house’s cover is “blown,” it is a time-consuming and expensive task to decommission it and establish a new venue.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

Crime prevention through environmental design (abbreviated as CPTED and pronounced *sep-ted*) is the application of architectural design and space management concepts to prevent crime. In this regard the CPTED concept has application to the work of counterintelligence. Although crime prevention theory incorporates other strategies, counterintelligence officers could gain much from studying CPTED principles and practices.

CPTED was coined by criminologist Dr. C. Ray Jeffery in 1971 in his book *Crime Prevention Through Environmental Design*.^[11] The purpose of CPTED is to attempt to influence a person’s behavior prior to committing an act. Specifically, it looks at prevention of the commission of a criminal act, but, in the case of counterintelligence, this would be the unauthorized disclosure of sensitive information or related disloyal or treasonous acts (which may also be a crime). The basis of CPTED strategies is that it increases the risk of the perpetrator being detected

and apprehended. Deterrence is one of the principles of counterintelligence theory, so it can be seen why the application of CPTED is so apt.

There are three overlapping strategies involved in CPTED and these comprise: natural access control; natural surveillance; and territorial reinforcement. Although these topics will not be covered in this book, it is worthwhile to briefly examine one of these as a means of demonstrating CPTED's application to defensive counterintelligence. Take, for instance, natural access control. According to the late criminologist Timothy D. Crowe, natural access control includes designs that control movement by directing it in certain ways, or restricting it: "create one-way in and out to promote the perception of potential entrapment for abnormal users of space."^[12]

There are complementary strategies for crime prevention that include Social Crime Prevention, Situational Crime Prevention, and Community Crime Prevention and these are worth examining in cursory fashion as a way of rounding off this review of CPTED.

Social Crime Prevention

These are strategies that are aimed at addressing the causes of crime and the dispositions of individuals to offend and engage:

- family-based interventions;
- training and education;
- youth work; and
- employment opportunities.

Situational Crime Prevention

Situational crime prevention includes strategies that focus on the design and management of the physical environment in order to reduce the opportunities presented for crime and to increase the likelihood of detection.

1. Security measures that remove the opportunity to commit an offense and/or make it more difficult to commit an offense by:
 - target hardening;
 - removing the target; or
 - removing the means of committing an offense.
2. Strategies that reduce the incentive for a person to offend while increasing the chances of detection by:
 - permanently marking property;
 - formal/informal surveillance; and
 - natural surveillance.

Community Crime Prevention

These are strategies that combine both social and situational crime prevention measures and are aimed at influencing behaviors in order to reverse “decline” in the physical environment in order to increase the capacity of the community (which may include residents and potential offenders) to exert a greater degree of control over this environment and their lives. These strategies may include:

- housing policies; and
- community development projects and services.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Access cards;
- Burn-in;
- CCTV;
- Chain of custody;
- CPTED;
- Dual technology sensors;
- Floodlighting;

- Flush bolt;
- Glass-break detector;
- Hide in plain sight;
- Lock picking;
- No-go zone;
- Passive infrared sensors;
- Perimeter beam;
- Security guard;
- SCIF;
- Speed style; and
- Vaults.

STUDY QUESTIONS

1. Describe two goals that perimeter fencing achieves.
2. Describe two situations where glass-break detectors could be used to improve security.
3. Explain why a counterintelligence security officer might consider a dual technology sensor over an infrared sensor.
4. List the four purposes of CCTV surveillance and describe the image size required to facilitate each.

LEARNING ACTIVITY

In the context of your current office environment, take stock of the physical security measures afforded the desktop computers in your immediate area. Then, using the list of the top eleven physical security countermeasures, rank the level of security in place. Do this by drawing up a table with the eleven suggested countermeasures represented in rows. In a column, note whether the countermeasure is complied with, or not. If the countermeasure is not complied with, list in another adjacent column your recommendation as to how best the countermeasure could be achieved, and include at the end an estimated cost for implementation. In a fourth column, estimate the costs that would be incurred if the data contained on the desktop computer were “compromised” by not having the countermeasure. That is, what would

the estimated value of the information be in the hands of the opposition, or what “damage” could it cause if it was released to the public domain or another metric of “loss”? The object of the learning activity is to demonstrate the value of security by looking at one aspect. This exercise can be conducted for the other defensive counterintelligence countermeasures—barriers, doors, and window treatments, along with others.

NOTES

- [1.](#) Commonwealth of Australia, *Protective Security Manual* (Canberra: Commonwealth Government Printer, 2005), i.
- [2.](#) Anil Jain, Ruud Bolle, and Sharath Pankanti, “Introduction to Biometrics” in *Biometrics: Personal Identification in a Networked Society*, ed. Anil Jain, Ruud Bolle, and Sharath Pankanti (Norwell, MA: Kluwer Academic, 2002), 16–17.
- [3.](#) Jain, Bolle, and Pankanti, “Introduction to Biometrics,” 16–17.
- [4.](#) See, for example, Roger Stalley, *Early Medieval Architecture* (Oxford: Oxford University Press, 1999), 86–91.
- [5.](#) Toilets and other out-of-the-way places within an agency’s building, whether in a security area or not, should be checked at the end of the day’s business for intruders who may be hiding there to launch their attack.
- [6.](#) Brandon Welsh and David Farrington, “Public Area CCTV and Crime Prevention: An Update Systematic Review and Meta-Analysis,” *Justice Quarterly* 26, no. 4 (December 2009): 716–45.
- [7.](#) Ronald V. Clarke and David Weisburd, “Diffusion of Crime Control Benefits: Observations on the Reverse of Displacement,” in *Crime Prevention Studies, Volume 2*, ed. Ronald V. Clarke, 165–83 (Monsey, NY: Criminal Justice Press, 1994).
- [8.](#) Placebo, decoy, or dummy cameras are intended to give the impression that the area is under surveillance when it is not. As such, some lawyers have argued that the installation of these cameras could create a civil liability. That is, it could create a risk in cases where a person is attacked, hurt, or injured in what would have been the view of the camera had it been operational. Here, a plaintiff could contend that he or she had a reasonable expectation that security would have responded to help. For instance, see Ron Lander, “Cheap Trick: Are Fake Video Cameras Inexpensive Solutions or Lawsuits Waiting to Happen?,” *Campus Safety Journal* 10, no. 9 (2002): 16–17.
- [9.](#) See note 10 in chapter 5 for a discussion of this power, but note that this is an academic discussion and should not be construed as legal advice.
- [10.](#) See, for instance, Director of Central Intelligence, *Directive Number 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities* (Washington, DC: CIA, November 18, 2002).

[**11.**](#) C. Ray Jeffrey, *Crime Prevention Through Environmental Design*, 2nd ed. (Beverly Hills, CA: Sage, 1977).

[**12.**](#) Timothy D. Crowe, *Crime Prevention Through Environmental Design*, 2nd ed. (Boston: Butterworth-Heinemann, 2000), 55.

Chapter 7

Defensive Counterintelligence: Personnel Security

Chapter 7 7 Defensive Counterintelligence: Personnel Security

This topic describes the essentials of personnel security by examining:

1. Introduction;
2. Central pillar of personnel security;
3. Types of harmful disclosures;
4. Hiring practices;
5. Nondisclosure agreements;
6. Background investigations; and
7. Key security obligations of employees.

INTRODUCTION

History has shown that one of the greatest openings for the opposition to infiltrate an agency and acquire its secrets is through trusted staff. There are two groups of people who fall into this category: those who set out to penetrate the agency from the beginning by trying to get hired and then compromise security, and those who are “turned” at some stage in their careers and then steal classified data. In the former group are the likes of the Soviet spies Kim Philby, Donald Maclean, Guy Burgess, and Anthony Blunt; and in the latter group are those spies who turn against their country for money—Aldrich Ames and Robert Hanssen. The purpose of personnel security is therefore to determine whether a person can be trusted with secrets or to carry out secret operations, and remain loyal afterward in order to maintain those secrets.

CENTRAL PILLAR OF PERSONNEL SECURITY

The central pillar regarding personnel security is this: ensure that the staff who work for the agency do not inadvertently disclose secrets, intentionally reveal classified information, or (in extreme circumstances) use that information in violent action against the agency's facilities, processes, or personnel. Take, for instance, the case in July 2011 where a trusted police official used his position of trust and insider knowledge to assassinate Ahmed Wali Karzai, the politically influential half-brother of Afghanistan's president Hamid Karzai, thereby undermining the country's slow progress to democratic rule.^[1]

Intentionally revealed information is different from whistleblowing—what is at concern here is the notion of selling secrets for personal gain, or trading secrets for ideological reasons. So, personnel security is not about control per se, but about the management of personnel who generate or use information to support or make decisions. It is about the prevention of poor hiring practices—practices that could lead to the employment of unethical people who may disclose confidential information—and the frustration of any attempt at penetration by an opposition agent.

TYPES OF HARMFUL DISCLOSURE

The amount of information that one has access to at work is quite sizable. And every business enterprise has vast amounts of information—whether they are a private sector business, a nongovernment organization, or a government agency. Even individuals hold secrets—about their bank details, the money they earn, what they buy, where they go, who they know, what their health is like, what their interests are, and many matters. In most cases these details are benign, but, in the hands of the opposition, these data can be used to devastating advantage.

HIRING PRACTICES

What Positions Require a Security Clearance?

Positions that require security-cleared personnel are those that generate, use, or handle classified data. Take, for example, intelligence analysts: they generate classified reports and use classified information in the process—so they need security clearances. Managers and policy- and decision-makers use classified reports—so they too need security clearances. The list is long, but suffice to say that anyone with access to classified data requires a clearance (including janitorial staff, as technically they too have access to data, even if it is indirect through being in the same room as intelligence analysts who are using that data).

Positions that require security classification can be in the military or government service, the private sector, or even those held by individuals who work on contract to any of these agencies. Recall the typology of counterintelligence discussed in chapter two—national security, military, law enforcement, business, and private. All of these employment sectors are environments of security-cleared personnel.

Screening Personnel

The screening process for personnel should start at the application stage with the applicant completing a detailed personal history statement (sometimes abbreviated as PHS). The reasoning behind this is to provide counterintelligence screening staff with enough information to verify that the person is who they claim, and has the necessary personal integrity to maintain confidences. In addition to the applicant's full name, current residential and business address, and date and place of birth, the PHS can include such subhistories as:

- residential history;
- educational history;
- marital history;
- citizenship history;
- employment history;
- military history;
- financial and credit history; and
- criminal history.

Other details that might be addressed include membership in organizations, and character, professional, and credit references. (See appendix A for an example of a personal history statement.)

When staff review the applicant's personal history statement, they are looking for any inconsistencies, discrepancies, or unaccountable periods of several months or more. If discovered, these should be verified. Even though an applicant may pass this initial screening process, once he or she is hired a probationary period should be set as a contingency for their possible dismissal should there be evidence of them being a security risk. Similarly, when an employee is promoted or assigned to sensitive duties, a screening procedure should be conducted. This screening process should cover the time elapsed from his or her initial hiring to the present. This is to ascertain if any factors during the promotee's recent past could place in jeopardy the confidentiality of the information he or she will be handling.

NONDISCLOSURE AGREEMENT

A standard means of safeguarding sensitive information is by drawing up a nondisclosure agreement. Sometimes these are also termed *secrecy agreements*. These agreements are intended to create a psychological impression on employees, reinforcing the importance of protecting information with which they have been entrusted. These agreements are in effect legal contracts and can be used as evidence in legal proceedings if an employee is found to be in violation of it (see appendix B for an example of a nondisclosure agreement). Nondisclosure agreements should be considered for temporary clerical staff, contract cleaners, indoor plant gardeners, and the like.

“Ask me about my vow of silence” —bumper sticker

BACKGROUND INVESTIGATIONS

A background investigation is the gold standard for security clearances. They are conducted to demonstrate an applicant's ability to reliably

hold confidential information that if revealed could adversely affect the agency or the state. The background investigation helps establish that the applicant is trustworthy, of good conduct and character, and a loyal citizen.

The background investigation involves counterintelligence investigators systematically checking the details of the personal history statement and/or a questionnaire, and then contacting former associates, employers, and other individuals listed by the applicant. But it needs to be borne in mind that, by and large, people who apply for security-classified positions are honest, law-abiding citizens. These people are fellow citizens who pay taxes, live decent lives, and are worthy of the agency's respect in every way. The background investigation therefore needs to be carried out in the most ethical and respectful manner.

Some, however, have issues or have committed infractions that will preclude them from selection. In conducting a background investigation the counterintelligence investigator is looking not at singular infractions or the isolated lapse of judgment to "catch a person out," but at a combination of factors that present a clear picture that the person is likely to be unstable—that is, not trustworthy and disloyal. This is a distinction that has not always been made well—"Careers of loyal officers have been destroyed on the basis of suspicion versus facts, assumptions versus proof."^[2]

Security Vetting Levels

As an *indicative guide*, below in bullet points are four levels of vetting. These levels and their corresponding classification designators may differ from agency to agency and from country to country. However, the point being illustrated is that, with each level of vetting, a more rigorous investigation is carried out. This is in line with the level of risk posed by the unauthorized disclosure of information. A detailed discussion of security classification levels appears in chapter eight (Information Security). But, for the purpose of understanding the vetting

process, these four levels, taken from the Australian security context, stand as examples.

- *Baseline Security Vetting*—this involves inquiries that will ensure that applicants are who they claim to be, live where they state on the application, and are not working illegally or committing any other form of deception. This level of vetting is considered suitable for accessing sensitive information at Protected (or Confidential) level.
- *Negative Vetting Level 1*—this involves a number of inquiries that are discussed in the following sections. The number or type of inquiries will differ by agency but generally this level of vetting is suitable for information classified at Protected (or Confidential) and Secret.
- *Negative Vetting Level 2*—this level is likely to be as per negative vetting level 1 but may involve inquiries that go back further in time, for instance, ten years rather than five for level 1. As such, it is suitable for personnel needing access to Protected (or Confidential), Secret, and Top Secret information.
- *Positive Vetting*—as this level permits access to the most sensitive types of information, including cavedated and code-word data, this level of vetting usually requires a more “aggressive” form of inquiry that may include psychological testing, as well as other intrusive inquiries.

Scope of the Investigation

In general, the scope of a background investigation covers the past ten years or until the person was age eighteen, whichever is less. Access to top secret or code-word data may require an investigation beyond ten years depending on the agency and country. The length of time that counterintelligence investigators go back is determined by the risk associated with each clearance category—it is proportional. That is, the

harm that could be caused by unauthorized release of top secret data is greater than that of secret, so the added expense of probing beyond ten years' background information may be warranted.

National Agency Check

A common check of personnel is that of a national agency check. Counterintelligence investigators may routinely check the applicant's record with police agencies on a state/province level, as well as the national police authority. The reasoning behind this is that the applicant may have lived in other jurisdictions and had adverse details reported against him or her. They may have simply visited other areas of the nation and encountered trouble while there. This is common where the applicant is involved in frequent interstate travel with a former employer.

Personal Interview

The purpose of the personal interview is to allow the applicant to clarify issues in their personal history statement or the questionnaire, if a counterintelligence investigator cannot resolve or reconcile a response with other data. It is also an opportunity for counterintelligence investigators to probe areas of possible inconsistencies that are not overt but hold the potential for hiding or telling half-truths (i.e., education qualifications).

But the personal interview is not a “fishing trip” where the investigator asks a stream of questions trying to “catch out” the applicant. The interview is designed to help the vetting process, not bring it into disrepute by trying to embarrass the applicant. The personal interview is not a modern-day version of King Henry VII’s Star Chamber,^[3] nor should the investigator present in the persona of Fyodor Dostoevsky’s the Grand Inquisitor in his novel *The Brothers Karamazov*.^[4]

Birth

The applicant's place and date of birth need to be independently verified as a basis for establishing the individual's identity. This is done by obtaining an original or certified copy of a birth certificate. Such certificates are issued under seal by an office or bureau of vital statistics or a registrar of births for a particular jurisdiction.

This is one of the more important aspects of verifying a person's identity. At one time, false documents were commonly referred to as simply *fake IDs*, and the act of passing oneself off as another character was known as *paper tripping*.^[5] But at the time of this writing this has become known as *identity theft*. Despite the evolution of the term, make no mistake—these documents remain fake IDs.^[6]

"It is very easy for criminals to obtain our personal information and our identities. Everything from low-tech to high-tech is readily available. It seems that not a day goes by without hearing about another news story on identity theft."*

* Martin T. Biegelman, *Identity Theft Handbook: Detection, Prevention, and Security* (Hoboken, NJ: Wiley, 2009), 3.

Citizenship

Verification of citizenship is an important aspect of the personnel security process. This is done for both legal reasons and ideological reasons. Anticipating the worst, if the person subject to the vetting process at some stage in the future discloses information in an unauthorized manner, then having jurisdiction to detain, question, and prosecute the person is an important aspect of the tenets of counterintelligence.

From an ideological point of view, if the person is a citizen of the country hiring him or her, then they may be required to take an oath or swear or affirm allegiance (usually under a specific statute). As strange as it may seem, some people will refuse to provide such an undertaking, thus bringing to a head a potential security issue. It is simple, but

effective. The applicant's immediate family members should be verified also. Immediate family members are usually those living with the applicant or who the applicant has care and control over. For instance, these people may include a wife, husband, or partner, children, and parents or other relatives living with the applicant.

If the applicant has a foreign-born family member in this category, then their citizenship needs to be verified also. The rationale is simple: if the applicant discloses confidential information to these unauthorized people, then counterintelligence investigators will want to interview them and subject them to the legal procedure of the jurisdiction as they would with the applicant. If they are foreign born, then it is doubly important that they are vetted, as their country of birth may be hostile to the agency or the agency's country and have placed pressure on these individuals to obtain information from the applicant via their family ties. This is, of course, country specific—some countries are openly hostile to others; some have strained relationships; and others are close friends and allies. So, the country context needs to be taken into account when considering this factor. It may or may not be an issue of paramount importance.

Educational History

Arguably, this is one of the most falsified areas of a personal history statement. Issues arise when applicants either overstate their academic qualification or fabricate outright the qualifications they hold. There is also the issue involving people who purchase qualifications that appear for all intents and purposes as the ones required by the hiring agency, but are issued by nonaccredited educational intuitions. Nonaccredited colleges and universities that offer these parchments for sale have been described as “diploma mills,” and the credentials they issue are bluntly termed “fake degrees” and “worthless degrees.”^[7]

For instance, if a position within an agency requires the applicant to hold a Bachelor of Arts degree, but the applicant left university in her last semester before graduating, she may not claim to hold this degree. If she falsely claims this, it raises several related issues: she is not

beyond falsely providing information; she may have a low threshold to other forms of deceit; and her low standard of ethics may apply to other areas of her life—both professional and personal, with the latter potentially impacting, in turn, her professional life (e.g., a gambling addiction that may drive her to sell classified information).

Accordingly, counterintelligence investigators need to verify these details. The most important to verify are those qualifications required for the position, or the highest degree/diploma attained. If the applicant's education or trade qualifications were attained outside of the scope of the period required for the security clearance sought, then the applicant's highest degree or diploma beyond high school is usually the only one verified. For instance, if an applicant claims to have attained a Master of Arts degree and this can be confirmed, then there is little point in confirming that they hold a high school diploma, which may have been issued fifteen or twenty years prior.

Employment History

A person's employment history is a telling source of the applicant's on-the-job performance when it comes to issues of security and confidentiality. Telephone interviews with past supervisors and/or co-workers can help verify whether the applicant is able to maintain confidences relating to sensitive work matters. They are also able to verify that the applicant has not been dismissed for inappropriate disclosure of information or issues that are relevant to a security clearance.

Counterintelligence investigators need to be cognizant that poor work reports by former supervisors may be the result of professional jealousies or animosities that have no bearing on the security clearance process. Very bright and highly capable people often get less capably colleagues off-side. This is a fact of work life, but should not color the applicant's vetting report as such motivations can be mischievous. Verification of the past two years of employment history is a usual standard and periods of unemployment that exceed sixty days should be verified.

Military History

In the same vein as an applicant's employment history, their military service dates should be verified from records searches or via the registrar. The most important issue here is the type of discharge awarded the applicant for their service, as it may be a factor in assessing their trustworthiness.

Personal References

These are different from the references who are asked to provide comments on the applicant's ability to perform the tasks associated with the job they applied for. Whether the applicant can perform the job and to what standard is outside the scope of a security clearance. Counterintelligence investigators are tasked security-related issues only. So, with regard to personal references, these are people who know the applicant personally and can speak about his or her ethical behavior.

Neighbors

A check of the applicant's neighbors is akin to a personal references check, except that neighbors are likely to be acquaintances through the neighborhood they share rather than social friends, though this can vary and they may be both. Interviews with neighbors can confirm any adverse behaviors that may not show up through outer checks—for instance, acts of personal violence, criminal activity, and the like. In the case where the applicant has not been at an address for long enough to make contact with neighbors (in the case of frequent movers or apartment dwellers), contact with landlords should be considered. However, some caution needs to be exercised with neighbor checks. As a person cannot select who lives next to them, personal disagreements are common. As such, the counterintelligence investigator should consider with care any adverse information as it may be wrongful or designed to "get even" with the applicant due to some falling-out over a minor residential issue.

Foreign Contacts and Activities

For some security-sensitive positions it is necessary to assess the applicant's foreign contacts. It is important to identify personal or business contacts in foreign lands who may have the potential to pressure the applicant to compromise classified information.

Consideration of issues such as the frequency, intensity, and means of contact (e.g., in person, telephonic, or electronic) will help this assessment process.

Likewise, the applicant's foreign activities may be another indicator of their state of mind and the way they may act in guarding classified information. But just because a person may travel regularly to a place that is at the time seen as hostile to the agency's country does not mean that they are a risk. For instance, there are places in the Middle East, North Africa, and Southeast Asia that could be considered hostile to one country or another. But if the applicant has a spouse who enjoys archaeology as a hobby, they may travel to these countries regularly. In such a case, counterintelligence training, rather than eliminating the individual from the employment selection process, may be all that is required.

Financial and Credit History

Verification of an applicant's financial and credit histories is a sound way of establishing grounds for a stable fiscal footing. Research shows that people who are chronically in debt, spend big, or are unable to maintain a budget often find themselves in financial jeopardy. Such a position could pose a risk to the granting of a security clearance. This is because being in financial difficulty, whether because of spending beyond one's means, gambling, or other compulsions, may place the applicant in temptation's way to sell information as a way to aid his or her financial situation.

This is a generalization and each case needs to be assessed on the facts, but it is a view shared in many security circles based on experience and research findings. Therefore, asset ownership, income, and liabilities

need to be estimated to see if the picture being presented by the applicant is accurate. One way of doing this is using an analysis of net worth.

Net worth is a calculation of the difference between the applicant's assets and liabilities. If the counterintelligence investigator conducts the net worth analysis over a period of time, say, for the end of each financial year, he or she can compile a picture as to whether the target is growing in worth or is experiencing losses and what the magnitude of these gains or losses might be.

The formula for calculating net worth is as follows,* step by step:

1. Assets – liabilities = net worth
2. Net worth – prior year's net worth = increase or decrease in net worth
3. Net worth increase (or decrease) + living expenses = income
4. Income – funds in known sources = funds from potentially illegal sources

* Leigh Edwards Somers, *Economic Crimes: Investigating Principles and Techniques* (New York: Clark Boardman Company, 1984), 99.

Association History

It is unlikely that any applicant with any intellect would admit on their personal history statement membership in a group that has intent to overthrow his or her government through violence or force. Or that they now support, or have in the past supported, organizations that have this as one of their goals.

Nonetheless, the counterintelligence investigator should put these questions to the applicant directly at interview or via a questionnaire.

Untruthful answers lay grounds for dismissal and/or legal proceedings if detected later, as well as provide leads for further questioning if information from any other sources reveals contrary indicators. Public records and open-source intelligence are an important source of such information.

Search of Public Records and Open-Source Intelligence

Open-source data is a valuable source of information that can complement the various history checks and interviews mentioned in the above sections. This may be in the form of publicly available records as well as other forms of “intelligence.”

Government records that show adverse data such as bankruptcy records and civil court judgments are examples. But, as pointed out in chapter one, the Internet is an information-rich environment where people post personal information many years before they realize the gravity of revealing so much personal information. Once posted, it is likely to be impossible to remove/recover.

There are a host of technical reasons for this that is beyond the scope of this book to explain, but suffice to say that, if a counterintelligence investigator searches the Internet, he or she may find information that suggests the applicant may have been involved in subversive activities at one time contrary to the assertions made on the current application.

Social Networking

In sociology and anthropology a *social network* is a social structure that comprises a relationship between individuals and/or groups. These relationships can be based on any number of factors including kinship, friendship, shared interests (or dislikes), political affiliations, business arrangements, and so on. Likewise, networks can also be associated with a set of objects or events. [8]

Although social scientists use the study of social networks to explore practical and theoretical questions relating to their discipline,

counterintelligence investigators can exploit social networking via social networking website services to complement their investigative sources of data. These Internet-based facilities allow people and organizations to meet and maintain contact based on the factors cited by sociologists—kinship, friendship, shared interests, political affiliations, and many others. A report on the social networking service Facebook claimed that the much debated^[9] “six degrees of separation”^[10] between any two people on the globe was, in November 2011, 4.74 using this social networking service.^[11]

It is no surprise then that employers use these services as information-rich sources of intelligence. For instance, an Australian study found that more than a quarter of Australian employers used social networking sites to screen job candidates “with almost half of these employers admitting to turning away prospects based on something they’ve seen on Facebook or Twitter.”^[12]

The issue of having so much personal data freely available online is a problem for security-cleared personnel who ideally should be “keeping a low profile” to avoid any contact, however remote, with the opposition. For instance, the issues that a staffer must consider with regard to physical and personal information and communications security are weighty. However, these issues are almost cast aside when that person places personal information about themselves on the Internet for others to read (regardless of what “privacy controls” are in place to limit viewing of these data).

From the point of view of the counterintelligence investigator who is vetting a potential applicant, these data can be invaluable. However, online social networking services can be a security worry once the person is granted clearance, as their use becomes a potential weakness in an agency’s overall defense. As an example, take the applicant who applies for a position in a covert unit as an operative who will go undercover. However, before joining the agency, that person was a member of a social networking service and posted many facts and comments about herself as well as her photographs at various events. At the time, these were all considered harmless but, now that she is applying for a covert assignment, these data are accessible to society’s

“global outlaws” and can be used against her and her agency. Recall the case of the chief of Britain’s secret intelligence service, MI6, Sir (Robert) John Sawers, who had his personal details along with a number of photographs publicly displayed on his wife’s Facebook page.^[13]

Facial Recognition

If it seems a remote possibility that the opposition will obtain an individual’s personal information on the Internet and then make the connection to, say, a covert operative, then consider the following. According to research being conducted at the time of this writing, “outlaws” are using facial recognition to identify undercover operatives. According to the former Australian Federal Police commissioner Mick Keelty, now a professor at the Australian Graduate School of Policing and Security, Charles Sturt University, and his research colleague, associate professor Nick O’Brien, there is anecdotal evidence that indicates outlaw motorcycle gangs have attended police graduations in one particular Australian state. The purpose was to take photographs of the graduating officers because in years to come some of these officers may become undercover operatives.^[14] These outlaws purportedly used commercially available facial recognition software to scan the images of the people they photograph (or download from social networking web services) and match these with people who they suspect as being a threat (i.e., potential undercover operatives).

If this is the case, then it is not unreasonable to suggest that other global outlaws may mimic this tactic and photograph, say, the graduates of the world’s military academies (e.g., West Point, Annapolis, Duntroon, Sandhurst, etc.) and use the same method to identify clandestine operatives. If this comes about, such a graduate, who is later recruited into a covert unit of an intelligence agency, may find it impossible to explain his or her military service when they turn up at their nation’s embassy in some troubled part of the world under diplomatic cover. In such a case the opposition would have a photograph of them graduating from their nation’s military academy a few years before, with an unexplained absence from the profession they purport to represent in

the interim years.^[15] But it need not be limited to just graduates of military academies. Any potential pool of personnel can be photographed and concealable digital cameras make the job so much more efficient and effective. The list of potential data collection sites for images of people's faces is very long—airport and seaport immigration queues, entrances to government buildings or research laboratories, and the list goes on (consider the wealth of photographic data contained in college and university yearbooks as a start).

Although this is an issue for an agency's defensive counterintelligence program, it is also a gold mine of rich information for the agency's offensive counterintelligence program. Because, what can be done to an intelligence agency, that agency can and should return in kind.

What Should Not Be Considered Adverse

There are two situations that present themselves as issues that should be approached by a counterintelligence investigator with balanced judgment. The first issue is with regard to a person's financial problems and the second involve psychological issues.

Noticing changes in staff behavior may be not only good management but good counterintelligence practice too. Changes in a person's mood or actions may be an indicator of deeper personal turmoil. If, say, a staffer has become more and more argumentative and his or her discussions with colleagues increasingly heated over time, it may mean more attention needs to be paid to find out why this could be happening. Take for instance the case of the alleged WikiLeaks informant, Private First-Class Bradley Manning. Media reports allege that he was suffering from forms of psychological stress before his alleged leaking of some 250,000 classified documents.^[16]

The excessive use of alcohol has been identified as one such indicator. This could potentially give rise to temptation or attraction to compromise information in a misguided attempt to solve personal issues (take, for instance, the case of Aldrich Ames who was reported to have had a drinking problem^[17]). It is not to say that a personal issue or a

drinking problem is cause by itself to not grant or revoke a security clearance, but it does mean that a closer examination is warranted. History has shown that such issues have led, directly or indirectly, to staff disclosing classified information as a way of exacting revenge against the agency, or to bail them out of financial difficulty, or any number of other justifications for these problems (real or imagined).

Getting a person to talk to a counselor who is part of the agency's employee assistance program is a good start to help resolve the problem before it harms the individual or the agency. Such steps are no longer considered in an adverse manner, but are seen as the healthy exercise of good judgment, as they seek to maintain a sound state of mind, as well as a way to keep up work performance. Just because a staffer seeks psychological counseling is not grounds per se for suspicion —it is a sensible move to get life back to normal. In contrast, not seeking counseling may be an indicator that things could get worse.

The same applies to financial difficulties. If a staffer seeks financial counseling and help with managing debt, it is a healthy sign that the person is now taking control of their life and trying to manage their way out of difficulty. Growing debt may give rise to the temptation to, perhaps, sell classified information as a way of clearing the debt. But to be upfront and seek help is an honest way of dealing with an embarrassing issue. Recall that a personal situation like this is similar to the thousands of companies that go into liquidation or bankruptcy each year because management may not have sought financial assistance early enough or tried to manage out of it through other means.

KEY SECURITY OBLIGATIONS OF EMPLOYEES

Fraternization

Interacting with foreign nationals is part of modern-day life. Many of an agency's citizens may even be married or in a long-term relationship with

people born abroad. This is not usually a problem unless an opponent uses this relationship as a means to exploit the agency's employee.

But, in the context of fraternization, what is meant is that a single employee should be conscious that an opponent may take advantage of a person's desire for human contact while living far from home, family, and friends by placing before that person an agent in the guise of a "companion." The term *honeypot* is often used in intelligence parlance to describe this trap.

The case of U.S. Marine Clayton Lonetree is an example of how an opponent can construct a situation where what appears to be a genuinely warm and caring relationship develops, but it is instead an elaborate plot to obtain classified information.^[18] USMC Sergeant Lonetree was convicted and sentenced to a thirty-year prison sentence (later reduced to fifteen years, but released after nine years) for spying. He was reported to have fallen in love with a Soviet intelligence officer while posted to the U.S. Embassy in Moscow in the early 1980s.^[19] This love affair was the groundwork for later blackmail and the revelation of secrets to a foreign intelligence service. Therefore, there is often a "no fraternization" policy in place to guard against these traps. (Although honeypots are clearly applicable to national security and military counterintelligence situations, they can apply in other contexts too.)

Contact Reporting

Agencies should have a policy that requires personnel to report any contacts with opposition personnel services for several important purposes. First, it facilitates the dissemination of the content of the contact—whether it was a personal encounter or a conversation via electronic or telephonic means. The person, what position they hold in the opposition agency, what was discussed, the manner in which it was discussed, and future arrangements to follow up on any issue rise, etc. can be vital insights for intelligence analysts who blend these data with many other pieces of information to answer strategic and tactical research questions.

The second aspect of reporting contact is from a counterintelligence point of view. To the counterintelligence investigator the details of the contact, as well as the method and timing of the contact, may provide

insight into a larger campaign to penetrate the agency. It could tie together other contacts with other agency personnel over time and at different locations.

Protecting Conversations

If the theoretical precept that every piece of correspondence and every record produced by the agency holds some intelligence value for the opposition, then this precept can be extended to conversations. Therefore, if personnel discuss sensitive matters in public where others can overhear, or carry out conversations on a telephone that is not secured through electronic encryption, or have conversations in rooms that are not proofed against technical eavesdropping, then it should be assumed that such conversations are under surveillance.

At first glance this may seem a dramatic conclusion, but the fact is that, unless a technical countermeasures sweep is conducted or a team of countersurveillance operatives are employed, there is no assurance that these conversations are not being surveilled. Any other view is simply wishful thinking. The point to be made is that personnel need to be cautious in any situation that does not carry the assurance that the area is secure.

Surveillance Detected

Physical surveillance is both an art and a science, and the methods for conducting surveillance could fill several book volumes. Therefore, it is meaningless to try and outline every possible type of method that may be employed against personnel of an agency. Suffice to say that surveillance is the following—or *shadowing*—of a person of interest. The general object of surveillance is to obtain details of the person's movements, the times they shifted location, and places they visited. It also includes the people met (or encountered along the way) and things performed or done while in motion or as an event.

The ability to detect surveillance is, like surveillance itself, an art and a science. It requires some level of formal study and training given the fact that surveillance is more than merely following a few steps

behind someone. It is therefore unlikely that an untrained person could notice surveillance. Nevertheless, there are some circumstances where a person may notice a vehicle or person and take further notice, giving rise to a suspicion that they are being watched. If the staffer suspects, or has evidence of, being the target of surveillance, agency policy should advise that they report this to counterintelligence investigators immediately.

Recognizing Physical Surveillance

Physical surveillance is the observation of people and places. There are many purposes for physical surveillance; some of these include obtaining information that may be difficult or impossible to obtain by any other method, confirming information at hand, developing leads, and establishing links between various people and between people and places. The information gleaned from such observations has inherent value in itself. In addition, this raw information can be used to form the groundwork for more elaborate and extensive plans for information gathering.

All employees should be cognizant of the possibility of physical surveillance of their offices and themselves by opposition personnel. Being aware that something is out of place is an excellent way of recognizing surveillance. It is, however, difficult to define "out of place." Persons loitering in halls, lobbies, or stairways, suspicious visitors, frequent passersby, and so forth should always be noted. If, after consideration, such activity is considered to be sufficiently suspicious, the agency's countersurveillance plan for notification should be followed. Employees should also be alert to the possibility of surveillance from the street, adjacent buildings, parked motor vehicles, and areas where employees park their cars.

Agency vehicles themselves should be visually examined occasionally for any signs of "marking" by opposition agents. Identifying marks such as broken taillights, removed lightbulbs, or pieces of reflective tape can permit an agent to distinguish a vehicle in traffic and therefore aid the agent in following the vehicle's movements. Of higher sophistication and much less visible are mobile transmitters. These

devices are usually attached to the underside of a car and can be located by *careful* visual inspection (see appendix C for a list of indicative analog electronic surveillance devices).

Rapid Developed Friendships

In the course of normal social interaction a person may have dozens of personal contacts each day with many people—family members, colleagues, retailers, bus and taxi drivers, restaurant waitstaff, and people they meet in bars and coffeehouses, to mention just a few examples. But from a counterintelligence point of view these contacts are not of interest. There is, however, a class of contacts that are of interest to counterintelligence investigators, and the contact as well as the nature and contact of the conversation are of interest.

The type of contact that is of concern is where the encounter leads to a rapid development of friendship. This is because the person may be trying to position themselves so that they can use their newly formed relationship as a means to obtain classified information. Those who are not schooled in this technique may ridicule it as paranoid, but the literature on penetrating agencies is replete with examples of how this method is used, and with great success.^[20] Policy should be to advise counterintelligence investigators if a befriending person has made suggestive or leading statements that could be a prelude to coaxing, coercing, bribing or blackmailing the staffer into compromising classified data.

Technical Countermeasure Sweeps

One response to the reported suspicion of surveillance may be to recommend that a technical countermeasure sweep of the staffer's house, apartment, and/or vehicle be conducted. Security engineers then use both physical inspection of the premises/vehicle and electronic equipment to detect and neutralize listening and tracking devices—or *bugs*.

Husbands, Wives, and Partners

Although staffer's spouses, whether married or in a de facto relationship, are assumed to be close and loyal to that person, they are not employees of the agencies and are not security cleared. Therefore, agency policy should remind staff that they are not to share classified information with these people.

The policy should draw to staff's attention that this is a potential source for leaks—even though inadvertent—but it also places these people at potential personal peril if they hold classified information in their heads. They become potential targets for exploitation, compromise, bribery, and blackmail, just like any security-cleared employee but without the protection that the employee has.

A Simple Personal Protection Measure

Like surveillance and countersurveillance, personal security is somewhat of an art as well as a science. Unlike a building that can be observed and its vulnerabilities analyzed so that the risks can be treated, people have far more dimensions to them and the lives they lead. Accordingly, to adequately cover the topic of personal security, it may take a sizable manual to address each concern and the different settings. For instance there are texts that cover dignitary protection (close personal protection).

So, from a general perspective, if there was only one simple staff policy regarding the establishment and maintenance of personal protection, it would be to keep a low personal profile. Having a low profile, by definition, lowers your risk to a number of hazards—violent individual and groups, and opposition agents seeking you for exploitation. Former CIA official, Patrick Collins, who planned personal protection programs for high-risk personnel working overseas, offered this advice on how to achieve a low profile: “Profile reduction is achieved by avoiding the public limelight. Basically, this means you should do nothing to incite undue interest in your name, personality, or position.”^[21] Simple advice, but no doubt effective.

PRACTICES TO GUARD AGAINST

Infiltration

A well-known espionage technique used to penetrate an agency is that of *infiltration*. Basically there are four methods of conducting an infiltration—telephone, mail or e-mail, in person, and indirectly.

“The art of using pretexts is a science and should be approached as one.”*

* Greg Hauser, *Pretext Manual* (Austin, TX: Thomas Investigative, 1994), 5.

A *pretext* offers an agent a plausible, common-sense technique for obtaining confidential information. A pretext is any act of deception—ruse, subterfuge, ploy, trick, or disguise—that allows an agent to solicit information by a false reason. This includes entering premises for obtaining information or being in a place (or a country) to which the agent wouldn’t otherwise have access or permission. In espionage the term used for this type of infiltration is *cover*—for instance, official cover or non-official cover.

Pretext should not be confused with the term *social engineering*, which has gained popularity in recent years. Social engineering is a slang term that commonly refers to an individual act of manipulation (usually for fraudulent purposes) to gain access to IT systems. This is vastly different from its true meaning, which is large-scale societal planning. The use of the term *social engineering* in this context is incorrect. The technique is nothing more than a ruse, subterfuge, or pretext. In fact, *pretext* is the term most used by private investigators, who rely heavily on this technique as a means of gaining information about their targets. [22]

Telephone

This method is used by operatives, usually on a one-time basis, to obtain general information about an aspect of the agency's affairs. It is the safest and most innocuous type of infiltration to perpetrate. This type of infiltration is carried out by simply telephoning the target agency, using a pretext, and attempting to extract as much information as possible. Several calls could be made over a period of time. On the surface, individual calls would appear to be unrelated, but each is designed to obtain specific pieces of information. Depending on the pretext and the number of pretext calls made, the depth of information an operative could gather might be limited and confined to general details. However, if the target agency has acute security awareness, especially about unknown persons, the information should be limited to general information that one could obtain on a public website. If the agency is suspicious, a staffer may try to identify a telephone caller by requesting the caller's telephone number and then verifying it by using an online telephone directory before calling the operative back (known as *confirmation by call-back*).

By Mail and E-mail

This is another form of low-grade infiltration. Again, using a pretext, the operative will write to a target agency requesting information. Security-aware targets will look for the warning signs of a mail infiltration, such as the use of post-office boxes, business name "fronts," and out-of-state addresses. As for e-mail, free web-based e-mail accounts can raise the target's suspicions because these are usually nonverifiable accounts.

In Person

Direct personal infiltration of the target may follow pretext contacts by telephone, mail/e-mail infiltration, and physical surveillance. In this way, operatives can gather enough information to establish a credible cover for a direct penetration, or acquaint themselves with the

information needed to recruit an agent (i.e., a proxy) to carry out the task.^[23]

Indirectly

This infiltration method is complex to organize and run, but can yield high-grade results. Basically, an operative creates a covert business or organization that is designed to draw in the target agency or a member of the target's staff. The bogus business is controlled by the operative. These covert enterprises can be as simple as a trade newsletter or as elaborate as a fully operational business. Once established, the operative uses this cover to gather the information required in his or her information collection plan. An example of this is the advertising of positions in a new and very attractive-sounding business. The business may offer a salary and fringe benefits package in excess of those offered in the market in order to entice the target. Once the target's *curriculum vitae* is received, it is analyzed for the desired information. If it does not disclose the information sought, additional information will be requested from the target applicant and/or a personal interview conducted. The operative, or someone from the bogus organization, would then "pump" the target for information.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Background investigation;
- Bugs;
- Confirmation by call-back;
- Honey pot;
- Infiltration;
- Low personal profile;
- Net worth analysis;

- Nondisclosure agreement;
- Paper tripping;
- Personal history statement;
- Pretext; and
- Shadowing.

STUDY QUESTIONS

1. Explain the central pillar of personnel security.
2. Describe the types of harmful disclosures that might be involved for a staffer who is working in (select one): (a) national security; (b) military intelligence; (c) law enforcement; (d) business; or (e) private security.
3. Explain why the types of information items in a personal history statement are important in checking the trustworthiness of a potential employee.
4. Other than personal, psychological and financial issues, discuss what types of situations may not be considered to be adverse counterintelligence indicators *per se*, and why.

LEARNING ACTIVITY

Using *yourself* as a case study, apply the four-step formula for determining a person's net worth to your current finances. Was this difficult? What did you find out as a result? What do you think others could find out if they performed this?

NOTES

1. Alissa J. Rubin and Scott Shane, "Assassination in Afghanistan Creates a Void," *New York Times*, July 13, 2011, A1, New York edition. See also news reports of how other inadequate vetting processes allowed insurgents to infiltrate the Afghan National Army. These infiltrators then launched armed attacks against members of the International Security Assistance Force. For example, in late 2011, several Australian soldiers were killed and others wounded in several of

these attacks (Jeremy Kelly, "Rogue Afghan Soldier Sought for Murder," *The Advertiser*, Adelaide, Australia November 28, 2011, 11).

2. Melissa Boyle Mahle, *Denial and Deception: An Insider's View of the CIA from Iran-Contra to 9/11* (New York: Nation Books, 2004), 134.

3. Theodore F. T. Plucknett, *A Concise History of the Common Law*, 5th ed. (Boston: Little, Brown, 1956), 181–83.

4. Fyodor Dostoevsky with David McDuff, trans., *The Brothers Karamazov: A Novel in Four Parts and an Epilogue* (London: Penguin Classics, 2003).

5. Barry Reid, *The Paper Trip II, For a New You through New ID*, 1980 ed. (Fountain Valley, CA: Eden Press, 1977). This was formerly entitled *The New Paper Trip*. This book was succeeded by Barry Reid, *The Paper Trip III: A Master Guide to a New Identity* (Fountain Valley, CA: Eden Press, 1998).

6. For example, in espionage a fake passport, often the basis for establishing one's identity, is known as a "boot" (or a "shoe") and the forger goes by the term a "cobbler." These expressions are said to have been derived from secret Soviet operations in Europe in the 1930s. See, William E. Duff, *A Time for Spies: Theodore Stephanovich Mally and the Era of the Great Illegals* (Nashville, TN: Vanderbilt University Press, 1999), 70. These terms are still used today in fiction—see, for example, Martin Roberts, *A Terrorist or Patriot* (Lincoln, NE: Writers Club Press, 2002), 52.

7. Lester S. Rosen, *The Safe Hiring Manual: The Complete Guide to Keeping Criminals, Imposters and Terrorists Out of the Workplace* (Tempe, AZ: Facts on Demand Press, 2006).

8. David Knoke and James H. Kuklinski, *Network Analysis* (Newbury Park, CA: Sage, 1982).

9. Judith Kleinfeld, "The Small World Problem," *Society* 39, no. 2 (2002): 61–66. Thomas Blass, *The Man Who Shocked the World: The Life and Legacy of Stanley Milgram* (Cambridge, MA: Basic, 2004).

10. Jeffrey Travers and Stanley Milgram, "An Experimental Study of the Small World Problem," *Sociometry* 32, no. 4 (Dec. 1969): 425–43.

11. John Markoff and Somini Sengupta, "Separating You and Me? 4.74 Degrees," *New York Times*, November 22, 2011, B1, New York ed.

12. Darren Kane, "Aussies Urged to Consider their Cyber CVs as Bosses Head Online," www.telstra.com.au/abouttelstra/media-centre/announcements/aussies-urged-to-consider-their-cyber-cvs-as-bosses-head-online.xml#Links (accessed December 1, 2001). Darren Kane is officer of Internet trust and safety and director of corporate security and investigations with Telstra Corporation Ltd, Australia.

13. Sarah Lyall, "On Facebook, a Spy Revealed," *New York Times*, July 6, 2009, A1, New York ed.

14. Michael "Mick" Keelty and Nick O'Brien, personal communication, October 18, 2011.

15. Michael "Mick" Keelty and Nick O'Brien, personal communication, October 18, 2011.

16. As an example, see the CBS News report, dated February 2, 2011, "Specialist Advised Not to Deploy Bradley Manning," www.cbsnews.com/stories/2011/02/02/politics/washingtonpost/main7309852.shtml (accessed November 24, 2011). See also Andrew Fowler, *The Most Dangerous Man in the World: How One Hacker Ended Corporate and Government Secrecy Forever* (New York: Skyhorse Publishing, 2011), 130–31.

17. David Wise, *Nightmover* (New York: HarperCollins, 1995), 87.

- [18.](#) Rodney Barker, *Dancing with the Devil: Sex, Espionage, and the US Marines: The Clayton Lonetree Story* (New York: Simon & Schuster, 1996).
- [19.](#) William Hoffman, *The Court-Martial of Clayton Lonetree* (New York: Henry Holt, 1989).
- [20.](#) See, for instance, Alex Caine, *Befriend and Betray: Infiltrating the Hells Angels, Banditos and Other Criminal Brotherhoods* (New York: Thomas Dunne Books, 2009).
- [21.](#) Patrick Collins, *Living in Troubled Lands: The Complete Guide to Personal Protection Abroad* (Boulder, CO: Paladin Press, 1981), 46. The book was later released by the same publisher but under a slightly different title—*Living in Troubled Lands: Beating the Terrorist Threat Overseas*, 1991.
- [22.](#) M. Harry, *The Muckraker's Manual: How to Do Your Own Investigative Reporting* (Mason, MI: Loompanics Unlimited, 1980), 73–78. Greg Hauser, *Pretext Manual* (Austin, TX: Thomas Investigative, 1994).
- [23.](#) See, for example, “cover for action” in Valerie Plame Wilson, *Fair Game: My Life as a Spy, My Betrayal by the White House* (New York: Simon & Schuster, 2007), 160.

Chapter 8

Defensive Counterintelligence: Information Security

Chapter 8 Defensive Counterintelligence: Information Security

This topic describes the essentials of information security by examining:

1. Information security defined;
2. Classifying information;
3. Types of data requiring classification;
4. Four basic classifications levels;
5. Code names;
6. Compartmentalization;
7. Handling sensitive information;
8. Accounting practices;
9. Advertisements;
10. Meetings and conferences;
11. Reverse engineering;
12. Trademarks, patents, and copyrights;
13. Clear desk policy;
14. Document storage;
15. When writing leaves an “impression”;
16. Authorized document reproduction;
17. Unauthorized document reproduction;
18. Document safeguards during use;
19. Document disposal;
20. Waste disposal; and
21. Carriage of classified information.

INFORMATION SECURITY DEFINED

The term *information security* refers to three pillars that underpin this security approach. These pillars are: *confidentiality*, *integrity*, and *availability*. The term is often used interchangeably in the literature with the related term *computer security*. However, this practice of interchangeable terms is not correct. This is because information security focuses on data in all its manifestations: books, journals, reports, photographs and other images, electronically stored data, and otherwise.^[1] Compare this to computer security that focuses on computer systems—mainframes, workstations, servers, notebooks, netbooks, and tablets—with regard for the data that is either stored on or processed by the computer.

The first pillar, confidentiality, is concerned with the prevention of unauthorized disclosure. The second pillar, integrity, is concerned with being able to detect if and when information is modified. And the third pillar, availability, is concerned with ensuring that the data is able to be accessed by those with a need to know when required (which, if you recall, is shared with the fifth tenet of defensive counterintelligence in chapter five). These three pillars are enshrined in legislation in the United States under the *Federal Information Security Management Act of 2002*^[2] and are reflected in protocols and standards throughout the security industry generally.

SUB ROSA

Like romance, intelligence has a long history of secrets, hence the shared symbolism in the rose.

“In secret; privately; confidentially. [Latin, ‘under the rose,’ from the practice of hanging a rose over a meeting as a symbol of secrecy, from the legend that Cupid once gave Harpocrates, the god of silence, a rose to make him keep secrets of Venus.]”*

* William Morris, ed., *The American Heritage Dictionary of the English Language* (Boston: American Heritage Publishing and Houghton Mifflin, 1971), 1,283.

CLASSIFYING INFORMATION

It could be argued that the first step in protecting information is to assess its impact if it were disclosed to a third party, whether this is the opposition or the general public. If the answer is that disclosure could cause harm, then it needs to be *classified*.

HERKOS ODONTON

The legendary writer of spy fiction Ian Fleming used the term *herkos odonton* in his novel *On Her Majesty's Secret Service* several times in dialogue between the book's hero, James Bond, and Marc-Ange Draco, a Corsican crime syndicate boss. Fleming used the term to mean that the conversation between the two men was to be *secret*—not to be discussed with others.*

The term is likely to have originated from the ancient Greek as there is a passage in Homer's *The Odyssey* where Zeus admonishes Athena for speaking too freely. He says, in effect: "My child, how could you let words slip through the barrier of your teeth." Although Fleming says *herkos odonton* means "the hedge of the teeth," the word *hedge* may be an English interpretation as there are few hedgerows in Greece. In classic Greek it may have been "fence" or "enclosure," or the like. To support this, Frederick Von Raumer, professor of history at the University of Berlin, used Homer's phrase in a letter to a friend, later published in "Letter X, April 9th, 1835."[†] He too used the word *hedge* in the phrase and in the same way as Homer—something like, "you should keep those thoughts to yourself."

However, Fleming's characters used *herkos odonton* as an idiom for "top secret." Though this has a slightly different emphasis, both meanings are likely to apply—for instance: "[h]erkos" would refer to a hedge, fence, or enclosure, and *odonton* would refer to teeth, as in *periodontist*. It is therefore the context in which it is used that provides meaning.[‡]

* Ian Fleming, *On Her Majesty's Secret Service* (London: Jonathan Cape, 1963).

[†] Frederick Von Raumer, “Letter X, April 9th, 1835,” in *England in 1835: Being a Series of Letters Written to Friends in Germany During a Residence in London and Excursions into the Provinces* (London: John Murray, 1836), 70.

[‡] I thank my colleagues of Greek scholarship for their assistance in interpreting the meaning of this phrase—Yiannis Polias, BSc, MA (AppLing), Yerasimos Patitsas, BArch, and Dr. Stamatiki Krita, PhD, personal communications, August 9 and 10, 2011.

Classification is both a process and the outcome of that process. For instance, a staffer can evaluate a piece of information to determine whether it needs protecting under a classification scheme, and the designation assigned the information at the end of the evaluation is the outcome—the information is now classified.

Under the first tenet of defensive counterintelligence (see chapter five), the agency head has responsibility for security in all its forms. So, although the agency head would not normally be involved in the activity of classifying information, it is his or her responsibility to ensure that this occurs. In most instances, this responsibility would be assigned to personnel within the agency. In the context of counterintelligence, information refers to data that is recorded in hardcopy documents or on files stored on electronic media (e.g., hard disk drives on a desktop or in portable computers, as well as agency servers). It also refers to knowledge—for instance, *conversations* or *understanding* derived from synthesizing information in a cognitive process.

The reasoning behind the classification of information is to be able to make these data available to personnel who have a need to know. Generally, it is in everyone’s interest not to hoard information, but to share it. As the saying goes, “information is power.” So, it makes sense to use the power of these data to support the agency and its clients in achieving their goals. This is an important issue and is integrally tied to the *need-to-share* principle, as well as the *responsibility-to-provide* principle.

Finally, under the first tenet of defensive counterintelligence, it is the agency’s chief officer who has responsibility for ensuring that all

staff are security trained. This training includes instruction in how the information classification system works as well as the theory that underpins these practices.

TYPES OF DATA REQUIRING PROTECTION

In order to foil possible attempts by the opposition to penetrate an agency, information about it and its activities should be assigned classifications of sensitivity. This is tenet thirteen (delineate and prioritize) of defensive counterintelligence. These classifications are then used to guide access and dissemination. Information in this context means data that requires protection from unauthorized disclosure. By way of example, below is a list of data items from the business sector that require some level of protection through a classification scheme. Equivalents of these and other data items would exist in the areas of national security, the military, and law enforcement.

- Production plans;
- Production methods;
- Production schedules;
- Product releases and schedule;
- Marketing strategies;
- Advertising campaign details;
- Customer/client lists;
- Trading terms and agreements;
- Details of alliances with other businesses;
- Proposed mergers;
- Policy directives;
- Rationalization plans;
- Sales projections;
- Material costs;
- Supply sources;
- Tenders;
- Research initiatives;
- Research and development funding;
- Technical discoveries;

- Personnel (their numbers, positions, salary packages, and expertise); and
- Employee recruitment, promotions, transfers, and dismissal details.

FIVE BASIC CLASSIFICATION LEVELS

Arguably, there are five levels of data classification. The lowest classification of information consists of information of a general and unrestricted nature. The type of information provided in company prospectuses is a good example of this. Such information would be suitable for all general inquiries and posting to a website.

In line with the lowest level of unclassified but not quite making the next classification level is a level that recognizes that there is some degree of sensitivity associated with the data. These pieces of information might be useful to the opposition or its client.

The next highest classification consists of information that should be available to customers only upon request. Information of this type is best described as information and/or material that, if disclosed to an adversary, could reasonably be expected to cause some degree of harm to the agency or its client.

Moving up the scale again is the second highest level of information classification. This information should be available to an agency's most important customers. Information with this designation would be information and/or material that, if disclosed inappropriately, could reasonably be expected to cause "serious harm" to the agency or its client.

Finally, the most sensitive information should be available only to staff with a need to know and government departments that have appropriate authority (i.e., a right to know). Information of this type, if disclosed to the opposition, would reasonably be expected to cause "exceptionally grave harm" to the agency or its client. (In a business setting, this classification might mean that the company's bottom line could suffer an impact of five percentage points or more.)

Sensitive but Unclassified is a security designation used by federal government agencies of the United States. It is used to denote information that does not warrant a classification that restricts access, but nonetheless requires consideration as to how that information is distributed and to whom.

Summary of Information Classification Descriptors

<i>Classification</i>	<i>Levels</i>
Top Secret	Information of this type, if disclosed to the opposition, would reasonably be expected to cause “exceptionally grave harm” to the agency or its client.
Secret	Information and/or material that, if disclosed inappropriately, could reasonably be expected to cause “serious harm” to the agency or its client
Restricted (or Protected or Confidential)	Information and/or material that, if disclosed to an adversary, could reasonably be expected to cause some degree of harm to the agency or its client.
Sensitive but Unclassified	Information that might be useful to the opposition or its client.
Unclassified	Information provided in company prospectuses is a good example. Such information would be suitable for all general inquiries and posting to a website.

The description typology for classified information may vary from country to country as well as between sectors—for instance, the government sector or military may use different descriptors than those used in business or the private sector. There may also be additional classification levels with varying descriptors. By way of example, the City of New York uses the following descriptors to identify its data: public, sensitive, private, and confidential,^[3] whereas in government and the military the descriptors of unclassified, sensitive but unclassified, restricted, confidential, secret, and top secret are likely to be used (refer to table 8.1).^[4]

The G8 countries comprise the world's eight largest economies—Canada, France, Germany, Italy, Japan, Russia, United Kingdom, and United States of America.

In the post-9/11 security environment, the new set of universal-sectoral descriptors comprising white, green, amber, and red have been coined. These are information classification descriptors that are based on the easy to understand and nontechnical traffic light concept, and hence are referred to simply as the *traffic light protocol*. The protocol was developed by the Group of Eight (G8) countries because these nations recognized the need to share information between the government and military sectors and the private and business sectors.^[5] It is reported that dozens of other countries have since adopted this protocol for the sharing of information. Unlike a national security classification that is based on the notion of damage or harm, the traffic light protocol centers around the concept of who may receive the information.

Traffic Light Protocol Descriptors

<i>Traffic Light</i>	<i>Protocol</i>
Red	Very limited distribution—for example, intended for a person or a group of people named as recipients
Amber	Information for limited distribution for people with a need to know
Green	Information for general distribution to people that have some connected involvement with the topic discussed in the information, but not for posting to the Internet or display on websites
White	For unrestricted distribution to anyone with an interest in the information

CODE NAMES

Classified research projects, as well as secret operations, use code names. The reason for this is because a code name offers a way of referring to the project or operation without referring to the actual details involved. This provides a level of secrecy. For instance, during the Second World War, the code name *Operation Torch* was a more convenient way to refer to the plans for the Anglo-American invasion of French North Africa.^[6] But the operation code name did not even hint at what it might be. Anyone who may have come in contact with the code name would have to solve the mystery surrounding the name.

Projects and operations are usually given single words to identify them. Compare this to training exercises that are given a code name of two words, or a short phrase (e.g., the biennial Australian-American military exercise that is held in Queensland is *Exercise Talisman Saber*). But this is not always the case; for example, *Operation Enduring Freedom* was the code name for the U.S.-led invasion of Afghanistan in 2001. Project code names follow the same rationale, for example Project Manhattan, the code name for the building of the first atomic bomb.

Code names are also used in business counterintelligence for the same reasons. Take for example the well-known code name used by Microsoft Corporation for its *Windows 7* operation system—*Vienna* (formerly *Blackcomb*). But some businesses may have a doctrine that prohibits the use of the code name outside the company and might go as far as to require employees and contractors to sign nondisclosure agreements.

TOP SECRET

Typical Label for Stamping Classified Documents and Files.

Courtesy of the author

COMPARTMENTALIZATION OF INFORMATION

Compartmentalization is a simple defense concept applied to partition information and those who access it. Compartmentalization works because data are first classified into security levels (e.g., restricted, secret, etc.) and, once this is done, the need-to-know doctrine is then applied. Using these two defensive security techniques allows the sharing of information that is necessary for staff to understand the issue under investigation and/or the taking of action relating to it without offering open and unrestricted access to all information.

The purpose too is simple; the fewer people who know about a secret, the more likely that it will stay a secret. The containment of sensitive information in this way complies with defensive counterintelligence tenet fifteen—if there is a breach of security, the pool of possible suspects needs to be small to help identify the perpetrator.

Declassification can be seen as important as classifying information. Declassification is the removal of the original security restrictions so that the data can be made more widely available. This process can be automatic under legal authority, say, after thirty years; or systematic as a regular practice within the agency; or mandatory under a specific application from an interested party to the information. Declassification can also take place via an application under a freedom of information law. Although, at first glance, declassification seems to be a practice that unnecessarily reveals secrets, it is essential to the maintenance of democratic principles and the rule of law. And, from a purely practical point, it promotes research and understanding by making more information on the workings of government available to historians, social scientists, and analysts of other academic backgrounds.

Usually code words are used to identify sensitive information that has been compartmentalized. For instance, a file containing top secret material may bear a code word that identifies it as belonging to a special project or operation. Note that a code word is different from a code name. An example of a code-word-classified project is the well-documented MKULTRA mind control project conducted by the CIA in the 1950s and 1960s. The code word was comprised of the letter-pair MK,

which signified the Technical Services Staff branch that ran the project, and the word ULTRA for the project. Until this material was declassified in the 1970s, it would have been only accessible by those with the appropriate security classification *and* a need to know denoted by the code word.

Personnel who have been cleared to have access to that code-word material are the only staff allowed access. This prevents personnel with a secret clearance to access this material and inadvertently discuss its contents with others within the agency, or in liaison with another agency's staff who may also have the same level clearance, but are not cleared with the code word.

HANDLING SENSITIVE INFORMATION

Staff authorized to access secret or top secret documentation should be required to sign a “chain-of-custody record” in order to assure control over its content. The chain-of-custody record also facilitates withdrawal and destruction when the documentation is no longer required (see appendix D). In order to inform staff members of a particular document’s degree of sensitivity, each document should be identified with a marking indicating its grade (bold letters in red ink).

When marking a document, staff should bear in mind that the entire document need not be classified at a particular sensitivity level. Take for instance a report compiled on a recent research project. It could be considered ideal for public release in a future counterterrorist awareness campaign in the media (lowest level), but a page (or even several paragraphs) may contain technical data about the research that is best kept reserved. That section can carry a classification stamp, while the remainder of the text displays the general distribution classification of, say, restricted.

If sensitive information has been compromised or just “lost,” the following guidelines will assist in minimizing the damage that may result:

- Attempt to regain custody of the documents/material;

- Assess the information that has been compromised (or subjected to compromise) to ascertain the potential damage, and institute action necessary to minimize the effects of such damage;
- Investigate to establish the weakness in the security arrangements that caused or permitted the compromise, and alter these arrangements in order to prevent any recurrence; and
- Take actions appropriate to either educate/counsel/discipline the person(s) responsible.

By using an information classification system, inappropriate disclosure is less likely to occur, and, as the information contained in various documents becomes dated and less sensitive with the passage of time, reclassifying the information's classification downward can then take place. The extent to which an agency goes to enact a classification system is determined by its size and the overarching authority imposed on it by its mandated creator (i.e., government and military agencies will have standards imposed by law or regulation, whereas private or corporate agencies will be guided by policy). In the case of a sole private practitioner or a small business firm, there will be far less need for formal arrangements when compared to large organizations.

ACCOUNTING PRACTICES

Although we have examined classification of information in the broad sense, it is worth discussing the accounting practices of the agency specifically. For, if accounting practices are not taken into consideration when classifying information, such loopholes can create serious weaknesses in a counterintelligence program. This issue is not a concern so much with government agencies that operate in the national security, foreign policy, or military arenas, as their accounting practices are regulated by law. In fact, complex arrangements are in place to shield the unauthorized disclosure of budgets and sensitive expenditures so that the opposition cannot obtain these data. For instance, some intelligence agencies operate front organizations, front groups, and front companies to act as shields. It is this consideration that is the point

being made here, but perhaps it is aimed at those who practice business and private counterintelligence rather than agencies of the government and military.

By definition, accounting is the practice of identifying, measuring, and communicating economic information about a business or private lives. Arguably, it is one of the most valuable sources of information for planning and control that a business has. Careful consideration should therefore be given to safeguarding financial data about sensitive matters. Such information should not be recorded openly in journals and the ledger along with supply items and petty cash purchases. Sensitive projects, whatever they may be, should have special accounting practices designed to minimize the risk of exposing their budgets, expenditures, and the like to staff that perform only routine accounting tasks.

ADVERTISEMENTS

Advertisements and editorial articles appearing in the print and online media are particular areas worthy of note. Such information can be very revealing about an agency. All information contained in advertisements for personnel, prestige, product or service development, technical advancements, or marketing should be analyzed as possible intelligence that might be used by the opposition.

Even the size of an advertisement and the frequency at which it appears are in themselves important factors when analyzing an agency's intentions and strategies. Likewise, the type of media a business uses and the positioning of an advertisement in the publication, website, or blog can also provide vital pieces of information. The same applies with editorial information. Customers of the agency are not the only readers of such media articles; the opposition will be privy to them also. In order to combat unwitting disclosure, a review procedure should be set up to screen information intended for publication or presentation at public meetings.^[7]

MEETINGS, CONFERENCES, AND ORAL CONVERSATIONS

If information that is classified as top secret is the subject of a meeting or conference, the date, time, and location of that meeting should only be promulgated to those people who will be attending and others on a need-to-know basis (for instance, the personal assistants or executive officers of those attending). Meeting organizers should be conscious of surveillance through windows and internal glass partitions and select venues accordingly. Agendas and conference notes should not be left behind, but destroyed in the manner discussed under the section on document disposal below in this chapter. If the meeting breaks for refreshments, arrangements should be made to secure the room or have it kept under observation.

Counterintelligence staff training needs to provide employees with an understanding that discussing classified matters over unsecured telephones, in e-mails, in public places, or on public conveyances (including taxis) is prohibited and this needs to be reflected in agency policy.

REVERSE ENGINEERING

Reverse engineering is a low-profile form of espionage that has the potential to yield high-impact results. Essentially, reverse engineering is the purchase of an agency's product (or service) and the subsequent disassembling of it into its component parts (or, in the case of a service, a careful analysis of the service's quantity, quality, presentation, follow-up, etc.) in order to determine how it was constructed and what manufacturing processes were utilized. Analysis of this type can provide the opposition with important data about the targeted agency.

Such details can be likened to providing the opposition with a guided tour of an agency's facilities or research and development division. There may not be anything an agency can do about this; however, every agency should be cognizant that it will occur as soon as their product or service enters the market.

Once an agency begins its marketing phase, it will need to practice reverse engineering itself in order to ensure that the opposition is not infringing patent rights (see Trademarks, Patents, and Copyright below). Although reverse engineering is an espionage technique, and agencies

need to practice defensive measures to protect their intellectual property, it is also an important *offensive* counterintelligence method, and this will be discussed in chapter twelve regarding detection operations.

TRADEMARKS, PATENTS, AND COPYRIGHTS

Trademarks, patents, and copyrights are all important elements in an agency's counterintelligence effort. A trademark is any symbol, word, or name or any combination of these that identifies a manufacturer's or merchant's goods or services and distinguishes them from those made or distributed by other businesses. Although there are common law rights granted to the user of a trademark, government registration provides *prima facie* evidence that an agency holds exclusive rights to its use, and permits legal action against others for its unauthorized use.

A trademark must be registered in each country in which an agency trades. If this is not done, a foreign competitor could not only capitalize on an agency's goodwill, but wreak havoc by downgrading its product's reputation through less stringent business practices or quality control.

In contrast, a patent is a special right conferred on the designer of a unique process or device, enabling the agency to exercise exclusive privilege in its manufacture, use, or sale for a limited period of time. A patent, like a trademark, must be applied for and is only enforceable in the country in which the registration is submitted. As with trademarks, if an agency trades overseas, applications for the registration of a patent must be lodged with the appropriate government agency in each country in which trade is carried on. Again, if an agency fails to do so, a foreign adversary may seize its idea through its own intelligence efforts. If this happens, not only will the agency have lost potential markets, it will have paid for all of the opposition's research and development expenses.

In contrast to these defensive measures, copyright is a legal right that protects a broad range of intellectual material, from computer programs to works of art. Literature of all descriptions, musical scores, films, photographs, and media broadcasts are also included under the copyright umbrella. Unlike trademarks and patents, copyrights do not

require an application to be made to a government instrumentality. Copyright protection is automatic, and copyright owners are protected in foreign countries under international convention. In order to afford full international protection to all intellectual property that an agency generates, a copyright notice should be placed in the front of these publications. The copyright notice consists of the word *copyright* followed by the symbol © and then the year of first publication followed by the name of the copyright owner—like thus: Copyright © 2012 by Hank Prunckun.

Arrow Information Paradox

The Arrow paradox is a conundrum that businesses face when dealing with intellectual property. The paradox is named after its creator, Kenneth Arrow, who devised it in 1971 in connection with his study into risk taking.^[8]

The paradox occurs when a company seeks to acquire information or knowledge (i.e., technology) from external suppliers or to promote its intellectual goods or services to customers or the marketplace. Specifically, the paradox is that the potential purchaser of the intellectual property needs to have the technology described or explained in some detail to be able to understand its utility and decide whether to acquire it (or, in the case where a company wants to buy, to sell it). However, once these revelations are made about the technology the intellectual property owner has in effect passed on their intellectual property to the other party without any compensation.

There is a lesson here for counterintelligence. That is, once an employee is given access to classified data in order to perform his or her job, the agency or its client has in effect transferred these secrets to that person and there is no way of retrieving them. It is only through the practices of counterintelligence that these secrets remain so until deemed appropriate to reveal.

CLEAR DESK POLICY

Sometimes termed end-of-day or end-of-shift security checks, a “clear desk” policy dictates that all employees and contractors need to store classified material in accordance with the appropriate classification level—unclassified, restricted/confidential, secret, or top secret or another classification system if used. A system of checking desks, workstations, and meeting rooms, as well as other aspects, needs to be designed to ensure that these data have been secured in the appropriate repositories, and, in turn, these have been secured.

DOCUMENT STORAGE

Under the tenet of defense in depth (tenet ten of defensive counterintelligence), an agency’s first line of defense against penetration by the opposition is its external barriers; that is, its fences, doors, and windows. Its second line of defense is the containers that hold its sensitive documents and data. For example, filing cabinets, hard disk drives, and a range of other devices are all containers in normal agency use.

It is therefore essential that an agency identify all documents and electronic records that may be the target of the opposition and secure these in containers that minimize the risk of their unauthorized acquisition. The concern is with both the theft of the documents themselves and the undetected theft of the information they contain. So, to further reduce the risk of attack on containers designated for sensitive information, an agency should not store valuables such as cash, securities, jewels, precious metals, and narcotics in them.

Data backup includes off-site storage of backup media. The same safeguards that apply to an agency’s workplace storage apply to these locations too.

WHEN WRITING LEAVES AN “IMPRESSION”

An often overlooked source of information leakage is the impressions left on writing pads. To guard against this a thin piece of aluminum,

plastic, or acrylic should be used under the top sheet of all memo pads and writing tablets to prevent the formation of impression marks.

With the ubiquitous availability of the laser printer, typewriter and printer ribbons, carbon paper, plates, stencils, and similar items should no longer be used. Needless to say, a readable copy can be obtained from any of these sources, and therefore they are as dangerous as the originals in the hands of the opposition.

Dictation recorded on tape or disks should be deleted immediately after being typed. There are many commercially available software packages that digitally shred such data and these should be used to remove the original data once transcribed. Bear in mind that deleting and running a digital shredder to clear or sanitize magnetic media sounds simple and straightforward, but the way modern operating system and software packages work may prevent this. That is, a data file that is accessed by a software program in the course of use may create temporary files of the data, backup copies, or hold data in various forms of memory and swap files on the host computer or on a network server, as well as other possibilities. The point is this, sanitizing software needs to be able to locate all associated files and data stored in memory or caches and clean these, or another software utility needs to do this prior to running the sanitizing software.

AUTHORIZED DOCUMENT REPRODUCTION

The reproductions of classified documents bearing any of the security classifications of restricted, confidential, secret, or top secret should all be marked with that classification on the original material. Only sufficient copies necessary to meet operational requirements should be made, and all reproductions should be destroyed as soon as they have served their purpose. With secret and top secret material, there may be agency policies that require that each copy be numbered and that receipt of the document is acknowledged by signature. Electronic copies are handled in the same manner, but there may be an automatic logging system that generates an e-receipt automatically. Signing and logging fulfils the twelfth tenet of defensive counterintelligence, as discussed in chapter five.

UNAUTHORIZED DOCUMENT REPRODUCTION

The surreptitious photocopying of sensitive documents or photographing them using a digital camera are the two most likely ways the opposition could obtain classified information without an agency's knowledge. Another method, although difficult to attempt, is to remove the documents from the agency's secure containers, copy them, and then return them to their repositories undetected.

To guard against the former case, a locking device should be installed on the office photocopier to strengthen this potentially weak security link. And to counteract both possibilities, the agency should ensure that the containers holding documents or data are fitted with locks and that these locks are used religiously.

Metal containers, such as filing cabinets with padlocks, offer a reasonably high level of security; however safes and cabinets with combination locks incorporated as part of their physical structure offer a much higher level of protection. These containers are usually constructed to withstand force and their level of resistance is stated by the manufacturer. Secure storage is equally applicable to computer hard disk drives and portable data drives that are used to backup data, as well as magnetic backup tapes.

When photocopying sensitive documents, do not leave the original behind in the automatic feeder or under the document cover.

DOCUMENT SAFEGUARDS DURING USE

When sensitive documents are not held in their secure containers as outlined above, the person using the documents should:

- keep the documents under constant visual watch;
- place the documents in a storage container, cover them, or turn them facedown when an unauthorized person is present;
- return the documents to their designated storage container after use;

- not allow classified material to leave the agency's offices unless it is carried in accordance with protective security while in transit at the same level as that when stored in an office environment; and
- in the case of maps, overlays, graphs, wall charts, or other forms of large documents, ensure they are labeled with a code name or code number and not openly bearing a designation that could identify the project to an unauthorized observer.

DOCUMENT DISPOSAL

An agency's wastepaper basket is an easily accessible source of information for the opposition. Probably two-thirds of the paper generated by an agency contains information that is sensitive to some degree; that is, information that, if acquired by the opposition, could adversely affect the functioning of the agency. This information gathering technique is known as *Dumpster diving*^[9] and is carried out simply by collecting the week's paper waste before the disposal truck arrives.

An easily overlooked source of information leakage is the office photocopier. Spoiled and overrun copies should not be indiscriminately dropped into the wastepaper basket. An important piece of equipment for all intelligence units is a document shredder. These devices are so common now that even retail stores carry them as standard items. An alternative for large units is to use a bulk document destruction service. These companies are usually listed in the yellow pages. But it is important to ensure that shredding is done with a cross-cut that reduces the document to the size of confetti or smaller. Low-security strip shredders may be cheaper to purchase but, as was found out in the aftermath of the 1979 seizure of the U.S. Embassy in Tehran, the opposition can reconstruct the documents. Many of the classified American documents that were destroyed using low-security devices were reassembled (though it took some years to complete the task).



Example of low-security strip shredded documents.

Courtesy of the author.

WASTE DISPOSAL

Obtaining information from discarded office material is a long-standing law enforcement and private investigator technique that is popularly referred to as *Dumpster diving*.^[10] Despite any aversion one may have to the thought of rummaging through someone's waste material, it is important to understand that this is a potentially rich and valuable source of information. Sensitive material of all types can be found in Dumpsters—manuals, notes, letters, memos, reports, files, photographs, passwords, identity cards, receipts, schedules, itineraries, telephone numbers, and much more (including computer hard disk drives, USB drives, and a variety of data that have been backed up onto CDs or DVDs). The reason why so much information can be collected from this source is that people believe that, once a piece of paper (or an old computer hard disk drive, etc.) is placed in a waste bin, it has “disappeared.” Some people believe that no one would bother getting dirty rummaging through a person’s garbage. They are wrong if they hold this belief.

Many computer printers have internal memory that cache data sent to them as a way of facilitating a smooth and uninterrupted printing queue. If this memory is accessible, for instance via theft, the opposition may be able to obtain the data relating to recent documents sent to the printer. In this regard, printers are like workstations and network servers as they store important information in obscure cyberlocations not readily understood by the casual user.

Recovery can take place at any point between where the waste leaves the agency's premises to, and including, the landfill site. Information obtained via waste recovery was at one time considered high-value and low-cost because it yielded more benefit than what it cost to gather it. However, with its popularization in the press and cinema, waste recovery has become more difficult. Government agencies, businesses, and individuals regularly use document shredders and are more conscious of how and what they dispose. Security surrounding waste has improved with commercial-scale confidential document destruction becoming a service that is widely available. The point to be made is that anything that has informational value needs to be destroyed, not just disposed of.

CARRIAGE OF CLASSIFIED DOCUMENTS

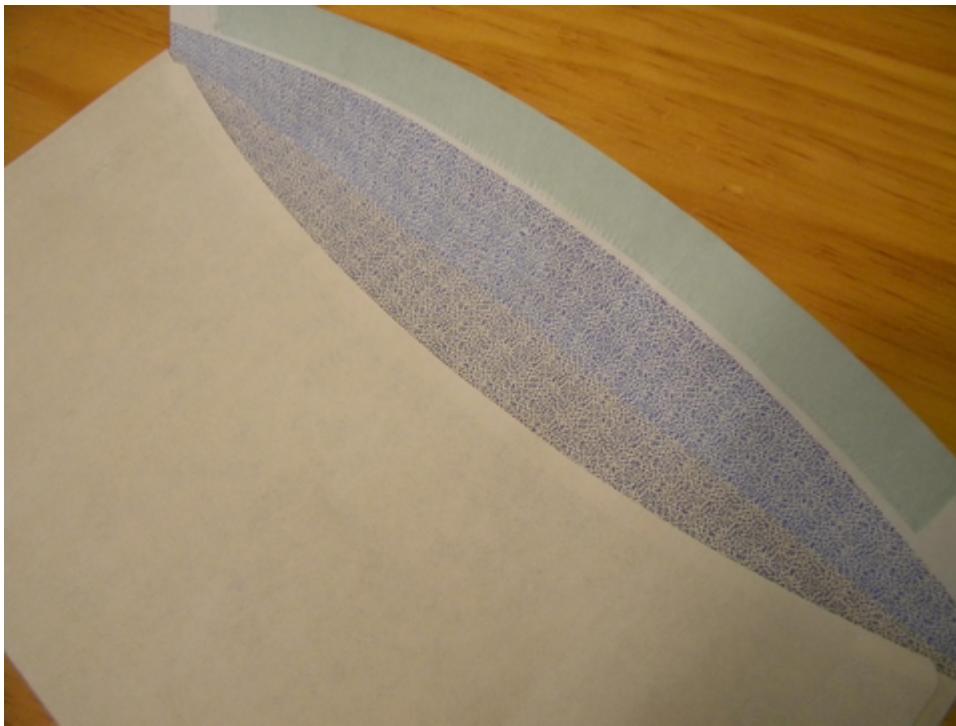
When documents are subject to government security classification, the rules concerning carriage of these documents outside the agency's offices are mandated by policy or other official instruction. It is not possible to outline these here as they are themselves restricted procedures. Nevertheless, the principles of sound document security can be applied to business and private counterintelligence. By studying these examples, the student of counterintelligence theory and practice can understand the gist of these procedures.

"The wax seal is a device put across the flap line of an envelope to prevent it from being opened surreptitiously by unauthorized persons. The bar of wax is heated until it becomes a gummy liquid and is applied in that form to suitable spots on the flap line. A metal stamp is then

pressed into the molten wax leaving an impression with a distinctive and usually complex pattern. . . . It is almost impossible to duplicate a seal exactly even if the original stamp is available.”*

* John M. Harrison, ed., *CIA Flaps and Seals Manual* (Boulder, CO: Paladin Press, 1975), 17.

When an agency needs to transmit documents of, say, a sensitive but unclassified nature through the public postal system, a service generically known as *registered mail* should be considered. This service is designed to be the most secure method of posting articles of value. Postal services maintain a record of the article’s whereabouts from lodgement to delivery, and, for a small additional charge, the agency can receive a receipt, signed by the addressee, confirming the document’s delivery.



Example of the printed pattern on the inside of an envelope. A pattern helps mask the envelope’s contents from unauthorized viewing.

Courtesy of the author.

To prevent unauthorized viewing of the document's contents while in transit, it should be folded or packed so the text will not be in direct contact with the envelope or shipping container. Only substantially constructed, opaque envelopes, boxes, and mailing tubes should be used for transmitting classified information. However, another method is to enclose the documents in a shielding envelope, which in turn is placed in the addressed covering envelope. Care should be taken not to call unnecessary attention to the package by labelling it with a description of its contents. The outer envelope should be marked: "Do Not Forward. If Undeliverable to the Addressee, Return to Sender." If the inner shielding envelope method is used, it should be annotated with: "To Be Opened by the Addressee Only."

COMMON LAW PROTECTION

Common law affords protection for confidential information and as such does not require parties to sign an agreement. Legal scholars advise that, in order for someone to exercise their common law right, it is only necessary for the communication between the parties to be confidential—that is, in trust that the other will not divulge the details. Often times this is done by the person or business that is asserting confidentiality by simply annotating the e-mail or document with words such as "*in confidence*," "*personal in confidence*," or "*commercial in confidence*," and so on.

Lawyers advise that four requirements need to be satisfied if confidential information is to be protected under common law. First, the information cannot already be in the public domain or be public knowledge (if so, the proverbial genie is already out of the bottle); second, the information must be clearly identified (hence, adding the words "*in confidence*" to the subject line of an email or at the bottom of a document); third, it needs to be clear that the situation in which the information is communicated is an event where trust was assured; and, last, the receiving party cannot indicate a willingness to disclose the information prior to the disclosure being made (again, this would demonstrate a lack of trust).

LEGISLATIVE PROTECTION

There are numerous pieces of legislation that are designed to protect information. In general terms, these include statutes and government policies. The terms and conditions upon which the information is confidentially held, and the circumstances of disclosure, are specified under each piece of legislation or the individual policy. These authorities also specify the jurisdiction, the enforcing body, and the penalty for breach. The Freedom of Information Act is an example of such legislation.

Freedom of Information Laws

These laws are designed to allow citizens to obtain information from government agencies through a straightforward application process. Although the title of these laws—*freedom of information*—implies unfettered access, these laws specify information that cannot be obtained by public application. These exemptions are one way governments protect confidential information. Examples of protected information include law enforcement investigation files, documents that are subject to legal privilege, documents that disclose people's personal affairs, files that contain trade secrets or information that is deemed commercial in confidence, information that if disclosed may cause harm to the economy of the state, and information that was provided under common law principles of confidentiality (see above). They may vary from jurisdiction to jurisdiction, but these categories provide a general picture of the scope of the exemptions.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Classified information;
- Code names;

- Dumpster diving;
- *Herkos odonton*;
- Secret;
- Sub rosa;
- Top secret;
- Traffic light protocol;
- Unclassified but sensitive; and
- Unclassified.

STUDY QUESTIONS

1. Explain how the common law provides protection for information and provide an example.
2. List six data items that might need protection and explain why each data item would require safeguarding and describe what type of defense you would recommend.
3. Explain the reasons for compartmentalizing information and describe how such a system might be devised for your present or past employer.
4. List five levels of security clearance and describe a situation where each level may be used with regard to your current or past employer.

LEARNING ACTIVITY

Inquire as to the format and style of policies used in your current place of employment. Using an existing policy as a template, write a “clear desk” policy. Even if your current employer does not use a system of classification for information, include the categories unclassified, unclassified but sensitive, and commercial in confidence (the latter meaning all business-related documents that should not be public). If your employer uses an information classification system, then use it.

NOTES

1. For example, see the treatment of information in its widest context relating to the business sector by Henry W. Prunckun, *Information Security: A Practical Handbook on Business*

- Counterintelligence* (Springfield, IL: Charles C. Thomas Publisher, 1989).
2. *Federal Information Security Management Act of 2002*, Chapter 35, U.S Code 44.
 3. The City of New York, *Data Classification Policy* (New York: The City of New York, June 16, 2011).
 4. See, for instance, Australian Government, *Protective Security Policy Framework* (Canberra: Australian Government, January 2011), 22.
 5. Organisation for Economic Co-Operation and Development, Directorate for Science, Technology, Computer and Communication Policy, *Development of Policies for Protection of Critical Information Infrastructure, Ministerial Background Report* (Paris: OECD, June 17–18, 2008).
 6. David Khan, *The Code-Breakers: The Story of Secret Writing* (Toronto: Macmillan, 1967), 501.
 7. An example of publishing sensitive information was that of Australia's Department of Foreign Affairs. It was reported that confidential documents outlining details of Australia's embassy in Baghdad, Iraq, had been posted on the Internet as part of a tender process for facilities management. See "Secret Plans on Website," *Adelaide Advertiser*, Adelaide, Australia, September 18, 2010, 41.
 8. Kenneth Joseph Arrow, *Essays in the Theory of Risk-Taking* (Amsterdam: North-Holland Publishing Co., 1971), 152.
 9. John Hoffman, *The Art and Science of Dumpster Diving* (Boulder, CO: Paladin Press, 1993).
 10. John Hoffman, *Dumpster Diving: The Advanced Course: How to Turn Other People's Trash into Money, Publicity, and Power* (Boulder, CO: Paladin Press, 2002).

Chapter 9

Defensive Counterintelligence: Communications Security

Chapter 9 9 Defensive Counterintelligence: Communications Security

This topic describes the essentials of defensive counterintelligence by examining:

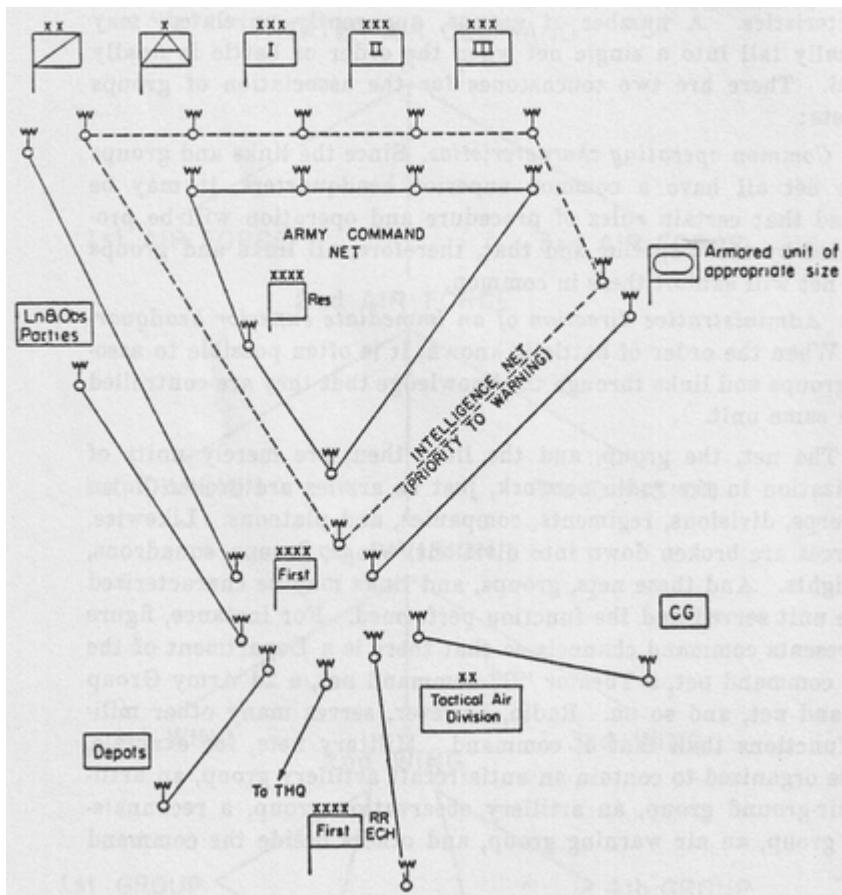
1. COMSEC fundamentals;
2. Technical security countermeasures;
3. Telephone wiring;
4. Cordless and cell telephones;
5. Facsimile machines;
6. Two-way radio systems; and
7. Encrypted communications systems.

COMSEC FUNDAMENTALS

Like many terms and phrases used in the intelligence world, the phrase *communications security* has been abbreviated for ease of use by blending the first parts of each of the words into the abbreviation *COMSEC*.^[1] COMSEC entails a number of provinces ranging from the physical security afforded to communication equipment and installations, the security surrounding the transmission of signals, and the emissions given off from cables and equipment, as well as the security of the messages that are transmitted—cryptosecurity. It also encompasses the frequency, volume, and structure of “stations” communicating with each other—traffic-flow security.

The reason for providing security for these facilities is because the opposition may exploit any of these realms for gathering intelligence—SIGINT, the abbreviation for *signals intelligence*.^[2] For instance, the simple monitor of the flow of radio transmission between stations is known as *traffic analysis* and has a long history of producing high-quality

and accurate assessments of, for instance, an enemy's order of battle.^[3] In an attempt to illustrate the COMSEC fundamentals, this chapter describes some of the key areas of concern and some of the basic security precautions. Because installations are highly technical, especially in the military, and communications equipment advances at rapid rates, it is not possible to canvass all. Nevertheless, the principles are presented here and are complemented with examples, as a way of providing a base of knowledge and understanding.



Notional example of an enemy army radio net that was constructed from intercepted radio traffic using *traffic analysis*. (Note that there is an endnote regarding the source associated—Department of the Army, *Fundamentals of Traffic Analysis [Radio Telegraphy]*, 12.)

Source: Department of the Army, *Fundamentals of Traffic Analysis (Radio Telegraphy)*, 12.

TECHNICAL SURVEILLANCE COUNTERMEASURES

Although it is impossible to determine the extent to which electronic eavesdropping exists in society, media reports indicate that it is widespread and not limited to any one government, industry, or commercial sector. If an agency suspects it is the target of either an illegal wiretap or bug, an audio countermeasure sweep is the best way of determining if there are any listening devices in operation. The sweep, however, will reveal devices operating at that given time only. Having said that, it must be stressed that no room can be guaranteed to be proofed against all forms of audio surveillance. Experience has demonstrated this to be the case; even the most sensitive rooms in the United States embassy in Moscow were once penetrated. In 1945, Soviet schoolchildren gave a replica of the Great Seal of the United States to the then-ambassador, Averell Harriman, as a gesture of goodwill. In 1952, a technical surveillance countermeasures sweep revealed that the Great Seal contained a listening device. Accordingly, agency security staff should be aware of the need to examine all gifts for this type of Trojan horse.

Conducting sweeps at irregular intervals is, therefore, the most effective way of reducing the risk of this hazard. It is arguably the most reliable way known to check for, and clear, audio surveillance devices.

There are limitations, however, in conducting sweeps. Firstly, with regard to telephones, even if the target agency's telephone devices appear to be clear at the time of the sweep, there is no way of determining whether the telephone of another party is under surveillance by inspecting the agency's end of the line. At the time of writing and to the knowledge of the author, there is also no technology available that can check for listening devices at, or beyond, the central telephone exchange. Second, there are some state-of-the-art devices and techniques used by opposition intelligence agencies, and possibly very well-financed private intelligence contractors and criminal groups, that may be undetectable because of their high level of sophistication. (For a list of some basic examples of analog audio surveillance devices and a brief description of their applications, see appendix C.)

An audio countermeasure sweep can be conducted by specialist counterintelligence firms operated by, say, private investigators and technicians of the government or military. The former are usually

contracted by private persons or businesses concerned about eavesdropping, whereas the latter are used to check and clear buildings and meeting rooms for political and government users. Nongovernment services are usually listed in the yellow pages or on websites. A professional sweep should include both a thorough physical search, inspecting literally every inch of, and every object in, the suspected area, as well as the electronic sweep. The electronic sweep may utilize a broad-band receiver and/or a specially designed field-strength meter to test for transmitters. Metal detectors can be used to hunt for bugs in nonmetallic objects and deeply planted devices in walls, floors, ceilings, and furniture. There are also a wide range of meters used to test the telephone line voltage for the presence of wiretaps.

TELEPHONE WIRING

Wiretapping is the interception of telephone and facsimile communication, as well as computer data that is transmitted over landlines. The interception of these signals can take place anywhere between the sender's offices and those of the receiver. The most vulnerable parts of the telephone system are at the agency's telephones and other data-transmitting equipment such as data routers, switches and modems, and the lines leading out of the building.

Once the targeted lines leave the agency's building, interception is more difficult, but certainly not impossible. Apart from a countermeasure sweep, the chief countermeasure against wiretapping is to ensure that the telephone wiring closet, terminal box, or data center is equipped with locks so that it can be secured at all times. In addition, all exposed wiring, or wiring that is easily accessible, should be shielded in metal conduit that is connected to electrical ground or earth. Providing a path to ground for the electric emissions radiated from communications cables and devices is the principal means for preventing the interception of electromagnetic emissions. This is because ground has the theoretical ability to absorb electric currents without changing its electrical potential or charge. The electromagnetic emissions from wiring and cabling are therefore contained by the metal conduit (which, in turn, is electrically grounded). The electrical currents produced by the

emissions then flow along the conduit (as it is a conductor of electricity) to ground.

CORDLESS AND CELLULAR TELEPHONES

Although cordless telephones offer many advantages over their wire-bound cousins, their use poses serious security risks. This is because most units operate within the standard radio frequency range of 30MHz to 300MHz (VHF band), 300Mhz to 3GHz (UHF band), and 3GHz to 6GHz (the lower end of the SHF band), making it possible for the opposition to intercept the conversation. Furthermore, a cordless telephone may respond to other cordless telephone equipment operating nearby or to radio equipment, including commercial transceivers.

It is an unwise decision to use cordless telephone technology for discussing confidential information of any description, and it is certainly not recommended for any environment that warrants security and secrecy. Hard-wired telephonic devices are better suited for maintaining a level of secrecy.

Cellular telephones are ubiquitous.^[4] Arguably, the business world and people's personal lives could not function properly without these devices. But, like cordless telephony, they are susceptible to interception because they transmit a radio signal from the handset to a cell tower that connects the signal into what is known as a *trunked network*. The trunked network is the landline telephone network that is connected by computers. Through sophisticated computer software, this network routes the signals from caller to receiver far beyond the normal transmission/reception distance of the cell handset (in fact, as long as the receiver has access to a landline telephone or is in range of a cell tower, there can be communication, regardless of where the two are on the globe). But it is the transmitting of the signal from the handset to the cell tower that is the weakest link and it is there that interception is likely to occur.

Granted, the risk of interception is low because it is a more difficult technical task, but it is far from impossible. In fact commercially manufactured radio receivers (e.g., radio scanners) have the cellular telephone portion of the radio spectrum blocked in some countries to

help prevent this from happening. However, these unblocked scanners are available at retail outlets in many countries around the world, and radio engineers can overcome the limitations of these commercially blocked radios on their electronic workbenches in a few hours.

If confidential information is being discussed on a cell phone, agency staff should consider using a device that encrypts the conversation. One such device is the Sectéra® cell phone that is marketed by General Dynamics. The manufacturer advises that the device is certified by the National Security Agency (NSA) for communicating information to a level of top secret and, of course, all classifications below. The device can be used in its secure mode as well as an unsecured mode, and can be used domestically or while travelling abroad.



General Dynamics' encrypted Sectéra® cellular telephone.

Courtesy of General Dynamics.

FACSIMILE MACHINES

At one time facsimile machines were essential for transmitting documents for business and government agencies alike. Until e-mail and

the ability to attach documents electronically, they were very effective in providing high-speed data transmission at very low cost. Their value was and, in some cases still forms, an integral part of many communication systems.

However, they pose potential risks. Aside from the risk of the data being intercepted, the way voice communications could be intercepted, the potential exists for documents to be inadvertently sent to an incorrect destination. Such breaches could occur by misdialing the desired number or entering a totally incorrect number. Therefore, prior to transmission, it should be confirmed that the number is in fact the correct one for the destination. Following this, the destination number should be entered into the facsimile machine with caution, and then visually checked to make sure that the correct digits have been registered before executing the transmission command.

TWO-WAY RADIO SYSTEMS

As with cordless telephone systems, two-way radio networks are highly susceptible to interception, even those employing some form of *voice inversion scrambler*. This is because software and electric kits are available commercially to descramble these signals. These scramblers use simple analog mechanisms to electronically obscure the radio operators' voices. Basically, the method inverts the high tones of the audio with those of the low tones, thus making the scrambled audio sound like what someone might perceive as Donald Duck with marbles in his mouth speaking gibberish.

However, if electronic kits are available on the open market and anyone with an interest in monitoring radio transmissions can buy these, then it follows that a radio engineer in the employ of the opposition could construct equipment far more advanced than these commercial descrambling units. Even the more advanced form of scrambling known as *rolling code voice inversion* may be descrambled if the opposition is a foreign power with the technical resources to allocate to the task (these circuits are available commercially and can be modified by radio engineers). Digital radio signals that are encrypted offer the highest commercial means for privacy, but, again, digital radio

scanners are on the open market and decryption, though difficult, is not impossible.

Therefore, if sensitive information is to be conveyed via two-way radio, a secure radio system designed specifically to counter attempts at interception must be used. Such systems are certified to carry radio traffic up to and including the top secret classification level. These systems are mainly used by the military and diplomatic missions of virtually all nations, but, for any business that relies on two-way communication, such a secure system is also a must. Manufacturers are usually listed in the yellow pages and on their corporate websites.

It is axiomatic that the more a piece of information is worth, the more it is worth obtaining, and the more the opposition is likely to pay to get it.

One limitation of using a secure radio communication system is that, if it requires encryption and the encryption device or software is classified, it makes interoperability with, say, public safety agencies impossible. This is because the device or software cannot be made available to these agencies if communications in a crises are crippled. If, however, the radios are able to be switched between an unencrypted mode and full encryption, it would alleviate this problem. But transmitting an unencrypted signal then presents issues regarding interception.^[5]

ENCRYPTED COMMUNICATIONS SYSTEMS

Agencies that need to send sensitive information of a level that warrants a “secret” classification or above over a telephone network (including SMS—short message service), a radio system, or via interactive whiteboards or facsimile will need to incorporate encryption in order to ensure the confidentiality of the information. In military and government agencies, dedicated lines and dedicated communication systems, such as secure VoIP (Voice over Internet Protocol), are permanently in place for this purpose. Agencies in the private or business sectors may not have the resources for such setups but

nevertheless should still consider encryption units that can be used on an ad hoc basis. In effect, they can be switched on and off as needed.

Permanent encrypted communications systems are often located within a strong room or vault and, as such, offer an extremely high degree of security. The security is at a level that meets the requirements of "secret" or above. If the opposition is attempting to intercept a conversation that is using a cipher unit, it would be digital noise.

Encryption units that are less permanent are still able to achieve this remarkably high degree of security by being able to randomly select from encryption codes that can be greater than 10 to the 30th power. If, for example, the opposition was successful in intercepting and recording an encrypted conference call among, say, a group of counterterrorism policy analysts, it would need the services of a mainframe computer and perhaps months, or even years, of around-the-clock computing time in order to decipher the data. Facilities to do this are realistically only available to intelligence agencies of wealthy nations, and it would be a course of action not embarked upon unless the benefits outweighed the costs.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- COMSEC;
- Signals intelligence;
- Traffic analysis;
- Trunked (radio) network; and
- Voice inversion scrambling.

STUDY QUESTIONS

1. List the different provinces, or subject areas, that COMSEC entails.

2. List two limitations of technical surveillance countermeasure sweeps and explain why these limit the effectiveness of debugging operations.
3. Explain why enclosing communications wiring and cabling in grounded metal conduits is an effective countermeasure against eavesdropping.
4. Explain one way the opposition might intercept cell phone communications.

LEARNING ACTIVITY

Imagine that your agency has need for a system of point-to-point two-way communication for several of its field officers. Envisage that the operating distance between the operatives is two miles, or about three-and-a-quarter kilometers. (1) Research what type of handheld radios the agency might select and list these in a column of a table (hint: look for radios that are manufactured for public safety agencies or the military); (2) in an adjacent column, note whether the radios in column one are manufactured with either scramblers or encryption, or have neither; (3) in a third column, note whether the radios could be used for unclassified information (i.e., information that, if intercepted, would have no adverse impact on the work of the operatives or the agency) or could afford some level of privacy (refer to the list of classification of information in chapter eight to refresh your memory). Based on this information, what is your recommendation for a radio that can provide secure communications at “secret” level?

NOTES

1. For example, see Bill Wedertz, *Dictionary of Naval Abbreviations*, 3rd ed. (Annapolis, MD: Naval Institute Press, 1984).
2. U.S. Department of the Navy, *Signals Intelligence*, MCWP 2-15.2 (Washington, DC: U.S. Marine Corps, 1999).
3. U.S. Department of the Army, *Fundamentals of Traffic Analysis (Radio-Telegraph)* (Washington, DC: Department of the Army, 1948), reprinted by Aegean Park Press, Laguna Hills, California, n.d., with an additional glossary and index added.

4. The term *cell phone* may not be used universally in Europe and other parts of the world, where the terms *mobile phone* (e.g., in Australia and the United Kingdom) and *handy phone* (e.g., in German-speaking countries) are used.

5. By way of example, the operatives who conducted the black bag operation in relation to the June 1972 Watergate break-in used four off-the-shelf Radio Shack TRC100B, five-watt, six-channel, citizens' band (CB) radios that operated on 27MHz. This meant that anyone who had a radio receiver or radio scanner tunable to the 27MHz band could eavesdrop on their conversations. As 27MHz is in the high frequency band (HF), the signal could have travelled well beyond the line of sight and might have been received several hundred kilometers away due to "skip," or the bouncing off ionized particles in the ionosphere. In fact, the operatives discovered that the frequency they were operating on was shared with a local taxi company. They rationalized not using another frequency, or doing what should have been done in accordance with sound counterintelligence practices—use of an encrypted radio system. Instead, they decided that the taxi traffic would provide cover for their transmissions. This tactical decision was consistent with other ill-fated decisions the group made that night, and these decisions demonstrated their lack of understanding of the finer points of counterintelligence. See G. Gordon Liddy, *Will: The Autobiography of G. Gordon Liddy* (London: Severn House, 1981), 165.

Chapter 10

Tenets of Offensive Counterintelligence

Chapter 10 Tenets of Offensive Counterintelligence

This topic describes the essentials of offensive counterintelligence by examining:

1. Preliminary thoughts; and
2. Tenets of offensive counterintelligence.

PRELIMINARY THOUGHTS

Offensive counterintelligence is concerned with *deception* and *neutralization*. Translating these concepts into actions within an agency should be considered as strategy and tactics, and this chapter provides a discussion of ten tenets.

Carl von Clausewitz once wrote: “The main feature of an offensive battle is the outflanking or by-passing of the defender—that is, taking the initiative.”* His words regarding fighting forces are analogous to offensive counterintelligence operations.

* Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Oxford: Oxford University Press, 1976), 200.

Like defensive counterintelligence, offensive counterintelligence comprises a number of tenets and these tenets mirror to some degree those of defensive counterintelligence. This is because, in defensive play, counterintelligence practitioners are thwarting the offensive moves of the opposition. Therefore, if we turn the focus around, we can then see how an agency should operate in this mode.

TENETS OF OFFENSIVE COUNTERINTELLIGENCE

Tenet 1—Executive responsibility. It should, therefore, not be surprising that the highest order tenet is the same as that of defensive counterintelligence—the responsibility for mounting an offensive campaign against any and all oppositions rests with the head of the agency. This is because it is a governance issue and good governance lies with the agency head.^[1]

The agency head may never be involved in any of the day-to-day tactical considerations of overseeing an operation, but he or she will be responsible for the program of aggressive secret operations. Functional responsibility therefore needs to be delegated to subordinates (or a committee), and, depending on the size of the agency, there may be several such delegations flowing down the chain of command. Nevertheless, the legal and ethical burdens of orchestration rest with that person. This is despite the fact that individual acts may be conducted by subordinates or agents employed by the agency.

As such, this tenet requires the agency head to put in place policies that convey the importance of following the rule of law and a standard of ethical conduct that projects an atmosphere of principled behavior—and to show through his or her actions that the agency should follow them. Although lower-level managers may ultimately be responsible for poor decisions made, the agency head must be in a position to stand on the moral high ground and call for them to account, rather than the other way around.

There is a theory of assumed vulnerability—that is, every target has at least one vulnerability that can be exploited.

Tenet 2—Executive justifiability. To conduct an offensive counterintelligence campaign, the agency head must be able to explain why such a program forms part of the agency's overall counterintelligence posture so that these actions are accepted in the most favorable light. The image of a campaign of unlawful behavior must be avoided, and this is associated with the first tenet. Attitudes must be cultivated to respect offensive counterintelligence's role in providing an active form of security and, as a consequence, legitimize

the program through formal policies and practices that provide transparency for this decision (note, not transparency for the actual operations—they, of course, need by their nature to be managed and conducted in secret).

Tenet 3—Ethical symmetry. People's acceptance of situations is to a large degree based on prevailing social norms that are balanced in proportion. So, if the first two tenets are established within the agency as a norm, ethical behavior will follow and, hence, so will acceptance. A management model that replicates procedural compliance despite staff misgivings, along the lines of, say, “like it or leave,” is most unlikely to be successful. Acceptance is an important factor for agencies, as, without the support of its staff, any program, let alone one as delicate as an offensive counterintelligence program, will not be successful, or could fail.^[2]

Tenet 4—Friendly access. In defensive counterintelligence the doctrine of *need to know* governs the accesses people have to areas where sensitive information is being processed, analyzed, or stored. In offensive counterintelligence operations, agency officers or agents need to be able to either recruit someone who has a need to know or be able to gain *friendly access*; meaning gaining access by deception rather than force.

Tenet 5—Deceptive operations. Despite all defensive countermeasures put in place to guard sensitive information, the opposition will make the assumption that there will be information that the agency has and/or operations it is conducting that may never be known. Therefore, the opposition will try to discover this information and locate its source. This tenet therefore deals with deceptive operations—that is, operations that are designed to throw the opposition off track so that the discovery of sensitive data is delayed and consumes a disproportionate amount of the opposition’s energy and resources.

Tenet 6—Counterreconnaissance and decoys. The opposition will no doubt be practicing reconnaissance to gather data about the agency’s programs and operations, as well as data that exists under the wider protective umbrella of its mandate (e.g., with regard to national security

and military intelligence). Therefore, this tenet addresses an agency's need to practice counterreconnaissance in order to be better able to place decoys to redirect the opposition to other areas that will yield nothing (though the opposition will be led to believe these data are meaningful). A simple example is to set up a sting-like operation to see if the agency can attract the opposition and, once attracted, feed it with misleading and deceptive data. Another is for the agency to simply actively scan the environment for signs of probing—for instance, on the Internet there are facilities that allow individuals to monitor the World Wide Web of new content. Though these commercial facilities have their own security shortcomings, an agency could establish a secure version for its own monitoring to “watch the watchers”—in this case, the opposition.

Tenet 7—Red team testing of defenses. Agency personnel should be probing its own countermeasures through *red team*^[3] exercises to determine if there are any systems or procedures in place that are so inflexible that they allow exploitation by the opposition. Rigid defensive tactics are predictable and, given time, the opposition is likely to find a way around them. For instance, agency staff may be tempted to bypass security procedures if they are seen as overly complicated or time-consuming. Red team exercises should result in recommendations for fluid, random, changing, and unpredictable tactics to present a more difficult situation to penetrate. Surprise is one of the underlying assumptions of the overall theory of counterintelligence and this element underscores this tenet.



Tenet 7—Probing defenses and a missed opportunity. Here an impressively uniformed, but inattentive, security guard protects a landmark building in Hyderabad from criminals and insurgents. As part of a “red team” counterintelligence exercise, the author was able to gather data unchallenged regarding the building and its occupants, including the taking of this target acquisition photograph. This was a missed opportunity for the target’s intelligence program as it failed to notice an offensive counterintelligence operation being conducted.

Courtesy of the author.

“When you’re catching spies, you have a bad counterintelligence service. When you’re not catching spies, you have a bad intelligence service. You can’t have it both ways.”*

* Judge William H. Webster, former director of Central Intelligence, 1987 to 1991, as cited in Frederick L. Wettering, “Counterintelligence: The Broken Triad,” *International Journal of Intelligence and Counterintelligence* 13: 294.

Tenet 8—Synergy with defensive counterintelligence. As offensive counterintelligence is active, especially those aspects that deal with neutralization (e.g., counterespionage operations), each operation needs to dovetail with components of the defensive program that might

otherwise interfere with the success of these operations. For instance, if a double agent under the control of the agency is meant to have access to classified data of a particular type, then the defensive arrangements need to be structured in order to allow these data to be accessed and handed over to the opposition (perhaps as part of a more elaborate plan of flushing out a mole or to sow disinformation, etc.).

Tenet 9—Synergy with positive intelligence. An opposition may move aggressively toward acquiring agency information or information under the agency's protection umbrella. The agency's defensive security program will frustrate these moves. But the fact that the opposition is moving to probe or penetrate the security defenses is, in fact, valuable data for both intelligence analysts (i.e., researchers) and counterintelligence analysts (i.e., spy catchers). An opposition's desire to seek certain data types is an important factor in developing and/or enhancing security. It is also important information for strategic intelligence analysts (i.e., positive intelligence) who are examining issues relating to the opposition or its interests. In this regard, this tenet requires that counterintelligence work closely with the intelligence side of the agency (e.g., positive collection).

"You can often predict what is going to happen, but it is devilishly hard to forecast when."*

* Alexander Downer, Australia's former minister for foreign affairs from 1996 to 2007, writing in an op-ed editorial in *The Advertiser*, Adelaide, Australia (August 8, 2011).

Tenet 10— Synergy with all-source and all-discipline collection. Data collection needs to incorporate strategies that seek information from domestic and overseas sources. This approach will lay a wide foundation for analysis as the world is arguably borderless; in practical terms, the universal convenience of air travel and information and communications technology have dissolved almost all international borders. This means the opposition can operate in multiple regions of the world simultaneously. Moreover, data sources need to include technical

collection methods^[4] as well as human sources.^[5] No source of information should be discounted.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Backup security support;
- Complicity;
- Early detection;
- Neutralization;
- Quality defensive system;
- Red team; and
- Time-delay system.

STUDY QUESTIONS

1. List the ten tenets of offensive counterintelligence and provide a brief explanation of each.
2. Tenet five deals with deceptive counterintelligence operations. Describe a deceptive ploy that a counterintelligence officer could use in one of these intelligence settings: military intelligence, law enforcement intelligence, or business intelligence. Describe the situation and the information that needs to be protected. Then describe the ploy that you have designed to throw the opposition off track. Explain how this strategy is designed to delay the discovery of the sensitive data, and/or consumes the opposition's energy and resources.
3. Describe in summary form the purpose of tenet six, counterreconnaissance. Give an example of how this tenet could be applied in practice to one of the following contexts: national security intelligence or business intelligence.
4. Tenet eight discusses offensive counterintelligence in relation to neutralization. Envisage a national security situation where a

counterespionage operation is underway—for the purposes of this question, let's use the 1994 Aldrich Ames case. Explain why the counterespionage operation would benefit by dovetailing with components of the agency's defensive counterintelligence program.

LEARNING ACTIVITY

Consider the offensive tenet of red teaming—tenet seven. Using an everyday situation, practice red teaming. For instance, select a building in the vicinity of your current workplace or where you live that you know no details of other than it is in the neighborhood. With this building identified, assume that your agency has been tasked to prepare a penetration plan for a business that resides in this building. Assume that the business is your notional opposition force (perhaps it might be fictionalized as a front for foreign intelligence operations).

In order to write your plan you will have to conduct reconnaissance and/or surveillance to gather data. You would normally do this by reconnoitering the building and making observations and taking photographs. But, in a security conscious world, a person conducting surveillance of buildings or people may be reported to the police (or may even be assaulted by people who feel threatened by such behavior). If this is a possibility, then an alternative is to conduct a simulated physical reconnaissance by conducting a (somewhat limited) surveillance via open-source data and images via the Internet and by using information held in public libraries.

WARNING! If you decide to conduct this learning activity, you do so at your own risk. And, if you decide to accept that responsibility by carrying out the exercise, it is important that you do not breach any law or local ordinance, or place yourself or anyone else in danger while doing so. Remember, if you cause any harm to others in carrying out this learning activity, you have not only failed the assessment by being indiscreet, but, also, you risk being arrested, fined, or reported. Ensure you operate within the law at all times and that you act safely and have regard for the privacy of others.

What did you find out about the building's physical attributes that might assist analysts? What did you discover about the business and what it does? Were there any conclusions (firm, tentative, or otherwise) that you could draw from your observations of the people entering or exiting the building? Now that these data have been collated, would you say that any form of counterintelligence was practiced? Are there vectors that could be exploited for penetrating the notional opposition target? If so, which ones and how would offensive measures be deployed?

NOTES

1. Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* (Washington, DC: Brassey's), 185–87.
2. The memoirs of former CIA case officers (i.e., operations officers) Robert Baer and Melissa Boyle Mahle illustrate this point. Their stories of how management mishandled various situations underscores the importance of this tenet. Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism* (New York: Crown Publishers, 2002), and Melissa Boyle Mahle, *Denial and Deception: An Insider's View of the CIA from Iran-Contra to 9/11* (New York: Nation Books, 2004).
3. The concept of a red team has existed throughout history in various forms. Exercises using red teams are used worldwide by governments and the private sector alike. Red teaming sees the problem through the eyes, and mind-set, of the opposition. It then emphasizes attack vectors based on vulnerability analysis. (Gregory Fontenot, "Seeing Red: Creating a Red-Team Capability for the Blue Force," *Military Review*, Sept.–Oct. 2005). Warrick describes how the CIA had implemented red teams to test the security of bases around the world in the aftermath of the Khost, Afghanistan, suicide bomber attack in 2009 (Joby Warrick, *The Triple Agent* [New York: Doubleday, 2011], 199). For more on red teams, see also, Michael K. Meehan, "Red Teaming for Law Enforcement," *The Police Chief* 74, no. 2 (February 2007): 22–28, and Stephen Sloan and Robert J. Bunker, *Red Team and Counterterrorism Training* (Norman, OK: University of Oklahoma Press, 2011).
4. For an examination of technical intelligence, see Robert M. Clark, *The Technical Collection of Intelligence* (Washington, DC: CQ Press, 2010).
5. Human intelligence can include the interrogation of non-official cover operatives, defectors, immigrants, liaisons, agents, double agents, defectors, and variations of these.

Chapter 11

Offensive Counterintelligence: Detection

Chapter 11 11 Offensive Counterintelligence: Detection

This topic examines the issues involved with the offensive counterintelligence principle of detection. Although this principle could be considered as part of a defensive counterintelligence program, it is included here under the auspices of offensive counterintelligence because the more passive countermeasures have been discussed in the chapters for defensive counterintelligence and what is discussed in this chapter are those aspects that involve more active measures. This chapter looks at these issues by exploring:

1. Detection in practice;
2. Preinvestigation; and
3. Investigation.

DETECTION IN PRACTICE

Detection is simply being aware that an event has taken place. In the case of counterintelligence, it is an event that is somehow associated with a breach or potential breach (including an attempted breach) of confidential information. The practice of detection follows five premises:

1. Identifying an event of concern;
2. Identifying the person(s) who were involved in the event;
3. Identifying the organizational association of the person(s) of interest;
4. Identifying the current location of the person(s) of interest;
and
5. Gathering the facts that indicate that the person(s) committed the event.

Each of these premises is examined in turn starting with an *event of concern*. This is used in a general sense in order not to limit the application to any class of event or to limit it to any particular type of practice (i.e., national security, military, law enforcement, business, or private). Nevertheless, the event of concern must be the center of a hostile information collection operation and is the beginning point for what can be considered the preinvestigation stage of an offensive counterintelligence operation.

PREINVESTIGATION

If, for example, an employee temporarily removes classified documents from the office and copies them, then there must be mechanisms in place that allow counterintelligence officers to recognize that this event has occurred (or to *identify* or signal/flag the event as requiring attention). The chapters on physical, personnel, information, and communications security discuss the practice of setting up systems to do this. Such systems are sometimes referred to as *trip wires*. Trip wires can be human assets (e.g., guards) or technical systems—alarms or digital image recording equipment, as well as others.

Once counterintelligence officers are alerted to an event of concern, the person or people involved need to be identified. Without a positive identification of the perpetrator(s), the ability to assess the damage caused by the breach is greatly reduced. That is to say that a counterintelligence officer could not conclude with confidence who may have been interested in the data and how that information was to be used and, from that, the implications the compromised data could have for the agency or its client. Although counterintelligence officers could estimate the potential damage and those who sought the information, as well as how they could possibly use it, this method would be based on inductive reasoning and hence not as reliable as knowing the identity of the person and the exact details involved in the breach.

The next step is to link perpetrators to the organization (opposition or otherwise) who would have been (or is) the ultimate recipient of the information. Although it is possible for a person to act alone without opposition support—a lone-wolf situation—in reality, this is not a likely

situation. Why would an individual act on his or her own without any association with anyone else or with any other organization? Even “leakers” work with others who receive the information.

Logically, an agency’s spies collect data to pass on to intelligence analysts who process the information to produce intelligence reports. Unless the event of concern involves an individual who has unilaterally embarked on a personal mission to uncover sinister happenings, it is hard to conceive a situation where no one else is involved. Even the “man-on-a-mission” person would surely give the information that is at the core of his or her distress to some legal authority for action or to the news media to expose. Accordingly, the perpetrator’s association with others needs to be identified. This allows for an assessment of damage and will aid evidence gathering—motivation is key to many a successful counterintelligence investigation. It also means that counterintelligence investigators can locate and interrogate the person as part of the investigation-in-chief.

“In the history of man’s struggle to survive there is no example of victory being won by purely defensive means.”*

* Peter Hamilton, *Espionage, Terrorism and Subversion in an Industrial Society* (Leatherhead, UK: Peter A. Heims Ltd., 1979), 131.

INVESTIGATION

Once the event of concern has triggered an alert and the person(s) involved, as well as their organizational affiliation, identified, they can be located in the preinvestigation stage. That accomplished, the investigation moves into the evidence-gathering phase. This phase sets out to establish the facts of the event. These facts help the counterintelligence investigator draw a picture of the event—what, where, when, who, how, and why. This approach is based on scientifically based techniques to locate, collect, and preserve evidence of the event. These are known as *criminalistics* or *forensics*. Whereas a criminal investigation seeks to collect evidence to prosecute the matter

in a court of law, a counterintelligence investigation may not^[1]—such an investigation may purposefully end in a counteroperation that obscures, confuses, or deceives the opposition. Nonetheless, a counterintelligence investigation has the same purpose in mind—to discover the truth of an allegation or a suspected breach of security policy or law.

Although there are many approaches to investigation, and equally many techniques for conducting an investigation, this section will canvass some of the more prominent methods. This is not to suggest that these are the only methods—they are presented as a way of exposing new counterintelligence officers to the practice.

Crime Scene

Every person leaves a trail as they go through life. From the time one rises in the morning to the time when they retire for the evening, every person touches or comes in contact with objects during the day. They are seen by others doing what they do and perhaps they leave physical and/or electronic “footprints” in the places where they travelled. It is in these contacts that the concept of the crime scene arises. A crime scene can be a place either in the kinetic world or in the virtual world. It is an area where activities of interest are thought to have taken place—in the context of counterintelligence an activity of interest could be, for instance, the suspected theft of classified material or a person’s unauthorized access to a restricted area.

But the crime scene is more than the immediate area where the activity of interest took place—for example, the filing cabinet where a file was taken. It includes the surrounding area within a reasonable distance; perhaps the entire room as well as doors, windows, and other access points to the room. The rationale is that these adjacent areas may hold clues to what took place and when it took place. More important, they may yield facts about who was involved. It is the counterintelligence investigator’s knowledge of crime scene searches and his or her experience in collecting physical evidence at crime scenes that may prove the most important aspect of the investigation. A small but vital clue could make or break the investigation.

The first step in a successful crime scene search is for the area to be isolated and secured from those not tasked with the investigation. This is to ensure that the area is not contaminated by others moving in and out of the area. It also ensures that any evidence remains where it was when the perpetrator(s) came in contact with it and ensures chain of custody (see appendix D).

Recording the Scene

Once the crime scene is secured, counterintelligence investigators then need to record the area as a means of recalling its details. It is particularly important to do this if the matter will eventually end in prosecution in a court of law. The three ways of recording the crime scene include sketches, photographs, which also include digital video recordings, and notes. Ideally, all three methods should be employed but, as with any busy, pressured job, not all three can be employed in every case. Such considerations as higher priority cases, limited resources, and agency policy may be factors that dictate a compromised approach to using all of these methods of recordings.

But in making that determination it is important that the investigators project their thinking into the future to the point where they need to take this information and act on it. The question to be asked is, "If shortcuts are taken now, how might they affect the outcome of the investigation?" At the very least, some handwritten notes in a field notebook can be made along with a rough sketch of the area. Cellular telephones have cameras built in (and some have digital video as well), so it would be a simple matter of taking a few photographs before departing the crime scene.

Sketches of the crime scene can be as simple as a drawing or as elaborate as a computer-aided diagram using a software package. When drawing a crime scene it is important to record the positions of particular pieces of evidence in relation to other objects in the area. If the crime scene is inside a building, it might be distance (even an estimate) to doors, windows, desks, computer workstations, and other room features. If the area is outside, say a dead drop used by the

suspect, then distances to trees, utility poles, pedestrian crosswalks, shops, and the like, depending on the situation, should be recorded.

Photographs do not have to be limited to the scene, though one effective approach is to photograph the crime scene starting from the general and moving to the specific, and the specific can be several areas within the overall area. Take for instance the outside crime scene of a discovered dead drop. The counterintelligence investigator may start with several photographs of the area looking from what might be the center out in the four directions—north, east, south, and west. He or she may then walk north, east, south, and west of the crime scene center and photograph the area looking back at it.

The investigator may also locate these area photographs in a larger photograph that has been organized from the air looking down at the entire area and its surrounds. If this latter point is beyond the budget of an agency, recall that there are satellite maps available from commercial providers on the Internet.

Then moving to the specific, the investigator may take several midrange photographs as a way of drawing the viewer's attention toward an object within the crime scene. These would be photographs that are not at the distance of the wide-area images but at a distance that is closer, but not close enough to cause the viewer to wonder where in the scene the photos were taken. Finally, close-up photographs should be taken of specific items or areas that show clues of value. In the case of the dead drop, it might be the hollow where the container holding the classified data was placed, the mark left to signal the dead drop needed "servicing," and so forth.

It is possible for a counterintelligence investigator with some degree of experience to take a number of purposeful photographs and then, using these, sketch the area (rather than rely on memory). Notes can also be deduced from photographs—for instance, descriptions of objects within the photographs, distances between objects, and where evidence was found. As the camera will record what the investigator sees it may be an efficient way of accomplishing the overall objective—accurately recording the crime scene. However, having said that, this is a compromise method and one not recommended unless under pressure and where the alternative is not to record the crime scene. As with all

compromises there may be practical drawbacks that may only come to light after the investigator leaves the crime scene.

The details of each photograph need to be recorded and this applies to both film-based photographs and digital photographs. If the photographs are to be used in a criminal prosecution, then the way the details are recorded and how the photographs are handled (i.e., so that the images are not inadvertently altered) need to comply with the rules for evidence in the legal jurisdiction in which the matter will be heard. These requirements will vary from country to country and by state, province, and tribunal (say, a military tribunal).

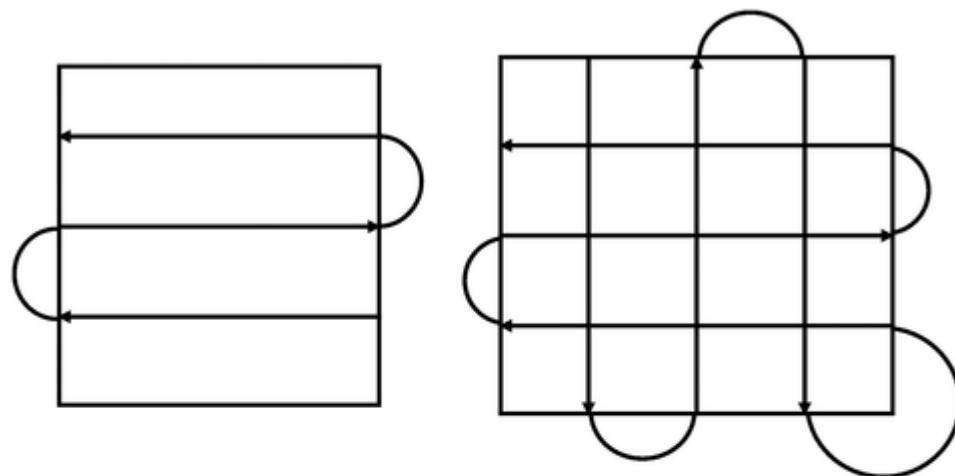
Notes should be made of any important aspect of the crime scene that the investigator may need to further his or her inquiries, or that may prove to be a lead for a further line of inquiry sometime in the future (recalling that the future may be years hence). If note taking is not possible at the minute the investigator is on the scene, perhaps due to the fact that they are in “hot pursuit” in an unfolding event, then digital recordings can be made, and, here again, cellular telephones have this facility. The investigator then transcribes his or her notes to paper or to an electronic document/database once back in the office, or via a communications link from a portable electronic device.

Search for Physical Evidence

The search for evidence can be approached several different ways and no one way is correct. It depends on the activity being investigated, area to be searched, and the objects within the crime scene. But, as a general proposition, the search needs to be based on some system. A systematic approach will help ensure that nothing is overlooked. There is nothing wrong with an investigator attending the crime scene and looking first for, and focusing on, obvious clues. But the counterintelligence investigator should then conduct a systematic search of the area to ensure that all possible evidence is collected and that the perpetrators have not placed decoy pieces of evidence in the area in the hopes of throwing investigators off track.

There are four generally accepted search patterns and these are shown in figure 11.1—the line search (upper left), the grid search (upper

right), the spiral search (lower left), and the sectorial search (lower right). Even though these basic patterns are shown as separate approaches, there is nothing preventing the counterintelligence investigator from combining two or more patterns if the objects within the crime scene prevent or obstruct the use of a particular pattern. For instance, returning to the dead drop example, if the dead drop is in a public park that features garden walls, ornamental ponds, and so on, a sectorial search might be appropriate, but within one sector a grid search could be conducted and, in the others, spiral searches.



Search patterns—clockwise from upper left—strip search, grid search, spiral search and sectorial search. Line search pattern—an investigator walks across the area in a line, then walks back across the area from the opposite direction, and so on. Grid search is the same as a line search, however the area is canvassed again; this time in a direction that is at a right angle to the first pattern. Spiral search pattern—starting at the outside of the crime scene and working in, or vice versa. Sectorial search pattern—each sector is divided into smaller zones and labeled so that each can be recorded as completed before moving to the next, and the next, and so forth, as illustrated in this example.

Courtesy of the author.

Physical Evidence

Evidence of a counterintelligence breach or an attempted breach can be either physical or digital. Here we summarize the physical aspects of evidence but will touch on evidence in the realm of computers and cybernetworks later in this section. As it is not possible to outline every possible event in which a security breach might take place, an overview will be provided to paint a picture of the depth and breadth of the type of objects that could be included.

Physical evidence can be large or even very large objects. They can also be small to microscopic particles. Those that are large enough for the investigator to see are logically those that can be detected in a crime scene search as being, say, out of place or, if common to the setting, somehow different or ones that might have been handled by the perpetrator, thus yielding clues.

In general there are two types of evidence, and these are termed trace evidence and link evidence. Trace evidence is created when two objects come in contact with each other and, in the contact process, material from one object is exchanged with the other, or both. For instance, when a person sits in the seat of a car with fabric seat covers, fibers from the person's clothes are left on the seat cover and fibers from the seat cover are picked up by the person's clothes. This is known as *Locard's exchange principle*. Dr. Edmond Locard was a forensic scientist who in 1910 established what many consider to be the world's first crime laboratory in Lyon, France.

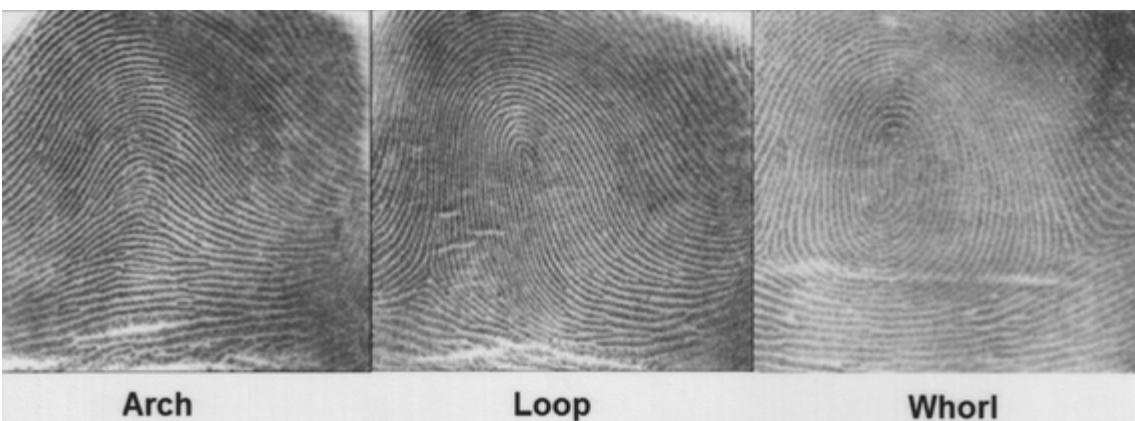
If one was to compile a list of the types of evidence that exist, the list would be very long indeed. However, the more common types of evidence include: fingerprints, DNA, hairs and fibers, documents, glass, impressions, paints, residues, soil, tool marks, and vegetative matter. In this section a few of the principal types will be discussed—fingerprinting, DNA, hair and fibers, and documents.

Fingerprints

The first type of physical evidence that comes to mind is a person's fingerprints. Fingerprinting has been used as a reliable source of identification for almost two hundred years. The first attempt at

formally classifying people's fingerprints was made by the Czech physiologist Professor Jan Evangelista Purkinje, in 1823. Since that time a series of scholarly developments and operational procedural refinements have increased the reliability and validity of the fingerprint system. Suffice to say that fingerprinting is a well-established science and is accepted in courts of law worldwide.

Counterintelligence investigators should therefore consider the collection of fingerprints as a potential source of evidence. The likelihood of a false positive (i.e., a Type I error) is enormously small and it is in this aspect that the power of this evidence lays. Fingerprint pioneer Francis Galton put this question forward when in 1892 he stated: "given two finger prints, which are alike in their minutiae, what is the chance that they were made by different persons?"^[2] Galton calculated that the chance of a Type I error was in the order of one in sixty-four billion. The chief drawback of fingerprinting is that there needs to be a sufficient print left on an object. A large enough print area is required so that the examiners can view the print in order to establish a number of points of similarity. Tied with this limitation is that the examiner needs a reference fingerprint to conduct his or her analysis. Without a reference print, no comparison can be done.



The three basic fingerprint patterns—arch, loop and whorl.

Courtesy of the U.S. Department of Commerce.

The arch pattern is characterized by ridges that pass from one side of the fingerprint to the other, forming a raised formation in the center that resembles an arch. The loop pattern features a series of ridges that

do not pass from one side to the other but rather “loop” in the center and terminate at the same starting point. The whorl is formed by a set of ridges that make a circular pattern in the center of the fingerprint. These three patterns are shown in figure 11.2.

DNA

DNA is shorthand for deoxyribonucleic acid, the material present in every cell in the human body. As such, collecting material at the crime scene that contains human DNA is another way to help identify a perpetrator as no two humans have the same DNA. Sources of DNA are many and include the following: blood, skin, sweat hair, dandruff, mucus, ear wax, and saliva. As with fingerprints, the power of being able to say that the sample collected does not match anyone other than the suspect is very strong. But, unlike fingerprints where a partial print may not contain enough of the pattern to be able to make a comparison, the amount of DNA needed to conduct a laboratory analysis in order to read the DNA “markers” is around one billionth of a gram.

Hairs and Fibers

Hairs and fibers can provide clues in two directions—linking the suspect to the crime scene and linking the crime scene to the suspect. That is, if the suspect has left hairs or fibers that he or she brought to the crime scene in the process of breaching security, these clues link the suspect to the scene. Moreover, if the suspect inadvertently collected hairs or fibers that were part of the area now determined as the crime scene and took these away, they link the scene to the suspect.

In the case of the latter, the suspect may have touched curtains or drapes in the office area that left fibers on his or her clothing. In the case of the former, the suspect may have had hairs of his or her pet dog on his clothing and these fell off in the crime scene area while they were there. In either case, these pieces of physical evidence can be analyzed in a laboratory and a probability assigned to the likelihood that these appearances of the hairs or fibers occurred by chance. Hairs can be

either human or animal (fur), and fibers can be from plants, minerals, or synthetic sources.

Documents

Document examination covers a wide range of forensic analyses that look to verify the source and authenticity of a document. It includes examining the words printed on the page as well as examining the document itself. Issues that might present for the counterintelligence investigator could include alterations to change the content or meaning of the words that appear on the printed page or alter the appearance of the physical form of the document. A person's handwriting may also be the subject of examination.

By way of example, an applicant for a security clearance may submit a number of documents in support of the application and one or more of these may be questioned. These *questioned documents* will have to be checked by an examiner with skills in detecting erasures and words that have been overwritten or crossed out using techniques of infrared and ultraviolet photography and microscopy. The actual paper stock and printing techniques may also be examined if the document is considered falsified—say, in the case of a passport.

When examining the printing techniques, the document examiner may need to examine documents produced by laser and other computer-associated printers, older facsimile machines, and photocopiers. With the steady increase in the quality of computer-based printing, forged documents are relatively easy to create using software packages. Although these documents may present as having no "alterations," their authenticity is what is questioned—that is, were they issued by the authority that is asserted on the document?

Interviews and Interrogations

The terms *interviewing* and *interrogation* are sometimes used interchangeably though in practice the two are different. An interview is an event where the investigator talks to a person who he or she

considers to have information relevant to the issue under investigation. An interrogation is to determine the innocence or guilt of a person. Although the two are integrally related, they are nonetheless distinct and different.

One way to look at interviews is that they are intended to collect information about the alleged breach, its background, events surrounding its occurrence, and what might have taken place after. It is information from those who observed it in its entirety or those who observed only aspects of it, or observed related events. Interviews can be informal—a brief, unstructured discussion lasting a few minutes—or formal, where the investigator systematically takes the interviewee through a sequence of events and then records the person's recollection in a written statement. The statement is then signed by the interviewee, the investigator, and perhaps a third party who witnesses their signatures. Alternatively, the interview may be recorded using audio-visual recording equipment and the discussion transcribed into text afterward.

The outcome of the interview process is to help build the case. Information from interviews can be used to discover new evidence and/or to obtain clarification about already discovered evidence.

If the purpose of an interrogation is to ascertain whether the suspect is innocent or guilty, then this is done by inducing the suspect to reveal:

- facts and circumstances pertinent to the breach under investigation, which might include the location of evidence that remains undiscovered (or even unknown), or alibis that support an assertion of innocence;
- an admission of guilt (e.g., a confession);
- accomplices to the security breach; and
- other security breaches by the suspect or his or her accomplices.

It is important to weigh all facts in the matter and follow up on all leads generated in the interrogation process, because selecting only the facts that support the hypothesis that the suspect is guilty is not only

ethically wrong, it is wrong in law (i.e., colloquially known as “framing” a person). It also means the true perpetrator has not been identified and risk of future damage remains.

Surveillance

Physical Surveillance

Surveillance is the observation of people, places, and objects. But surveillance is not something that is performed openly where the intent of the observer is declared. Surveillance is conducted covertly, or secretly, even though the *surveillant* (or *operator*) may be observed. So, surveillance is a secret activity not because the surveillants cannot be seen, but because their purpose would be considered by anyone observing them to be other than that of collecting information.

Surveillance can be used in a number of applications but a common use is to supplement information obtained from interviews or from evidence already collected. However, it can also be used to develop new leads in a case that is lacking direction or to corroborate existing information.

Surveillance is arguably both art and science. It uses time-tested techniques for carrying out observations of fixed locations (i.e., places and objects, and sometimes referred to as *static surveillance* or, more informally, as a *stakeout*) and for moving surveillance (referred to as *tailing* or *shadowing*). The techniques used to do such surveillances are voluminous and have been developed through a process of science and skillful interpretation of human behavior—this is where the art comes in.

As the craft of surveillance has developed, practitioners have developed their own terminology. A few examples suffice to demonstrate these terms: the subject of a surveillance operation is termed the *target* and the group tasked to conduct the surveillance is termed the *surveillance team*. The surveillant who has visual observation of the target is termed to have *command* (in the case where the surveillant changes throughout the operation). There are many others

but it is worth noting that, when discussing the use of surveillance in an investigation, those who are tasked to carry out the job may lapse into their own jargon.

Although surveillance can yield high-grade results, it is time consuming and has drawbacks. One is that, if a surveillance team is tasked to do a job, there is no guarantee that the operators will be at the right place at the right time. Large amounts of time and financial resources can be spent on surveillance with no results. For instance, a surveillance team may miss observing the anticipated event by minutes without even knowing it—the target may have departed just before the surveillance team arrived to take up their observation posts, or the operators may depart at the end of their shift only to have the target then arrive. To a large degree there is the element of chance involved with being successful with surveillance, unless operational resources and funds are available for twenty-four hour operations.

The biggest weakness is that all the advantages gained by carrying out a surveillance could vanish if an operator or the surveillance team is discovered (termed *burned*). As soon as the target is aware that he or she is being watched, he or she is likely to implement countersurveillance tactics and/or avoid the activity that the surveillance was designed to capture.

Information captured by surveillants may include a log of their stakeout or shadowing activities as well as pertinent events under their gaze. A log might record such details as start and finish times/dates, locations, field of view, people observed and what they were doing, the times these people were observed, and physical descriptions of them and the things they were doing. In short, anything that may help the investigation should be collected and recorded. In recording people and events during a surveillance, still and motion photography are almost always used. These images combined with logs and information provided by operators during their debriefing can be invaluable to the investigation.

Electronic Surveillance

Electronic surveillance covers a wide range of techniques for collecting evidence but is most likely to be in the form of audio surveillance (i.e., room listening devices or *bugs*) and telephonic intercepts. There are other forms of electronic surveillance, such as radio frequency intercepts (i.e., the interception of radio transmissions) and data interception relating to the Internet, but the most commonly used intercepts are likely to be audio methods.

The fundamental principle of any audio surveillance operation is to be able to plant a quality microphone as near as possible to the target and, in doing so, avoid background noise that may render the intercept unintelligible. There are hundreds of devices and as many methods for installing these devices, enough to fill many technical manuals. But all of these aspects relate to two simple principles. Because the farther a person is from the surveillance microphone, the less chance there is for collecting an intelligible voice message. And the more background noise, again, the less likely it is that the target's voice and the message it carries can be deciphered. Though there are several software packages that can filter background noise, it means a further step in digital processing that may degrade the fidelity of the original recording.

The telephone is arguably the most useful medium for electronic surveillance as its use is ubiquitous, even in the most remote places on the planet. Obtaining information using the telephone involves two methods: the first uses devices that intercept conversation directly from landlines and requires no entry into the target's property, and the second is intercepting the voice message as it passes over landlines to the telephone exchange. This applies to both landline telephones and cellular telephones as the latter share part of the landline system via what is termed a trunked network. That is, although the sender and receiver may be using radio signals to transmit to the nearest cell tower (i.e., a full duplex repeater), the voice message is then conveyed to the next cell tower via landlines.^[3]

Undercover Investigation

Operatives who go undercover during an investigation are able to get close to individuals or inside organizations to make firsthand observations. Such information can be valuable to an investigation because it is an opportunity to get a glimpse of the target's intentions, thereby providing an insight into the target's thinking, rationale, and behaviors that could not be obtained by other means.

But the use of operatives is risky for the operative, both physically and psychologically, and it is risky for the agency in many ways, too. The operative risks physical harm in the form of bodily injury and death as well as a range of psychological injuries spanning from mild anxiety to severe psychiatric disorders. The physical risks are more apparent as one can easily visualize the ramifications of having to penetrate an illegal enterprise. The psychological injuries arise from the stresses associated with working in isolation, working in a dangerous environment, and perhaps engaging in activity that is illegal (including consuming illicit drugs and alcohol in binge quantities).

However, given the risks and the monetary costs of conducting an undercover operation, it is a method that is not often used in the first instance. It is usually reserved as a means of last resort or for counterintelligence cases that pose a serious danger to society or national security.

Because the operative will be in direct contact with the target, there are a number of issues that must be kept in mind. The most important is that the operative's identity must be guarded with utmost secrecy. If knowledge of the operative leaks to the target, the operative's cover will not only be "blown," but also the operative is likely to suffer injury.

The goal of an undercover operative in a counterintelligence investigation is to infiltrate "as deep as possible and [gather information and evidence] on the opposition or enemy."*

* J. Kirk Barefoot, *Undercover Investigation* (Springfield, IL: Charles C. Thomas, 1975), 4.

Part of the operative's brief is to obtain evidence of wrongdoing (or innocence), as well as information generally related to the investigation. Evidence may be in the form of admissions, but intelligence data may also be in the form of indicators of intent. To capture these data the operative can either commit the details to memory and then record them later for transmission back to the agency or use some electronic device that transmits the data live for recording and transcription. The latter is the most reliable and the best solution as it does not rely on the operative's ability to remember the details, which, from an intelligence point of view, can be critical. Data can be qualitative (e.g., discussions with the target) and quantitative (e.g., numbers of items, times, routes, colors, preferences, and others).

Computer Forensics

Investigating the recording, storage, retrieval, and transmission of electronic data, as well as the means for transmission of these data packets over networks, falls to the investigator who is skilled in computer forensics. Although this may be a specialized field within counterintelligence investigation, all counterintelligence investigators should have at least an advanced working knowledge of the issues involved in probing the cyberworld. Such inquiries are known as *computer forensic examinations*.

The days where data were predominately based in paper files started to disappear in the 1980s when the microcomputer (later known as the *personal computer* or, simply, *PC*) became affordable to businesses and individuals. Now, governments, businesses, and peoples' personal lives could not function without digital computing. It follows that security breaches are most likely to first occur in a computer system and then lead to the kinetic world. So, given this scenario, digital evidence should be a prime consideration in investigating security breaches and other counterintelligence issues. The forensic processes and investigative techniques parallel the physical world and similar steps are taken to secure the crime scene and prevent people from destroying or removing potential evidence by the electronic equivalent of cordoning off the

equipment and network access and well as restricting physical entry into the area.^[4]

Depending on the situation, equipment may need to be removed from the crime scene, or examined in place. Like with a physical crime scene, procedures are sequential to ensure preservation of data vital to the investigation. This information may lead investigators to other sources or the potential identity of the perpetrator. There are growing numbers of analytic software programs that allow the computer forensic investigator to explore the digital crime scene looking for clues.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Bugs;
- Burned;
- Command;
- Computer forensic examinations;
- Criminalistics;
- Forensics;
- Interrogation;
- Interview;
- Investigation;
- Locard's exchange principle;
- Operator;
- Shadowing;
- Stakeout;
- Surveillance team;
- Surveillant;
- Tailing;
- Target; and
- Trip wires.

STUDY QUESTIONS

1. In order, list the five premises of detection.
2. Describe three ways a counterintelligence investigator can record a crime scene and then discuss the pros and cons of each method.
3. List the four generally accepted search methods and explain the theory that underpins systematic searching.
4. What is the fundamental principle of any audio surveillance operation? In a hypothetical situation, explain how this might be accomplished.

LEARNING ACTIVITY

For this learning activity you will need: (1) a black ink pad; (2) a sheet of paper; and (3) a magnifying glass. Starting with your index finger, gently roll the finger on the ink pad and then roll the finger on the sheet of paper leaving room for the other fingers. Follow this with a print of each of the remaining fingers and thumb. Once the ink dries, use the magnifying glass to observe the patterns. Although there are many different fingerprint patterns, there are three that form the basis for all others—the arch, loop, and whorl. These three patterns are shown in figure 11.2. Using these indicative patterns as an initial guide, determine the basic pattern of your fingerprints. Are all the fingerprints of the same pattern? Compare your fingerprints to those of, say, another family member, a friend, or work colleague. What have your observations revealed? Explain.

NOTES

1. Although a deception or neutralization operation may be the prime focus of such an investigation, a criminal prosecution cannot be discounted; take for instance the cases involving Aldrich Ames and Robert Hanssen.
2. Francis Galton, *Finger Prints* (New York: Macmillan, 1892), 110.
3. This is a simplified explanation of what actually happens—for instance, the transmission from the two parties could also include satellite links if the people are in different countries. Or it could include microwave links and other combinations if in different regions of the same continent. Nevertheless, interception can be by accessing a node that handles the transmissions from the cellular handset.

4. Bear in mind that people can access information stored on workstations and data servers remotely—physical presence at a terminal in the “restricted area” may not always be required.

Chapter 12

Offensive Counterintelligence: Deception

Chapter 12 12 Offensive Counterintelligence: Deception

Deception is one of the four counterintelligence principles that form the quartet that comprises counterintelligence theory. This is an active countermeasure and this chapter examines deception in relation to:

1. Cognition;
2. Decoys;
3. Camouflage;
4. Pretexts and ruses; and
5. Case study regarding “the man who never was.”

COGNITION

Deception is a method an agency can use to overpower the cognitive processes of opposition agents, operatives, officers, and analysts in order to induce errors in their thinking. These errant perceptions can, in turn, be exploited.

Not surprisingly, deception finds its theoretical roots in cognitive psychology. This is a subbranch of the discipline of psychology that examines a person’s mental process relating to perception, memory, reasoning, and decision making. Because it recognizes internal mental states, such as mental imagery, belief, motivation, and desire, the reverse application of cognitive psychological principles can be used to deceive. In essence, this is done by presenting a situation that resembles what one might expect to exist in a particular setting, but in fact is a pure fiction. Magic is an act of deception that comes to mind and this was used by the Central Intelligence Agency (and no doubt other intelligence services) to its advantage. These exploits are discussed in

the now declassified manual entitled *The Official CIA Manual of Trickery and Deception*.^[1]

The historical record on intelligence and espionage activities is replete with examples: Allen Dulles summarizes four classic cases in his book *Great True Spy Stories*, including Ewen Montagu's World War II deception that featured in the now famous tale of "The Man Who Never Was."^[2] Pretexts and ruses are used regularly by private investigators and can be exploited in counterintelligence operations in the same way. In espionage, pretext is synonymous with *cover* (e.g., a cover story, a cover identify, etc.). Camouflage is a trick technique that makes objects disappear. And decoys achieve deception by presenting the opposition with what appear to be viable targets but are nothing more than illusions.

DECOYS

Anyone familiar with duck hunting will be aware of the use of decoys. These are usually wooden or plastic replicas placed in, say, a pond to tempt ducks passing overhead to stop and join them. Once the real ducks are sitting next to the decoys, the hunter has his target. The same intent and psychology is employed in offensive counterintelligence operations. Counterintelligence personnel conducting an offensive operation can use decoys to confuse the opposition. There are several contexts in which decoys can be used and the chief uses will be discussed—political decoys (or body doubles), voice decoys, ghost armies, and computer decoys.

A political decoy is someone who stands in for a high-profile political leader, usually in times of peril, to deceive the opposition. The political decoy is selected for his or her physical resemblance to the leader being protected. Acting lessons and instructions as to how the decoy should impersonate the protected person are part of the operation, as is dress, deportment, and elocution.

The use of a political decoy has great offensive advantage as it not only offers an alternative target (in the literal sense) to the leader; the planned activities and places visited by the decoy can mislead and/or confuse the opposition. This has the effect of expending surveillance

resources and analysis time and energy on tasks that are barren and fruitless.

A voice-only decoy performs the same role and function as a political decoy but is limited to oral impersonation of the protected person. This may include providing telephone interviews or radio and other media appearances. Terrorists and leaders of outlawed and underground groups, as well as a range of criminals, have been known to use this method. These are usually voice recordings sent to authorities to make demands, taunt, or simply waste their time and energy and, in the process, project the appearance that they are somewhere where they are not, or in a place at a time when they were not, or both.



Decoys come in many forms—here an American AH-64D Apache helicopter firing decoy flares during a mission over Iraq on April 29, 2011.

Photograph by Chief Warrant Officer Daniel McClinton. Courtesy of the U.S. Army.

A *ghost army* is the term soldiers used during World War II for a unit of the U.S. Army—the 23rd Headquarters Special Troops. Its mission was to present a false picture of the Allied military's strength, location,

and intent to the Nazi military leaders. This unit used a number of creative deceptive methods to achieve this, including visual, sonic, and radio deceptions. Inflatable rubberized tanks, field artillery, jeeps, and even inflatable aircraft were used so that enemy reconnaissance aircraft would spot them and report these decoy sightings.

Using troops with an abundance of imagination, creative skills, and artistry, it is now known that the once-classified project could erect airfields, bivouacs, and tank formations with a very short period of time. It is estimated that some twenty battlefield operations were staged by the ghost army during the Second World War.^[3] The 23rd Headquarters Special Troops also used fictitious radio signals and traffic, special effects (“atmosphere”^[4]), and noises (e.g., the grinding and clanking of tanks) to deceive Nazis forces.

It is understood that, during the Vietnam War, U.S. forces used dummy paratroops made of ice to simulate an airborne assault in order to flush out hidden Viet Cong units. The Viet Cong troops would see the paratroopers land nearby and would come out of hiding to move to the landing zone to engage these enemy troops. But when the Viet Cong arrived the ice (i.e., the paratroop decoys, or PDs) would have melted in the heat of the steamy jungle. It was reasoned that the Viet Cong would then be duped into believing that the decoy troops were, perhaps, in a defensive position nearby. In the meantime, an air strike would be called in to destroy the Viet Cong at the PD landing zone. Because of their effectiveness, it is understood that paratroop decoys are still being used from time to time in various conflicts around the world.

Decoys can be in either two-dimensional or three-dimensional models. Two-dimensional decoys can be configured in a vertical or a horizontal profile. Vertically constructed decoys are used for presenting a view from the front or sides (e.g., a battlefield decoy presented to the opposing forces), whereas horizontal decoys are used for presenting a profile to over-flying surveillance aircraft and satellites. Three-dimensional decoys can be used for either application—ground surveillance from the front or sides, as well as aerial reconnaissance.

Computer Decoys

In cyberspace physical decoys have no value. However, the concept can still be applied to these digital zones on the Internet. Termed *honeypots*, these are decoys that attract the opposition like duck decoys do for the small-game hunters. This honeypot method is not to be confused with the method of recruiting an agent through sexual seduction, though the principle of luring the opposition into the trap is analogous and hence the use of the term. A computer honeypot can be used to simply detect interest in an agency or its client's activities or to deflect the opposition away from the real activity.

A honeypot as its name implies is considered a piece of bait or a lure that attracts the opposition to it. The honeypot might be a computer, stored data, or a network. Although it appears to be part of a larger network, the honeypot is usually an isolated facility that allows counterintelligence personnel to monitor those accessing the honeypot. Computer honeypots can also be used to sow disinformation in another type of offensive counterintelligence operation—neutralization (see the section on “traps” in chapter thirteen).

CAMOUFLAGE

If the purpose of a decoy is to present the illusion that something that does not exist is present, then the purpose of camouflage is the reverse—to make something that is present disappear. Camouflage is therefore the polar opposite of decoys. It is a time-tested and proved method of deception.^[5]

Although the prominent image of camouflage is a military vehicle hidden under a net of natural or manmade material so that it blends in with its surrounds, the principles of camouflage extend well beyond such a narrow application. For instance, the opposition may use camouflage to cloak their espionage activities. If the opposition is a terrorist group, then camouflage can be used to screen their subversive doings. One of the first forms of screening that comes to mind when thinking about such a group is the use of a *front organization*. For all intents and purposes a front organization appears to be a legitimate organization with visible business-like activity. However, behind the

organization's movie-set image will lay a clandestine operation that has an entirely different purpose.

Camouflage can also be used in an urban setting. Although mainly thought of as a means of disguising personnel and materiel deployed about the countryside, the same techniques can apply to city and suburban settings to make people and things blend in.

Businesses and Companies

Sometimes an agency might need to run an operation that needs to operate in the open—perhaps as a business or company trading in goods or services. Ostensibly, this company operates as any other business in the commercial marketplace, but behind the management structure exists a clandestine purpose; one that is designed to support an intelligence operation.

“You can fool all the people all the time if the advertising is right and the budget is big enough.”*

* Attributed to the late, American film producer Joseph E. Levine (September 9, 1905–July 31, 1987).

An example of a front company for intelligence operations is Air America. It supported covert action in Southeast Asia, Central America, and Africa. The bona fide airline was needed to maintain cover for the paramilitary operations that included “supplying guerrilla forces in Laos, moving Cuban émigrés to their training bases or ferrying arms to Angola.”^[6] Many other dummy companies have existed from time to time in both Western and the former Soviet-Bloc countries. These were used for a variety of tasks ranging from procurement to storage to transport. Also, they have been used to maintain facilities and staff to conduct specialized training, or to conduct propaganda operations. Take for instance the use of clandestine broadcasting stations as a form of front company. These stations transmit politically based messages and programs, or information that has an underlying political tone. They use

call signs like other broadcasters and have scheduled programs and news, but the backers of these stations are intelligence services.^[7]

The purposes of clandestine front organizations can be as varied as the secret groups operating. However, in the context of an offensive counterintelligence operation using deception, a front organization may be one that is established by the agency to mask its undercover operatives—for instance, a warehouse-type operation where operatives come and go camouflaged as tradesmen (say, as electricians) or a bed and breakfast-style accommodation that is a safe house for agents and operatives. In this sense, camouflage can be used to screen personnel, organizations, installations or buildings, and other objects.

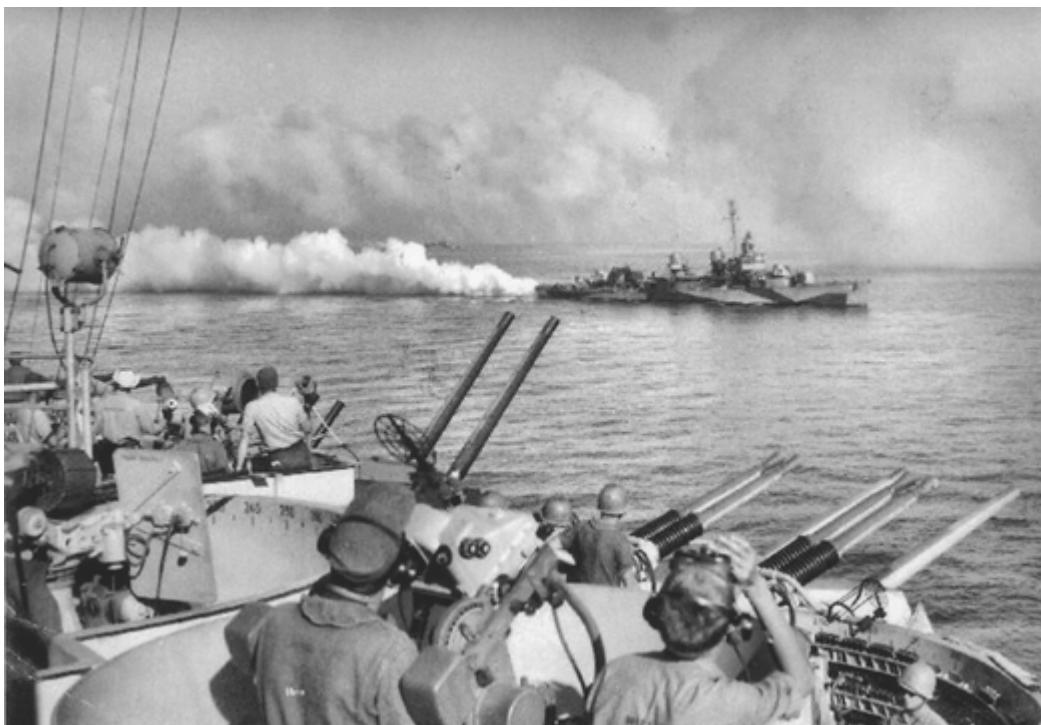
Environmental Camouflage

Returning to the traditional application of the term—the use of natural or manmade materials to make an object or person blend in with the surrounds—a number of methods have been used to make objects disappear from view. These methods can use live or cut vegetation, or artificial materials arranged as drapes, flat tops, and screens. Or they can be used to simply disrupt the true outline or pattern formed by the person or object. An example of the latter can be seen in the archival photograph of the Fletcher-class destroyer USS *Cony* during the Second World War (figures 12.2 and 12.3). In these photographs the ship's hull is painted a disruptive pattern to distort the ship's outline.

A drape is a hiding device that is erected vertically, whereas a flat top is erected a meter or so above an object (but can drape down at the edges). This can be used to camouflage small, fixed positions, or mobile units that are at rest (e.g., a parked vehicle). An example of a screen is the use of smoke. A smoke screen is a thick “cloud” of smoke that is laid between the object at the center of the deception and those trying to view the same (see figure 12.3).



USS Cony (DD-508) painted in a disruptive camouflage pattern, February 25, 1944.
Courtesy of the U.S. Navy.



USS Cony (DD-508) (background) laying down a smoke screen off Leyte, Philippine Islands, October 24, 1944. The smoke screen was intended to hide the Colorado-class battleship, **USS West Virginia** (BB-48) from Japanese torpedo bombers. Also note **USS Cony's** disruptive wartime camouflage pattern.

Courtesy of the U.S. National Archives.

PRETEXTS AND RUSES

A *pretext* is used in espionage as a method for obtaining confidential information. A pretext is any act of deception—ruse, subterfuge, ploy, trick, or a cover story—that allows an operative to solicit information by a false reason. This includes entering premises or countries for obtaining information or being in a place that an operative wouldn't otherwise have access to or permission for or simply to be inconspicuous. In a counterintelligence context, the pretext can be used for the same purpose; however, the intent is not to obtain intelligence to supply analysts with data for synthesizing into an intelligence product. Instead, it is a deceptive technique that allows access to information to provide operational security.

CASE STUDY: THE MAN WHO NEVER WAS

During the Second World War, between 1942 and 1943, the Allies were preparing to invade Italy. A seaborne invasion relies on a number of factors in order to be successful and the ability to establish a beachhead is just one. If reinforcements and resupply, as well as the ability to advance off the beachhead in a reasonably short period of time, were not possible, these issues could factor against the operation's success.

The Axis forces were highly aware that the Allies were anticipating such an invasion, having fought them throughout North Africa and monitoring their advance in the region. The Nazi's Supreme High Command had focused its many intelligence assets on the production of intelligence assessments that would inform them where such an invasion might take place in order to anticipate this and to have the potential beachhead fortified in order to destroy the Allies' forces.^[8]

The British mounted an offensive counterintelligence operation using deception to safeguard the location of the invasion—Operation Mincemeat. The plan was to convince the Supreme High Command that the invasion was to take place in Greece and Sardinia instead of the actual location of the island of Sicily.



Welshman Glyndwr Michael, who was “recruited” into the Royal Marines after his death to become, Captain (Acting Major) William Martin in the 1943 offensive counterintelligence deception code named Operation Mincemeat.

Courtesy of the Public Records Office, United Kingdom.

In order to deceive the Nazis, British Naval Intelligence devised the scheme to plant a number of falsified documents so that the Germans would find them and believe them to be true, and act on their content. The documents were secret plans of the invasion of Italy as well as supporting documents. The documents were planted in an official British government briefcase carried by the corpse of Welsh civilian Glyndwr Michael. Mr. Michael was presented as the fictitious Captain (Acting Major) William Martin of the Royal Marines and fitted with battledress—hence the description, “the man who never was.”

Major Martin’s death was concocted to appear that he died at sea after an aircraft crash (hypothermia and drowning) while couriering the secret documents. His body was placed overboard from the British submarine HMS *Seraph* off the coast of Huelva, Spain at a place where the tide would take the corpse ashore. Huelva was selected as the spot of the deception as it was consistent with Allied air traffic to North Africa and British intelligence understood that there was a Nazi *Abwehr* agent who maintained contact with the local Spanish officials. As such, the secret documents would subsequently become known to German intelligence. Major Martin also carried a number of personal effects and

personal papers that, when inspected by the German intelligence, would draw them to conclude the scenario was true.^[9]

The British then perpetuated the ruse by placing a death notice in *The Times* and transmitting messages that gave the impression that British military commanders were desperate to retrieve the briefcase and its documents. This appeared to work as German intelligence put pressure on Spanish secret police to locate the papers. Once German intelligence finally examined the secret documents, they considered them authentic and the deception was complete. History shows that, on July 10, 1943, the Allies successfully invaded Sicily and there is little doubt this was due in large part to this counterintelligence deception.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Camouflage;
- Computer honeypot;
- Decoy;
- Ghost army; and
- Pretext.

STUDY QUESTIONS

1. Explain the role cognition plays in counterintelligence deception operations.
2. Describe two hypothetical situations where the use of camouflage could be employed in counterintelligence—one in a military context and the other in a private counterintelligence setting.
3. Describe two hypothetical situations where a pretext could be employed in counterintelligence—one in a law enforcement context and the other in a corporate counterintelligence setting.

4. Argue the case why Operation Mincemeat was so successful.

LEARNING ACTIVITY

Using the concept of a front organization in the context of a law enforcement operation of your choosing, describe how such a deception could be created and employed. What type of information could be protected using your example? What type of information, if any, could be collected this way? What are the key considerations for the deception to succeed? Explain.

NOTES

1. H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (New York: William Morrow, 2009).
2. Ewen Montagu, “The Man Who Never Was” in *Great True Spy Stories*, ed. Allen Dulles (Secaucus, NJ: Castle, 1968), 256–62.
3. Jack M. Kneece, *Ghost Army of World War II* (Gretna, LA: Pelican Publishing Company, 2001), 280.
4. The term *atmosphere* includes the wearing of uniform shoulder patches, vehicle bumper markings, the display of signage, and the production of traffic that would be associated with the activity trying to be created. Kneece, *Ghost Army of World War II*, 154.
5. For an excellent discussion about the artists and designers who contributed to giving invisibility its place in modern defenses through the use of camouflage, see Ann Elias, *Camouflage Australia: Art, Nature, Science, and War* (Sydney: University Press, 2011).
6. Harry Rositzke, *The CIA’s Secret Operations: Espionage, Counterespionage and Covert Action* (New York: Reader’s Digest Press, 1977), 183.
7. Hank Prunckun, “The Secret Spectrum—Clandestine Broadcasting,” *Amateur Radio*, September 2006, 10–11.
8. J. C. Masterman, *The Double-Cross System in the War of 1939 to 1945* (Canberra: Australian National University Press, 1972), 133–38.
9. This is termed *pocket litter*. These bits of paper (e.g., a theater ticket stub, a wallet photograph, clothing labels, etc.) produce “footprints” that help to establish evidence in support of the false story being presented. H. H. A. Cooper and Lawrence J. Redlinger, *Catching Spies: Principles and Practices of Counterespionage* (Boulder, CO: Paladin Press, 1988), 261–62.

Chapter 13

Offensive Counterintelligence: Neutralization

Chapter 13 13 Offensive Counterintelligence: Neutralization

This topic discusses neutralization. This is an active countermeasure and this chapter examines offensive strategy in relation to:

1. Counterespionage;
2. Traps;
3. Agents provocateurs;
4. Spies and counterspies;
5. Double agents; and
6. Double-crosses.

COUNTERESPIONAGE

The children's saying of "sticks and stones may break my bones, but words will never hurt me" must have been coined by someone who also believed that fairies lived at the end of their garden. Nothing could be further from the truth. If this saying had any semblance of truth then why would laws exist to govern defamation—libel and slander—and why would intelligence operatives seek information (words . . .) that could discredit the opposition, or be used to blackmail opposition personnel, or undermine opposition operations, and so on? A person would have to be naïve to think that only a physical attack may inflict injury and an attack that uses information cannot.

The use of neutralization as a method for dealing with the opposition is clearly an offensive stance and is termed *counterespionage*. At face value, counterespionage can present as simple spying but it is a specific counterintelligence function. It is a precise function that is the most subtle and sophisticated of all the counterintelligence functions. It calls for the engineering of complex strategies that deliberately put

one's operatives and/or agents in direct contact with the opposition's intelligence personnel. This is done so that the opposition can be fed disinformation, which should lead to confusion, thus disrupting the opposition's plans and allowing the agency and its client to prosper.

In his landmark study of subversion, Professor Edward Luttwak described counterespionage as "the most subtle and sophisticated of all the functions. . . . [As such,] it is unlikely that more than one agency carries out this work because it requires an extremely precise control over operations . . . especially over counterintelligence, which relates to counterespionage as a butcher does to a surgeon."^[1]

Although Luttwak's description sums up the function's complexities, it unfortunately separates counterespionage from counterintelligence, which is not the view taken by this writer. Counterespionage is in fact integrally tied to counterintelligence but forms the offensive arm—to neutralize the opposition. Counterespionage has been described as "the clandestine warfare waged between rival intelligence agencies," "usually referred to more delicately in the spy business as counterintelligence."^[2] The key strategies that comprise neutralization involve "cunning entrapments, agents provocateurs, spies and counterspies, double and triple crosses. It is the stuff spy novels are made of, with limitless possibilities for deception and turns of plot."^[3]

"Counterespionage is often touted as the aristocratic sector of secret operations. In the romantic image the counterespionage man is pitted against his fellow professionals on the other side who are trying to get his nation's secrets. His job is to foil them. It is a true adversary relationship unlike the espionage situation, in which two men work together to purloin secrets. Most spy stories are not about spying but about counterspying."*

* Harry Rositzke, *CIA's Secret Operations: Espionage, Counterespionage, and Covert Action* (New York: Reader's Digest Press, 1977), 119.

TRAPS

In a law enforcement sense, entrapment is where an officer of the law, or an agent of the government, coaxes a person or group to commit (or omit) an act that is illegal. It is where the commission (or omission) was not in the mind of the person or group before the law enforcement officer or the government agent put it forward. In effect, there was no criminal intent before the notion was advanced and encouraged by the officer/agent. While entrapment is not legal, it is, however, permissible in law to “dangle bait” for those who have already formulated intent and see the bait as one of a number of opportunities that they can target.

In this sense, offensive counterintelligence officers may do the same thing. That is, they may set up a *trap* to entice an opposition spy or place one of their own operatives purposefully in front of the opposition as bait for them to attempt to recruit. It is this sense of the terms that is used here—not the illegal setting up of incident victims.

Many variations of traps are possible including *sting operations*.^[4] For instance, say there is a newly assigned officer to a foreign post who is given cover that makes her look attractive as a potential recruit. She may be located in an area of operations that allows her access to sensitive information, or have access to people who have that access. She may present at, say, social engagements in any number of personas that project the image that she may be approachable as a recruit. All along, she is a counterintelligence officer waiting for the “offer” and, once recruited by the opposition, she is seen as their double agent. But the opposition has been caught in a sting operation. Some indicative examples from law enforcement include:

- Positioning an attractive motor vehicle to catch automobile thieves;
- Arranging for a person under the legal drinking age to ask an adult to purchase them alcoholic beverages;
- Placing an officer/agent in the street where illicit drugs or contraband are sold to catch traffickers;

- Passing small arms or (deactivated) explosives to a would-be terrorist; and
- Setting up a honeypot computer to lure criminal hackers or to gain information about hackers' activities.

Of course, the opposition will be anticipating the possibility and before making their approach to her, they will have tried to establish whether there is any chance of her being a plant. They will continue the watch and observe her induction into their scheme; interrogation and polygraph examination may feature as part of this process. The opposition may request that their newly recruited agent obtain certain information as a way of testing her: first, to determine whether she has access to the types of information claimed; second, to confirm she is willing to follow through with her commitment; and, third, to establish a hook that the opposition can use as blackmail to help ensure continued pressure.

One method of setting up potential traps is to present defectors (including new immigrants and other such categories of displaced people) to the opposition. Then, in the interview/interrogation process, the opposition realizes the intelligence potential in the person and tries to “turn” them into a double agent. But, in fact, if they were placed in this position (as in the example just given), they become a triple agent.

Or it could involve setting up a situation made legion in espionage fiction—the honeypot. Honeypot is a term that loosely refers to a situation where the opposition uses a person who can engage the agency's officer in a romantic or sexual relationship, and then use either the emotional dependency thus established or the dependent need of the sexual contact as blackmail to exploit for intelligence gathering.

In the computer realm, honeypots are situations that are “as sweet as” the promise of sexual contact, and attract cyberspies. The computer honeypot appears for all intents and purposes as the real thing (whatever that may be) but is in effect false (a deception)—like a decoy discussed in the previous chapter. Once lured into the trap, the counterintelligence officer can then exploit the trapped spy as deemed necessary.

The core of a counterespionage trap is the theory of *assumed vulnerability*. That is, everyone is deemed to have at least one vulnerability. If this vulnerability is discovered, say, through poor physical, communications, or personnel counterintelligence practices, then this weakness can be exploited. There is little sense in sending a physically attractive male to entice a potential woman agent if the woman is not heterosexual. Likewise, there is no sense offering money to someone who is financially well off or otherwise not attracted to the idea of material wealth. The vulnerability must be targeted.

AGENTS PROVOCATEURS

In the previous section we discussed the setting of traps to catch those who are intent on committing treason and, depending on the operation, turn the agent (double agent operation) or exploit the information they have (defector). We differentiated between the legal interpretation of entrapment and trapping. However, in some situations where an agency is allowed to engage in entrapment, the concept of *agents provocateurs* is used. This method of offensive counterintelligence is where an operative somehow induces others to engage in an activity that, once committed, leads them into disrepute, unlawfulness, or other forms of infamy. This can be seen in the following theoretical sequence:

- A counterintelligence operative works for Agency A.
- Opposition B is antagonistic, belligerent, and/or in competition with Agency A or Agency A's client.
- Opposition B (or its client) has a friendly relationship with Group C.
- Operative A makes contact with Opposition B using the ruse that he is with Group C.
- Operative A using various methods gains the confidence of Opposition B and induces its personnel to do certain acts.
- These acts are then exposed by Agency A and public opinion/legal authorities condemn Opposition B or take legal action against it.

By way of example, take the following as a possible situation. There exists a large and growing group of prodemocratic protesters in an authoritarian country. In order to discredit the hitherto peaceful protests in the eyes of the world, the authoritarian regime sends a unit of counterintelligence officers—the agents provocateurs—into the large group of protesters to cause the group to become agitated and unruly and either commit or see the agents provocateurs commit violence. Anticipating this outcome, the authoritarian regime has provided for the world’s media to be present to record and televise the violence. The authoritarian regime then denounces the protesters as violent criminals and uses this provocation as the reason to crack down on the protestors.

Many and varied scenarios can be crafted around the theoretical underpinning of provocation. These can be either against an opposition, or in support of a friendly ally. The latter point—in support of a friendly ally—should not be overlooked. Counterintelligence work can often be in support of allies.

SPIES AND COUNTERSPIES

Spies are operatives who go forward to obtain sensitive information. Their methods are many, but the point is that their task is usually focused on a single purpose—to collect sensitive information. In contrast, *counterspies* is a colloquial term for counterintelligence officers, security personnel, and investigators. Their job is to protect sensitive information, investigate breaches of security, or run offensive counterintelligence operations against the opposition.

“If the spy is the sword, the counterspy is the shield.”*

* Bob Burton, *Top Secret: A Clandestine Operator’s Glossary of Terms* (Boulder, CO: Paladin Press, 1986), 30.

DOUBLE AGENTS

Double agents are likely to be both a scourge and a blessing for counterintelligence officers. It is a scourge in the sense that identifying one that may be operating in an agency will be a task of sizable proportions. However, if the double agent is under the control of the agency counterintelligence officer, then the tables are turned on the opposition.

A double agent, usually, starts off working for, say, the opposition. He is, at some stage of his career, with the opposition recruited (or self-recruited in the form of a secret defection). The defecting opposition operative is debriefed by the agency on all important aspects of the defector, his life, and career, and details of the opposition and/or its client are obtained, recorded, and analyzed. If the defector stays in the employ of the opposition and continues to provide sensitive information to the agency, he is known as an *agent doubled-in-place*.

Although this may be a common route into the doubling of agents, another method is also known—that is, the recruiting of an opposition-leaning officer who, once employed with the agency, defects. A case in point is that of the former British intelligence officer Harold Adrian Russell “Kim” Philby. Philby was one of several Cambridge University students who, in the 1930s, became absorbed by the romantic notions offered by communism. This philosophical position later led him (as well as others) to side with Soviet intelligence and to be, in essence, a double agent. His espionage activities naturalized many British, and perhaps other allied intelligence services’, operations and, in some instances, ended in the deaths of agents.

A triple agent is an extension of the double agent. Using the above example of an agent doubled in place, he would become a triple agent if he then had second thoughts about his defection and confessed to his opposition service what he had done and what he told the agency. If the opposition considered it worthwhile, they could then turn him again, thus becoming a triple agent. This, however, would be a very difficult case to manage. Although there is no empirical evidence to support this, it would be reasonable to conclude that such cases would be rare because of the inherent difficulty in dealing with such a disloyal and intensely narcissistic person. For instance, what would stop him from becoming a quadruple agent? Nevertheless, Joby Warwick documents a

case where an al-Qaeda mole infiltrated the CIA in a triple-agent operation.^[5]

In this regard, there is little doubt that agent controllers have a perennial problem in continually assessing the accuracy of the information being provided by a double agent. Even if the double agent is reliable and provides what he considers to be quality information, it is possible that the opposition may suspect his treachery and place in his way what is akin to a “barium meal”—that is, a pieces of information that can be traced back to him through, say, an opposition double agent in the agency. This could flush out the defector and make him ripe for turning again. Or, as the British did during the Second World War under what has become known as the *double-cross system*, the agent could be eliminated (one way or another) and replaced with one of their own in order to feed disinformation to the opposition.^[6]

“Get your facts first and then you can distort them as you please.”*

* This quotation has been attributed to Samuel Langhorne Clemens (November 30, 1835–April 21, 1910), the American author and humorist who wrote under the pseudonym of Mark Twain.

DOUBLE-CROSSES

Although the exploits of British intelligence under the Twenty Committee during World War Two are legendary, another example from history will serve to underscore how this method can be used to neutralize the operations of the opposition. During the tail-end of the Russian Civil War (which followed the October 1917 Bolshevik Revolution and ultimately resulted in the collapse of the Russian Empire), the secret police ran a decoy underground organization that held itself out as anti-Bolshevik. This counterintelligence operation was known as the *Operation Trust* and ran from 1921 to 1926. History documents many of the trust’s operations, but one of the most well-known is the double-cross operation that captured British secret agent Sidney Reilly.

Reilly, whose “real name was Rosenblum . . . [having] taken his name from his father-in-law, an Irishman named Callahan,”^[7] was born in Odessa under what was then the Russian Empire. He was involved in counterrevolutionary stratagems against the Bolsheviks and was, amongst several roles he played in espionage, an operative for the British Secret Intelligence Service (MI6).

His secret operations ended in 1925 when he was caught in a double-cross operation orchestrated by the trust. Lured into Russia by counterintelligence operatives posing as anti-Bolsheviks, he was reported to have been shot by Russian border guards while trying to cross at the Finnish frontier, but was likely taken to a dacha near Moscow and interrogated.^[8] Reports state that he was executed shortly thereafter.^[9] British secret agent R. H. Bruce Lockhart, writing in his memoirs, stated that “such evidence as is available would seem to prove that he walked into a Bolshevik trap, and that his [anti-Bolshevik White] Guards officers, whom he met abroad, were really Cheka agents . . . ,”^[10] who betrayed the faith and alliance he gave them in a double-cross operation.

Case managers for double agents need access to agency files across many compartmentalized groups so they don’t, for instance, “buy” the same agent twice, or run an agent against himself. (This is tenet eight of Offensive Counterintelligence [synergy with defensive counterintelligence]).

But double-crosses are not only the purview of national security or military operations. The world of commerce and industry is also a topical area for double-crosses. For many decades the area of industrial spying has been in the subject literature but mainly to document intelligence-gathering methods and some security issues. However, there are a few books that specifically examine the use of the double-cross system. Stephen Barlay in his book *Double Cross: Encounters with Industrial Spies*^[11] tells of numerous cases of betrayal in business, with

serious financial and security consequences. In a contemporary assessment of economic espionage, Colonel Kevin J. Degnan of the U.S. Army explores the impact of the unauthorized acquisition of sensitive information and technology, as well as the countermeasures needed to guard against this subversive activity, in his strategy research report entitled *America's Soft Underbelly: Economic Espionage*.^[12] There are many other treatments of the topic, all of which indicate how the double-cross system extends beyond what might be generally regarded as national security and military operations.

DISRUPTION

Neutralization is not just by destruction but also by paralysis. Although not as dramatic as destruction, it is an effective method nonetheless. Disruption operations play a key part in this counterintelligence strategy. The operational goal of disruption is to inflicting paralysis (usually temporary in nature) on some aspect of the opposition's operation or the entire operation itself. The intent is to cause the opposition to abandon its undertaking in this area and dismantle any ongoing espionage operation—perhaps an active sleeper cell—to avoid detection. Paralysis can be initiated by the agency as a preemptive measure in order to, say, flush out an opposition operative.

Disruption is also classified as actions to frustrate hostile intelligence operations. This includes identifying who the perpetrators are (via record keeping, logs, etc.), expelling operatives and agents, trailing and jailing them for espionage or related crimes, or denying them entry or access to sensitive information or people who hold or access that type of information. Other methods include controlling their movements or observing their activities (e.g., via fixed and mobile surveillance, as well as electronically).^[13]

An example of an offensive counterintelligence that entailed disruption was the case of the ten Russian sleepers in the United States in 2010. Such operatives are termed *illegals* because they took civilian jobs within the community in which they lived and not under official cover at, say, the Russian embassy. The mission of these sleepers was to establish quiet lives in middle-class neighborhoods and work ordinary

jobs as a way of burrowing into American society (i.e., develop a *legend*^[14]). Under this cover they were to cultivate contacts within and among academic circles, business enterprises, and government policy-and decision-makers who had links to a range of Russian strategic interests—computer and communications technology, defense developments, economic matters, and the list goes on.^[15]

As part of Operation Ghost Stories, the Federal Bureau of Investigation conducted a ten-year counterintelligence operation involving these operatives that employed a variety of surveillance methods that gathered data about the spies, their motives, their topics of interest, and their operational methods (as well as other aspects that remain classified). In the end, the FBI exposed the operatives by arresting them before any sensitive information was obtained and provided to Moscow. The FBI then arranged for these sleepers to be swapped for four Russians who were imprisoned for spying for the West.

Arguably, the offensive counterintelligence operation netted a vast amount of data on Russian espionage methods and intents and in the process wasted vast amounts of Russian time and money for an operation that yielded nothing. The Americans then ridded themselves of this nuisance by expelling them, and in the process gained the freedom of four of their agents whose service was valuable to the West.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Agents provocateurs;
- Counterespionage;
- Counterspies;
- Double agents;
- Double-cross;
- Honey pots;
- Illegals;
- Sleepers;

- Sting operations;
- Theory of assumed vulnerability; and
- Traps.

STUDY QUESTIONS

1. Explain how a sting operation works and cite two examples in any counterintelligence context where these have been used.
2. Explain the theory of assumed vulnerability and how this is used in a counterespionage trap.
3. Explain some of the difficulties that might be encountered in doubling an agent. Provide an example to illustrate your points.
4. Using a hypothetical example, describe how a sleeper agent could be employed in the following two contexts: law enforcement and national security.

LEARNING ACTIVITY

Research the use of agents provocateurs. List three examples of their use in history and describe the counterintelligence context (e.g., law enforcement, national security, military, corporate, private, or a combination) in which they were used. What was the outcome of these operations? Were they successful? Why or why not? In hindsight would you suggest another variation to the use of an agent provocateur in these cases? Explain.

NOTES

1. Edward Luttwak, *Coup d'etat: A Practical Handbook* (Great Britain: Allan Lane, The Penguin Press, 1968), 101.
2. Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence* (New York: Knopf, 1974), 211.
3. Marchetti and Marks, *The CIA and the Cult of Intelligence*, 211.
4. See, for example, Henry Prunckun, "It's Your Money They're After: Sting Operations in Consumer Fraud Investigation," *Police Studies* 11, no. 4 (Winter 1988): 190–94; Henry Prunckun, "Sting Operations in Consumer Fraud Investigation," *Journal of California Law Enforcement* 23, no. 1 (1989): 27–32. In the national security context, see Joby Warwick, *The Triple Agent* (New York: Doubleday, 2011), 81.

5. Joby Warwick, *The Triple Agent*.
6. J. C. Masterman, *The Double-Cross System in the War of 1939 to 1945* (Canberra: Australian National University Press, 1972).
7. R. H. Bruce Lockhart, *Memoirs of a British Agent* (London: Putnam, 1932), 323.
8. Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev* (London: Hodder and Stoughton), 74.
9. Andrew and Gordievsky, *KGB*, 72–77.
10. R. H. Bruce Lockhart, *Memoirs of a British Agent*, 324.
11. Stephen Barlay, *Double Cross: Encounters with Industrial Spies* (London: Hamish Hamilton, 1973).
12. Kevin J. Degnan, *America's Soft Underbelly: Economic Espionage* (Carlisle Barracks, PA: U.S. Army War College, 2009).
13. Frederick L. Wettering “Counterintelligence: The Broken Triad” in Christopher Andrew, Richard J. Aldrich and Wesley K. Wark, ed., *Secret Intelligence: A Reader* (London: Routledge, 2009), 291–94.
14. One of the issues pointed out in the subsection entitled “Social Networking” under “Background Investigations” of chapter eight—Defensive Counterintelligence: Personnel Security—was the matter of not being able to effectively hide a covert operative’s background if parts of that background have been exposed on a social networking website. Well, here the opposite is true if an operative is trying to develop a legend. That is, an operative may find it difficult to develop a credible legend if the identity they are using for cover is not a member of a social networking website.
15. Generally speaking, sleeper agents can be left in place for very long periods of time before being activated. One extreme case, although not strictly a sleeper agent, was that of the Japanese intelligence officer Lieutenant Onoda Hiroo who was inserted on Lubang Island in the Philippines during World War II. His instructions were to carry out a guerrilla-style campaign to hinder the Allied invasion and not to surrender. He was advised that, no matter what happened, someone would come back for him. Dutifully he carried out his irregular war on the island and waited. But once Imperial Japan was defeated he was advised by various messages to stand down; however, as he had been advised before his deployment that there might be attempts like these to deceive him into believing he should surrender, he remained in hiding and resisted all attempts to flush him out. He waited thirty years in the mountain jungles before the Japanese government, in 1974, located his former commanding officer and flew him to the island to order the intelligence officer to stand down. Lieutenant Onoda’s case demonstrates the will some sleeper agents can exercise in their mission. See details in Hiroo Onoda (trans. Charles S. Terry), *No Surrender: My Thirty-Year War* (Tokyo: Kodansha International Ltd., 1974).

Chapter 14

Ethics of Counterintelligence

Chapter 14 14 Ethics of Counterintelligence

This topic discusses the ethics of counterintelligence. The chapter covers issues involving:

1. Background;
2. Ethics as moral philosophy;
3. Codes of conduct;
4. Ethics in the context of intelligence;
5. Illustrative dilemmas;
6. Market research;
7. Legally related issues; and
8. Concluding thoughts.

BACKGROUND

Topics such as morality, politicization, principles, codes of conduct, and values are not that common when it comes to textbooks on the practice of counterintelligence. Concepts like these might be more common in a course of study relating to theology rather than intelligence tradecraft. Indeed, such a collection of ethics-based issues is an unlikely feature for the intelligence profession, which, arguably, focuses on analysis that is based on fact and reason.

Nevertheless, counterintelligence practitioners are likely to face a number of dilemmas if they remain in the profession for any length of time. These dilemmas will probably come without warning and arise over routine matters. However, the event, when it does present, will not only test the individual's moral fabric but will also test the individual's sense of what is needed to be done to safeguard the agency and its client, which may be the nation and its people. At the center of many of these ethical dilemmas is the fact that counterintelligence officers are required to act ethically but at the same time engage in what some may

portray as an unethical business—counterspying—with its Orwellian overtones of a secret police state.

Decision making is not an easy task at the best of times but being faced with a choice that will cause a clash between the counterintelligence officer's personal moral views and his or her professional duties and obligations needs to be anticipated. Given the nature of counterintelligence work, it is very likely that such a situation will occur at some time in a person's career.

Countries are founded on high ideals. So, a counterintelligence service should be founded on staff who hold equally high ideals.

ETHICS AS MORAL PHILOSOPHY

Ethics is a term that is often used interchangeably with *moral philosophy*. *Philosophy* is the study of a number of concepts including knowledge, existence, reality, values, and others, and how these concepts can be interpreted, understood and applied to everyday life. *Moral philosophy* is a subfield of the academic study of philosophy that examines questions pertaining to morality.

“While laws are always formal, ethics may be either codified or informal, undocumented principles. [And the interpretation of] . . . ethical standards is likely to be left to the individual.”*

* Hans Born and Aidan Wills, “Beyond the Oxymoron: Exploring Ethics through the Intelligence Cycle,” in *Ethics of Spying: A Reader for the Intelligence Professional*, vol. 2, ed. Jan Goldman (Lanham, MD: Scarecrow Press, 2010), 38.

Morality in this sense includes the examination of such concepts as what is right and what is wrong, what is good and what is bad, what is virtuous and what is sinful, and, of course, what is legal and what constitutes a crime. Certainly there are other examples, but for the purpose of examining counterintelligence practice, a simple examination

of right and wrong may be sufficient to illustrate that there is not going to be a clear or decisive answer to any dilemma a counterintelligence officer may face during his or her career; it may be a matter of exercising balance and maturity in the context of the circumstances that prevail at the time and, above all, what feels like the best thing to do.

CODES OF CONDUCT

It must be said upfront that there are no definitive answers as to what “doing the right thing” means in any given situation. So, if this is the case, then how does a counterintelligence officer consider all the issues that will be running through his or her thoughts when such an event presents itself? One source of advice can be found in a *code of conduct*. A code of conduct is a broad set of guidelines that outline what personnel entrusted to do what counterintelligence officers do and, in doing so, what would be considered by the “reasonable person”^[1] as proper practice or what is fair and reasonable.

In this regard many places of employment outside the intelligence community—both public and private—have implemented codes of conduct for their employees. Many organizations that represent professionals have also instituted codes of conduct for their members. In some cases, holding membership of a professional body is required for government licensing, and therefore this means adhering to the code of conduct is a mandatory requirement for continued registration and practice.

Although not a licensing requirement to practice, in Australia, the body representing the intelligence profession (including counterintelligence officers) is the Australian Institute of Professional Intelligence Officers (APIO). APIO has established a code of conduct that it terms a code of ethics, and these guidelines state that members, who represent all intelligence fields—national security, military, law enforcement, and business intelligence, as well as private intelligence—must strive to:

- continually endeavor to increase professionalism, integrity, respect, and recognition of the profession;
- ensure that duties and responsibilities are carried out with diligence while maintaining the highest degree of professionalism and avoiding all unethical practices;
- fully comply with all applicable laws and regulations in relation to official duties;
- protect intellectual property and confidential information with strict observance of the protocols in this regard; and
- promote and encourage compliance with these standards within the profession and work environment.^[2]

Reading the five elements that comprise this code, it is clear that there are no hard-and-fast directives as to what needs to be done by its members, but instead it presents principles that act to guide members so that, if their actions were ever called into question, the reasonable person might deem those actions fair and reasonable.

ETHICS IN THE CONTEXT OF INTELLIGENCE

Before the issue of ethics within the field of counterintelligence is discussed, it is important to reflect firstly on the wider context in which ethics impacts the work of analytic intelligence. In this regard, it is beneficial to look at how *ethical dilemmas* play out for intelligence analysts.

Generally, intelligence analysts are recruited because of their academic backgrounds in such fields as sociology, criminology, anthropology, psychology, history, political science, and the military sciences. But while they pursued their academic credentials, these analysts were likely to have been taught research ethics—for instance, to take responsibility for the mental, emotional, and physical well-being of those who they research.^[3] So, when they start work with an intelligence agency, a number of questions immediately present, and these concern both research ethics and practice ethics:

- Should intelligence analysts be bound by the same ethical guidelines as their research colleagues in the social and behavioral sciences?
- If so, how does an intelligence analyst reconcile being asked to carry out secret intelligence research where the welfare of those researched is not only removed from the fore of the analyst's considerations but also is likely never featured anywhere in the research methodology?
- Likewise, how do analysts restrain their personal opinions from making their way into formal reports and intelligence assessments?
- How do they guard against presenting their own beliefs in what are objectively reasoned intelligence products?
- How do analysts maintain professional distance and not attempt to influence decision makers through their analytic products, yet still provide advice as to policy options or operational actions?

ILLUSTRATIVE DILEMMAS

Defensive Counterintelligence

As intelligence analysts face many ethics dilemmas in carrying out their duties as secret researchers, so do counterintelligence officers. Whether operating in the area of defensive counterintelligence or offensive counterintelligence, officers and their agents will find most every situation will potentially pose some form of ethical dilemma for them. Here are a selected few of what could be an endless stream of such situations that could conceivably arise:

- Being approached by a new co-worker who is waiting for his security clearance to come through and asks a “favor” to access classified data in the meantime—do you allow him to use your computer logon ID and password?;
- Being asked by a work colleague to cover up a security breach that she committed “inadvertently”; and

- Being told by a close associate about that person's new friend who you know to be a person of interest as you have seen the friend's name on a classified report—do you breach security to tell your associate?
- Does keeping quiet about something one considers illegal make that person an accomplice?
- If one “blows the whistle” on illegal activity within the agency (or its client) how does that person deal with the fear of being accused of being unpatriotic (or, worse, being accused of aiding the opposition)?
- Unethical conduct can also include inadequate training and underequipping of personnel, underresourcing of operations, and underpaying and overworking of personnel.
- Failing to purge intelligence files dating back to the 1950s, 1960s, and 1970s regarding beats and hippies who were the targets of surveillance, but never violated any criminal statutes or posed a threat to civil society other than to hold a different view of the world.

A perennial ethical impasse is whether to give priority to one's conscience or one's career.

Offensive Counterintelligence

As with defensive counterintelligence, a whole set of equally perplexing ethical dilemmas face the officer or agent operating within the field of offensive counterintelligence. To demonstrate this point, here are a couple of illustrative examples of situations in which agency personnel may find themselves:

- A private psychologist is asked to work with a counterintelligence interrogation team to question a suspect. The psychologist, who holds a government license to practice, is asked to assess the suspect and based on that assessment provide advice

as to how to reduce the person's mental health to the point that the suspect will reveal the information required by the interrogators. Should the private psychologist participate?

- Countries A and B have long-standing friendly political and economic ties. Country A makes inquiries of country B about an agent it is dealing with. The agent is controlled by B but does country B expose its agent to country A, even though it is considered an "ally"?
- A counterintelligence officer is tasked by his or her supervisor to devise a sting operation that will net a person suspected of selling classified information.
- A counterintelligence officer becomes aware that one of the agency's case officers is "skimming" money from payments destined for the contract agents being handled by the case officer. When confronted, the case officer thrusts cash into the pocket of the counterintelligence agent to "forget" about it and move on to other issues. Does the counterintelligence officer accept the "gratuity"?
- The agency head is called before a Congressional Committee to answer questions about past intelligence operations, including counterintelligence related activities, that were suspected of being illegal. Should he appear before the Committee or "stonewall"? If he does appear, should he answer truthfully all questions put to him?^[4]

Although these examples only scratch the surface, these dilemmas stand as illustrations of what career counterintelligence personnel may face. Although some of the examples outlined may seem clear and the decision what to do equally clear, the ethical dilemma may seem insignificant when confronting the reality of being in a foreign place, perhaps operating on the edge of legality within that country, and being faced with an aggressive and potentially hostile situation, placed under time and resource pressures. However, back in the office and reflecting on what went on, such reflections may shine a different light on the magnitude of what was decided. The point that needs to be underscored is that sitting in a classroom discussing ethics can be a

different world when compared to the pressures imposed by the reality of working in a dangerous and uncertain environment.

MARKET RESEARCH

Traditionally, the reason for market research is to establish the need for goods and services by consumers. However, in some business circles market research is acknowledged to be a euphemistic reference to electronic and other forms of illegal espionage. But there are an enormous number of open and semi-open sources of information that can supply a research analyst with raw data for conversion into finished, focused intelligence. These data may also be supplemented by information obtained by legal and acceptable covert operations, such as the time-honored art of physical surveillance, if need be.

In some circles the term *security consultant* has been used instead of the more indelicate term *spy*. These types of “consultants” have been viewed by some as mercenaries in suits and ties—that is, some believe they will do almost anything for money. Ethics becomes a secondary consideration in how they operate, if it is thought about at all.*

* See, for instance, Peter Heims, *Countering Industrial Espionage* (Surrey, UK: 20th Century Security Education Ltd, 1982); Jim Hougan, *Spooks: The Haunting of America—the Private Use of Secret Agents* (New York: Morrow, 1978); and Adam Penenberg and Marc Barry, *Spooked: Espionage in Corporate America* (Cambridge, MA: Perseus Publishing, 2000).

Given that there are so many open sources of information, it could be argued that there really is no need to engage in illegal forms of information gathering. In fact, if it becomes known that an agency uses illegal tactics, it will put its own attempts to thwart espionage by others at a disadvantage. It could also lead to both criminal and civil penalties for all participants, including the body corporate and its directors. Recall the ultimate consequences of the 1972 Watergate affair.

Nevertheless, market research plays an important part in making sales and a vital part in a business's counterintelligence effort, thus ensuring that the business continues to make sales. When used in this role a business should closely monitor the information gathering process employed by research analysts. This will help ward off any possible illegal acts that may be perpetrated by overenthusiastic, naïve, egotistical, or careless researchers. Even though competitors may not exercise such restraint, curbing excessive zeal will put an agency in a stronger position to deal with any external espionage threat.

LEGALLY RELATED ISSUES

If the counterintelligence officer is an employee of a government (e.g., military or national security, as well as law enforcement and regulatory or compliance), then it could be said that the agency that employs the officer has a social contract between it (or, more precisely, between the government client the agency represents) and the people it governs. This social contract is usually translated and embodied in a constitution (and/or statutory and common law). It is therefore an undertaking that the officer gives to that social contract, through other legal instruments, such as secrecy agreements, which must be honored. So, it is more than just being clear about what a person opposes, but also what that person stands for. Counterintelligence officers should not only be concerned with dealing with "bad guys" but also dealing with "bad systems."

If the counterintelligence officer is in the employ of a business or is a private individual, then it could be argued that that officer is not discharged from the social contractual arrangements that exist between governments and their populaces. Businesses and private persons also have an obligation to act not only within the law but within the framework of what is fair and reasonable.

CONCLUDING THOUGHTS

Having discussed some of the issues involving the ethics of counterintelligence, it is obligatory to address the equally perplexing dilemma of dealing with issues that purport to be in the public interest

yet go beyond what could be considered a responsible limit to criticism. Former CIA officer Philip Agee, who exposed classified information, arguably undermined the intelligence service of the United States (and consequently the Five-Eyes allies) under the guise of exposing injustices. [5] It is the view of this writer that, without a robust intelligence service, detractors of the craft of intelligence, like Agee, would not have been able to criticize the system as the system exists to allow such freedoms.

Another thought is that of perspective. For instance, it could be said that the most unethical position in which to place yourself, your agency, or your nation is in the position where you/they lose. This may sound trite but righteous stands that are blind to the reality of intelligence operations, and in particular counterintelligence operations, deny the fact that these operations will always remain a feature of the world of *realpolitik*. To consider otherwise is to show the same naïveté U.S. secretary of state Henry L. Stimson displayed in 1929 when he advanced the now often-cited dictum that “gentlemen do not read each other’s mail.” [6] That is, when Stimson learned of the existence of Herbert O. Yardley’s “Black Chamber,” he rejected the argument that the ends justified covert code-breaking ops. Stimson strongly disapproved of Yardley’s clandestine activity, regarding it as a low dirty business that violated the principle of mutual trust upon which, in Stimson’s view, foreign policy should be based. Stimson then shut down Yardley’s Black Chamber. Since, history has shown the fate America suffered in the years leading up to the Second World War because of Stimson’s morally based but politically ill-conceived decision. It could be said Stimson lost perspective.

It has been said that “idealism and realism are at opposite ends of the scale when defining ethical intelligence,”* but shouldn’t practitioners seek to arrive at an ethical way of “doing intelligence” that is not only seen as striving for the ideal, yet is realistic and achieves operational goals?

* Jenifer Morgan Jones, “Is Ethical Intelligence a Contradiction in Terms?” in *Ethics of Spying: A Reader for the Intelligence Professional*, vol. 2, ed. Jan Goldman (Lanham, MD: Scarecrow Press, 2006), 25.

The post–Cold War global community faces threats different from those of the past. There are nontraditional challenges for which the state-centric paradigm no longer applies (e.g., al-Qaeda). Free societies face threats from weak and corrupt governments, rogue states, substate and transstate actors, as well as criminal, radical ethnic, racial, and religious groups, and ultra-right-wing political groups—all openly defying international control.

A few examples of such threats materialized in the terrorist events of September 11, 2001, as well as the bombings in Bali, Indonesia, on October 12, 2002, Madrid on March 11, 2004, and London on July 7, 2005; the question that presents is: “do secret operations corrupt secretly”? A balanced reply might be: “can free societies tolerate groups that, if they came to power, would destroy the freedoms that tolerated them?”

Moira Rayner stated that: “Public faith in the ideals of ‘justice’ is perhaps the most fundamental sign that a society is truly civilized.”^[7] However, hero of the American Revolutionary War, and one of the nation’s first spies, Nathan Hale said: “Any kind of service necessary to the public good becomes honorable by being necessary.”^[8] But the issue lies in deciding what is necessary for the public good, especially when that decision falls to an officer or agent at the operational end of the decision-making chain where the interpretation of “any kind of service” may be seen as permissible for the public good, when it may not be.

Perhaps what is needed is training not only in counterintelligence tradecraft, but also in how to deal with some of the ethical issues that are likely to arise for officers engaged in counterintelligence work. This approach may empower officers by providing them with moral signposts that can guide them to make quick decisions that will withstand public scrutiny should the event come to light.

Nevertheless, these guidelines may best originate from public opinion that exists at the time because what may be viewed as “wrong” changes with time. Take, for instance, the firebombing of Japan in the Second World War. The public view at the time was largely accepting of this tactic. But, at the time of this writing, the idea of mass destruction of highly populated cities is far less accepted, if tolerated at all (in fact, even minor collateral damage is met with public outrage). [9]

In conclusion, it is not necessarily a case of having “bad apples” in the barrel—of being deceitful and untruthful. There are many cases in which “the golden apples” amongst an agency’s staff do the wrong thing. This is known as *noble cause corruption*—where people do the wrong thing but for the right reason and where the ends are believed to justify the means. But this could be regarded as a person becoming what they oppose.

Nonetheless, there is a balance to be struck, and this needs maturity and wisdom to know what is required for any given situation, and to never be placed in a situation where you lose sight of the “big picture” for the narrower questions. This too would equally be unethical. So, it is worth repeating—the most unethical position in which to place yourself, your agency, or your nation is the position where losing would be judged by history as being as unethical as if you had acted unethically. This is not an easy decision, and one with no clear answer. It is likely that no one will know what to do until they face the question in a field situation, perhaps “under fire.” Until a practitioner experiences the gravity of such a situation and the weight such decision making has (i.e., the consequences of acting on those factors, or not acting on them), this thinking is merely an academic exercise. Regardless, there is surety in the knowledge that those who practice counterintelligence will one day face such a dilemma. When confronted, their preparation for such decision making will then be as important as the preparation they undertook for the more technical side of the profession.

REVIEW OF KEY WORDS AND PHRASES

The key words and phrases associated with this chapter are listed below. Demonstrate your understanding of each by writing a short definition or explanation in one or two sentences.

- Code of conduct;
- Ethical dilemma;
- Ethics;
- Moral philosophy; and
- Philosophy.

STUDY QUESTIONS

1. Explain what your understanding is of a “reasonable person.”
2. Explain what the concept of being “fair and reasonable” means.
3. Explain the term *realpolitik*.
4. Describe *noble cause corruption*.

LEARNING ACTIVITY

Suppose that you are a police officer tasked with a group of other officers to execute an arrest warrant for an alleged narcotics dealer. The raid takes place in an urban area of your state or in your provincial capital. You and your team execute the warrant by bursting into the specified house, and, as you do, shots are fired from the alleged drug dealer. One of your fellow officers is hit by the spray of bullets and is killed. The drug dealer instantly surrenders and is taken into custody. However, in the immediate aftermath of the shooting, you hear some of your fellow officers in the raid whispering that the information that formed the basis of the warrant was based on false information from a fictitious informant. You know that, if this information is made known, there is an almost certainty that the courts will dismiss all charges against the accused, including the murder charge for the dead officer.

Explain what you would do if you found yourself in this situation. For instance, would you withhold this information from investigators? Why, or why not? If you revealed this information, what would this

mean for your career? How do you think other officers would view you if you spoke up? How would the thoughts and opinions of the dead officer's family weigh on your mind? If you withheld this information, are you not guilty of a felony for covering up a serious crime? How could you continue to work with officers who you know have committed such a crime and, in doing so, caused a fellow officer to die?

NOTES

1. The term *reasonable person* is one used in common law countries as a standard against which an individual's actions can be judged.
2. Australian Institute of Professional Intelligence Officers, Inc., *Intelligence Officer Code of Ethics*, www.aipio.asn.au/files/file/CODE_ETHICS.pdf (accessed April 25, 2009).
3. Max Futrell and Cliff Roberson, *An Introduction to Criminal Justice Research* (Springfield, IL: Charles C. Thomas, 1988), 201–4.
4. For a discussion of how an agency head grappled with this dilemma see William Colby with Peter Forbath, *Honorable Men: My Life in the CIA* (New York: Simon & Schuster, 1978), 7–21. Colby's reasoning was to assist the Congressional inquiry as he saw his duty to uphold and defend the U.S. Constitution, which Congress was exercising its right and duty in conducting the inquiry. Others have argued that his loyalty should have been to the U.S. president (at the time it was Gerald Ford) and that he should not have cooperated. Colby was subsequently criticized for taking the position he did and President Ford terminated him as the director of Central Intelligence. Clearly, Colby put his conscience before his career and willingly accepted the price this levied—an end to his thirty-year intelligence career. However, vindication came from President Ford's secretary of state, Dr. Henry Kissinger. It was reported that Kissinger told Colby before he left office that Colby had done the right thing (p. 19).
5. Chapman Pincher, *Traitors: The Labyrinths of Treason* (London: Sedgwick and Jackson, 1987), 47, 167, 174.
6. As Michael Herman points out, "Note, however, that the actual words were [Stimson's] rationalization seventeen years later: see correspondence in *Intelligence and National Security* 2, no. 4 (October 1987)." See Michael Herman, "Ethics and Intelligence after September 2001," in *Ethics of Spying: A Reader for the Intelligence Professional*, ed. Jan Goldman, vol. 2 (Lanham, MD: Scarecrow Press, 2006) 119.
7. Moira Rayner, with assistance from Jenny Lee, *Rooting Democracy: Growing the Society We Want* (St. Leonards, NSW: Allen and Unwin, 1997), 63.
8. James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (Washington, DC: Potomac Books), 34.
9. Paul Ham, *Hiroshima Nagasaki* (Sydney: HarperCollins, 2011).

Appendix A: Sample Personal History Statement

Appendix A Sample Personal History Statement

This is an example of what a personal history statement might look like and the types of information that it seeks from a job applicant. The purpose is to systematically elicit background information about the person and their life in relation to the skills, abilities, and knowledge that the job calls for. The applicant's curriculum vitae usually contains evidence of the latter while the personal history statement contains information regarding the former.

The personal history statement shows the types of questions that are likely to provide information that a counterintelligence investigator can use to test the honesty and integrity of the applicant. The personal history statement does this by providing a basis for checking gaps and contradictions as well as embellishments of the truth.

This sample personal history statement is provided as an example only. In your jurisdiction there may be federal and/or state/provincial laws that regulate the types of questions an employment application can ask. Anyone contemplating using such an instrument to collect data should first seek legal advice. The information presented here is for illustrative purposes only and is not to be construed as legal advice.

APPLICATION REGARDING POSSIBLE EMPLOYMENT

[Insert the agency's name]

[Insert the agency's address]

Position applied for: _____

Personal Details

1. Name: _____

First	Middle	Last
-------	--------	------

(a) Previous name(s) used and dates:

— Residential address:

— _____

— _____

2. Home telephone: () _____

3. Date of birth: _____

4. Place of birth: _____

5. Marital status: _____

6. Driver's license: Yes / No

(a) State of issue: _____

(b) License number: _____

(c) License type/class: _____

7. If successful with this application, on what date would you be available to commence work?

— 8. List the names, addresses, and telephone numbers of two references who are not related to you.

You may attach photocopies of your curriculum vitae, academic credentials, or any other supporting documents that you feel may be helpful in considering your application. Use additional pages if there is insufficient space to answer any of the following questions.

Employment History

9. Are you currently employed? List employer:

— Who can we contact at this business for a work report?
Telephone: () _____

10. List your employment history, starting with current or last job and working backward. Do not omit any period and include volunteer activities if applicable. A break in employment is to be explained. Please include the following details:

- (a) Occupation
- (b) Employer
- (c) Employer's address
- (d) Starting date
- (e) Name of your supervisor at the time
- (f) Termination date

11. Reason for leaving

12. In the last five (5) years have you ever been fired from a job?

Yes / No

13. In the last 5 years have you ever resigned from a job after being notified that you would be fired? Yes / No

If you answered yes to either 12 or 13, please explain:

14. Have you ever been convicted of a felony? Yes / No

15. Have you ever been convicted of an offense involving violence?

Yes / No

16. Are you currently on probation or parole? Yes / No

If yes to 14, 15, or 16, please explain:

Education

17. List your educational history, including the following details:

- (a) Name of school/college/university
- (b) Years completed
- (c) Highest certificate/diploma/degree awarded
- (d) Description of course of study

18. Specialized training, apprenticeship, skills, or other courses if applicable.

Military Service

19. Have you ever served on active duty in a branch of the armed forces? Yes / No

If yes, please state:

- (a) which nation _____
- (b) branch of service _____
- (c) dates of active duty _____
- (d) highest rank held _____
- (e) type of discharge _____
- (f) date of discharge _____

Special Skills and Qualifications

20. Summarize any special skills and/or qualifications you may have acquired through employment, study, or other experiences. Include membership in any organizations and any professional associations.

Agreement

I certify that the answers given herein are true and complete to the best of my knowledge and belief, and that I have made them in good faith.

I authorize investigation of all matters contained in this application for employment as may be necessary in arriving at an employment

decision, including a criminal record check with the relevant police authority.

In the event of employment, I understand that any false or misleading information given in my application, its attachments, or interview(s) that I participate in (whether in person or via the telephone) may result in dismissal. I also understand that permanent appointment will be subject to an initial _____ month probationary period.

_____	_____
Signature of Applicant	Date

Appendix B: Sample Nondisclosure Agreement

Appendix B Sample Nondisclosure Agreement

This sample form is presented for illustrative purposes only and is not to be construed as legal advice.

Agency Name

Agency Address

DECLARATION OF CONFIDENTIALITY

I,

(insert full name)
of

(insert address)

in the State [or Province] of [insert name of state /province], do solemnly and sincerely declare, that, except in the course of my official duty with [insert the name of the agency], I will not communicate or divulge, directly or indirectly, information relating to any matter that comes to my attention as a consequence of my employment, either now, or at any time in the future.

Signature: _____

Declared at _____
(insert place)

this _____ day of _____ 20

Before me: _____

Justice of the Peace

Appendix C: Selected Summary of Audio Surveillance Devices

Appendix C Selected Summary of Audio Surveillance Devices

The following list of selected devices illustrates how common electronic components, which are available from local electronic and science stores or online suppliers, can be used in audio surveillance. The devices and components are itemized with a brief description of their application. They do not represent all devices or electronic components that can be used in audio surveillance but they are representative and demonstrate what is available on the over-the-counter market and how they are employed in practice.

MICROPHONES

Dynamic and Crystal

Microphones collect sound energy and two commonly used types are dynamic and crystal, and these are used for general purpose audio work. No electric current is required to use these. They are available in two directional patterns: omni- and cardio-.

Condenser

A third type of microphone is a condenser. These are battery powered and are usually more sensitive than dynamic and crystal microphones but are usually available only in an omni-directional pattern.

Tube Microphones

Tube microphones have a special function. Their main feature is a hollow tube (miniature) fixed over a microphone element. They are designed to be inserted through walls, floors, and so on.

Stethoscope Microphones

A stethoscope microphone is another specialized microphone with its chief purpose being listening through solid objects (e.g., floors, ceilings, and walls).

Contact Microphones

Contact microphones have the same function as stethoscope microphones.

Spike Microphones

Spike microphones have the same purpose as contact and stethoscope microphones; however, this device is distinguished by a spike-shaped electronic “pick-up.” The pick-up works in the same fashion as a phonograph needle.

Shotgun Microphones

Shotgun microphones (sometimes termed *rifle mics*) are yet another special function microphone that utilizes a cluster of varying length tubes to achieve a directional pattern for listening. These are designed for overhearing conversations across large, open areas.

Parabolic Reflectors

Parabolic reflectors are a “dish-type” arrangement around a microphone to give directionality. They are similar in purpose to the shotgun microphone; however, the tubes of the shotgun are replaced with a parabolic collecting reflector.

Induction Coils

These are not microphones at all, but an electronic device that is used in place of a microphone to intercept targeted audio signals via electrical induction; so, they act like microphones. They are chiefly used in telephone surveillance. They are usually only able to be detected by physical search.

ANCILLARY DEVICES

High-Gain Amplifiers

These are used to boost audio signals received from a microphone. They can be employed with contact and spike microphones and induction coils.

Frequency Equalizers

Equalizers are used to eliminate background noise and other sounds that interfere with the target conversation, for example, in electronic intercepts.

Remote Control Devices

These are typically a transmitter/receiver combination similar to those used by model hobbyists. They are used to switch surveillance equipment on and off from a distance.

Voice Operated Relay

A voice operated relay (VOX) is used to start and stop, say, a digital audio recorder. Its primary advantage is to conserve digital memory (and tape, when tape recorders were used) as it only records active conversations, not periods of silence.

Drop-Out-Relay

This device has the same purpose as a VOX; however, it is used to turn a recorder on or off when it is connected to a telephone line. That is, when the handset of a landline is removed from the hook, the relay is “tripped,” starting the recorder. When the handset is replaced, it turns the recorder off.

WIRELESS MICROPHONES

Varieties

There are numerous varieties of what are termed *miniature transmitters* and these range from the most sophisticated down to the very basic home-made, or store-shelf-purchased, devices.

Range

The transmission range of these electronic devices depends on the sophistication of the unit’s circuitry, the placement of the transmitter (i.e., interference may be caused by buildings, nearby steel structures, etc. that shorten range), and to some extent the sensitivity of the communications receiver.

Power Supply

Some miniature transmitting devices use their own energy supplied via batteries. Others utilize the power of, say, telephone lines or even the AC power in the building in which it is secreted.

Frequency

Commercially purchased and “home-made” transmitters are reported to operate in the area of the VHF part of the radio spectrum—that is, between 25 MHz to around 512 MHz. This part of the spectrum

includes the commercial FM broadcast band that lies between 88 MHz and 108 MHz.

TRANSMITTER REPEATERS

A repeater is used in conjunction with a miniature transmitter that is installed in the target premises. The low-power, miniature transmitter broadcasts its signal to the secreted repeater nearby. The repeater then boosts the signal strength and rebroadcasts the intercepted conversation on a different frequency so that a monitoring post can intercept and record the conversation for analysis.

HOMING TRANSMITTERS

These devices are fastened to, or secreted in, the target motor vehicle. The purpose is to declare the location of the vehicle to a surveillant who is tailing at a safe distance. These devices can emit either an audio tone or series of beeps. Tracking is accomplished via radio direction finding and signal strength devices. The target vehicle can be more easily located by the employment of two tracking units to triangulate the transmitter's position. Some simply send data via a global positioning system (GPS).

LASER SURVEILLANCE

The primary purpose of laser surveillance is to intercept audio communication. The device is sophisticated and operates by detecting minute vibrations produced on a room's window caused as a result of internal audio. The device consists of a laser, which projects a beam onto the target window, and a telescope/decoder, which detects the vibrations and translates them into sound waves (audio).

LANDLINE TELEPHONES

Devices

Direct Tap

A direct “tap” is acknowledged as the easiest method to intercept a telephone conversation on a landline telephone as power is derived from the telephone line to operate the device. The actual tap is effected by connection of a recorder (via, perhaps, a VOX), a transmitter, or headphones for live monitoring.

Near Direct Taps

These types of taps utilize induction coils. The installation can be configured to include headphones (live surveillance), a digital recorder (VOX), or a miniature transmitter (and possible repeater).

Bypass Wiring

This operation involves the shorting-out of the landline telephone’s hook switch (for a nondigital unit) using a resistor, a capacitor, a silicon-controlled rectifier, or a tone-activated latching switch (also called an *infinity transmitter*). In this configuration, the targeted instrument acts as a hardwired microphone. Room conversations around the telephone can be monitored anywhere down the line. It cannot be used to monitor telephone conversations, only room audio when the handset is on the hook.

Ancillary Devices

Capacitors

These small electronic components are used to match the impedance of a surveillance device (e.g., headphones) to a landline telephone (nondigital), thus reducing the risk of a technical countermeasures sweep that might otherwise indicate a “load” on the line.

Transformers

These components perform the same function as capacitors.

Appendix D: Specimen Chain-of-Custody Record

Appendix D Specimen Chain-of-Custody Record

This sample form is presented for illustrative purposes only and is not to be construed as legal advice.

CHAIN-OF-CUSTODY RECORD

I the undersigned state that I took possession of the documents listed below on the date and time specified. Transfer of these documents was made as indicated. Further, while in my possession the documents were secure and inaccessible to unauthorized persons.

DOCUMENTS

CLASSIFICATION

1) INITIAL POSSESSION BY: _____

Time:

Date:

Signature:

2) TRANSFERRED TO:

Time:

Date:

Signature:

3) TRANSFERRED TO: _____

Time:

Date:

Signature:

Index

5Is model, [1.1-1.2](#)

Abbottabad, Pakistan, [1](#)

access controls

cards, [1.1-1.2](#)

intruder detection systems, [1.1-1.2](#)

keys, [1.1-1.2](#)

technological improvements, [1.1-1.2](#)

types of sensors, [1](#)

Afghanistan, [1](#) , [2](#) , [3](#) , [4](#) , [5](#) , [6](#) , [7](#)

agency, term defined, [1.1-1.2](#) , [2](#)

agent, term defined, [1](#)

all hazards, term defined, [1](#)

al-Qaeda, [1](#) , [2](#) , [3](#) , [4](#)

Ames, Aldrich, [1.1-1.2](#) , [2](#) , [3](#) , [4](#) , [5](#)

Annapolis, [1](#)

assumed vulnerability, theory of, [1](#)

Australia, [1](#) , [2](#) , [3.1-3.2](#) , [4](#) , [5](#) , [6](#) , [7.1-7.2](#) , [8](#) , [9](#) , [10](#) , [11](#) , [12](#) , [13](#) , [14](#) , [15](#) ,
[16](#)

background investigations, [1.1-1.2](#)

barrier controls, [1.1-1.2](#)

Belgian troops in WWII, [1](#)

Bernstein, Carl, [1](#)

See also Deep Throat *See also* Felt, W. Mark *See also* Woodward, Bob

bin Laden, Osama, [1](#)

black bag operations, [1](#) , [2](#) , [3](#) , [4](#) , [5](#)

See also covert operations *See also* covert operatives

black chamber, [1](#)

blackmail, [1](#) , [2](#) , [3](#) , [4](#) , [5](#) , [6](#)

black operations, [1](#) , [2.1-2.2](#) , [3](#) , [4](#)

See also black bag operations
bodyguards See close personal protection
Bond, James, 1, 2
Britain, 1.1-1.2, 2, 3
See also British *See also* United Kingdom
British, 1.1-1.2, 2, 3.1-3.2, 4, 5, 6, 7.1-7.2, 8.1-8.2, 9.1-9.2
See also Britain *See also* United Kingdom
bugs, 1, 2, 3, 4
See also debugging *See also* listening devices *See also* wiretaps

camouflage
Australian study into, 1
businesses and companies, 1.1-1.2
environmental, 1.1-1.2
purpose of, 1.1-1.2
Canada, 1
case officer, term defined 2.18 2n3
CCTV, 1, 2, 3, 4, 5.1-5.2, 6, 7
detection, 1.1-1.2
image quality, 1.1-1.2
monitoring, 1.1-1.2
recognition, 1.1-1.2
signage, 1.1-1.2
chain of custody, 1, 2, 3, 4
chain of evidence *See* chain of custody
citizens' band (CB) radios, 1
classification, five basic levels, 1.1-1.2
closed circuit television *See* CCTV
close personal protection, 1, 2
code names, 1.1-1.2
cognition, role of in deception, 1.1-1.2
Collins, Patrick, 1
commercial cover, 1, 2
See also non-official cover
communications security
cellular phones, 1.1-1.2

cordless phones, [1.1-1.2](#)
defined, [1](#)
encrypted systems, [1.1-1.2](#), [2](#)
facsimile machines, [1.1-1.2](#)
radios, scanners, [1](#), [2](#)
radios, two-way, [1](#), [2](#), [3.1-3.2](#), [4](#), [5](#)
telephone wiring, [1.1-1.2](#)
computer physical security, [1.1-1.2](#)
top eleven countermeasures, [1.1-1.2](#)
video display units, [1.1-1.2](#)
COMSEC See communications security
confirmation by call back, [1](#)
counterespionage
agents provocateurs, [1.1-1.2](#)
counterspies, [1.1-1.2](#)
defined, [1.1-1.2](#)
disruption, [1.1-1.2](#)
double agents, [1.1-1.2](#)
double-crosses, [1.1-1.2](#)
legend, use of, [1](#), [2](#)
sting operations, [1](#), [2](#), [3](#)
traps, [1.1-1.2](#)
counterintelligence
anatomy of, [1.1-1.2](#)
atmosphere, defined, [1](#)
axioms, [1.1-1.2](#)
business, [1.1-1.2](#)
competitor, [1.1-1.2](#)
corporate, [1.1-1.2](#)
counterespionage, [1.1-1.2](#), [2.1-2.2](#)
ethics, [1.1-1.2](#)
event of concern defined, [1](#)
function of, [1.1-1.2](#)
fusion of security, law enforcement, and intelligence, [1.1-1.2](#)
ghost army, [1](#), [2.1-2.2](#)
investigation, [1.1-1.2](#)

law enforcement, [1.1-1.2](#)
logical model, [1](#)
military, [1.1-1.2](#)
national security, [1.1-1.2](#)
offensive, deception, [1.1-1.2](#)
offensive, detection, [1.1-1.2](#)
offensive, neutralization, [1.1-1.2](#)
preinvestigation, [1.1-1.2](#)
principles of defensive counterintelligence, [1.1-1.2](#)
principles of offensive counterintelligence, [1.1-1.2](#)
private, [1.1-1.2](#), [2](#)
taxonomy of, [1.1-1.2](#)
tenets of defensive counterintelligence, [1.1-1.2](#)
theory, [1.1-1.2](#)
typology of, [1.1-1.2](#)
counterreconnaissance, [1](#), [2](#)
cover, term defined, [1](#), [2](#), [3](#)
cover story See pretext
covert operations, [1](#), [2.1-2.2](#), [3](#), [4](#), [5](#)
covert operatives, [1](#), [2](#), [3](#)
CPTED, [1.1-1.2](#)
crime prevention through environmental design See CPTED
curtains and reflective film, [1.1-1.2](#)
cyber weapons, [1](#)

Davis, Raymond, [1.1-1.2](#)
de-bugging, [1](#)
decoys, [1.1-1.2](#)
Deep Throat, [1](#), [2.1-2.2](#)
See also Felt, W. Mark
Deutch, John, [1.1-1.2](#)
dignitary protection, [1](#)
diplomatic cover, [1](#)
documents
carriage of, [1.1-1.2](#)
disposal, [1](#)

reproduction, [1.1-1.2](#)

safeguards, [1.1-1.2](#)

storage, [1.1-1.2](#)

doors

external, [1.1-1.2](#)

internal, [1.1-1.2](#)

Downer, Alexander, [1](#)

drones, [1](#), [2](#)

dummy agent, [1](#), [2](#)

dummy cameras, [1](#), [2](#)

dummy companies, [1](#)

dummy paratroops, [1](#)

Dumpster diving, [1](#), [2](#)

Duntroon, [1](#)

electronic countermeasures See technical surveillance countermeasures

Elias, Ann, [1](#)

Ellsberg, Daniel, [1](#), [2](#), [3](#)

entry and exit controls, [1.1-1.2](#)

environmental scanning, [1](#), [2](#)

espionage, term defined, [1](#)

ethics

codes of conduct, [1.1-1.2](#)

context of intelligence, [1.1-1.2](#)

illustrative dilemmas, [1.1-1.2](#), [2](#)

legal issues, [1.1-1.2](#)

moral philosophy, [1.1-1.2](#)

noble cause corruption, [1](#)

relation to market research, [1.1-1.2](#)

evasion, [1](#), [2](#)

fake IDs See identity, fake

Felt, W. Mark, [1.1-1.2](#)

See also Deep Throat

field officer, term defined, [1](#)

five-eyes, [1](#), [2](#), [3.1-3.2](#)

Flemming, Ian, [1.1-1.2](#)
foreign intelligence service See opposition
French government, [1.1-1.2](#)
French intelligence, [1.1-1.2](#)
French North Africa, [1](#)
French troops in WWII, [1](#)

Gaines, William C., [1](#)
glass-break detectors, [1.1-1.2](#)
Greenpeace, [1](#)
guarding services, [1.1-1.2](#)

Hale, Nathan, [1.1-1.2](#), [2](#)
handler
defined, [1](#)
role and skills, [1](#)
See also case officer
Hanssen, Robert, [1](#), [2](#)
hazard, term defined, [1](#)
herkos odonton, [1.1-1.2](#)
Hewlett-Packard, [1](#)
Hunt, E. Howard, [1.1-1.2](#), [2](#)
See also Deep Throat *See also* Ellsberg, Daniel *See also* Liddy, G. Gordon
See also plumbers *See also* Watergate

identity, fake, [1](#), [2](#), [3](#), [4](#)
identity theft See identity, fake
illegal entry, [1.1-1.2](#)
information
accounting practices, [1.1-1.2](#)
advertisements, [1.1-1.2](#)
clear desk policy, [1.1-1.2](#)
common law protection, [1.1-1.2](#)
compartmentalization of, [1.1-1.2](#)
freedom of information, [1](#), [2](#), [3.1-3.2](#)
handling sensitive, [1.1-1.2](#)

legislative protection, [1.1-1.2](#)
meetings and conferences, [1.1-1.2](#)
oral conversations, [1.1-1.2](#)
reverse engineering, [1.1-1.2](#)
trademarks, patents and copyright, [1.1-1.2](#)
types requiring protection, [1.1-1.2](#)
waste disposal, [1.1-1.2](#)
information security, [1.1-1.2](#)
classifying data, [1.1-1.2](#)
defined, [1.1-1.2](#)
intelligence
customers defined, [1.1-1.2](#), 2
defined, [1.1-1.2](#)
insight, 1
positive collection, 1
reduce uncertainty, 1
research and analysis, [1.1-1.2](#)
role of security, [1.1-1.2](#)
secondary data, use of, 1
signals, 1
traffic analysis, 1
investigation
computer forensics, [1.1-1.2](#)
crime scene, [1.1-1.2](#)
evidence search, [1.1-1.2](#)
interrogations, [1.1-1.2](#)
interviews, [1.1-1.2](#)
physical evidence, [1.1-1.2](#)
recording the scene, [1.1-1.2](#)
surveillance, [1.1-1.2](#)
undercover, [1.1-1.2](#)
Italian invasion in WWII, [1.1-1.2](#)

Japanese intelligence in WWII, 1

Lahore, Pakistan, [1.1-1.2](#), 2

Liddy, G. Gordon, [1](#)
listening devices, [1](#), [2](#), [3](#)
Lonetree, Clayton, [1](#)

Manning, Bradley, [1.1-1.2](#), [2](#), [3](#)
See also WikiLeaks
“the man who never was,” [1.1-1.2](#)
Martin, William (captain, acting major), [1.1-1.2](#)
McNamara, Robert S., [1](#)
MI6, [1.1-1.2](#), [2](#), [3](#)
Michael, Glyndwr, [1.1-1.2](#)
Mururoa Atoll, [1](#)

need-to-be-there basis, [1](#)
need-to-know principle, [1](#), [2](#), [3](#), [4](#), [5](#), [6.1-6.2](#), [7](#), [8](#)
need-to-share principle See need-to-know principle
News of the World, [1.1-1.2](#)
New Zealand, [1](#), [2.1-2.2](#), [3.1-3.2](#)
Nixon, Richard, [1](#), [2](#), [3](#)
nondisclosure agreements, [1.1-1.2](#), [2](#), [3](#)
non-official cover, [1](#), [2](#)
defined, [1.1-1.2](#)
role, [1](#)

observation, term defined, [1](#), [2.1-2.2](#)
operation ghost stories, [1](#)
operation mincemeat, [1](#)
operations officer See case officer
opposing forces, [1.1-1.2](#)
See also opposition
opposition, term defined, [1.1-1.2](#), [2.1-2.2](#)

Pakistan, [1](#), [2](#), [3](#), [4](#)
paper tripping See identity, fake
passports, fake, [1](#)
Pentagon Papers, [1.1-1.2](#), [2](#), [3](#)

perimeter beams, [1.1-1.2](#)
perimeter fencing, [1.1-1.2](#)
perimeter towers, [1.1-1.2](#)
perpetrator, defined, [1](#)
personnel security, [1.1-1.2](#)
central pillar of, [1.1-1.2](#)
contact reporting, [1.1-1.2](#)
employees' obligations, [1.1-1.2](#)
fraternization, [1.1-1.2](#)
hiring practices, [1.1-1.2](#)
infiltration, [1.1-1.2](#)
positions requiring clearance, [1.1-1.2](#)
protecting conversations, [1.1-1.2](#)
recognizing physical surveillance, [1.1-1.2](#)
screening personnel, [1.1-1.2](#)
simple personal protective measures, [1.1-1.2](#)
placebo cameras, [1](#) , [2](#)
plausible denial, [1](#)
plumbers, [1.1-1.2](#)
pocket litter, [1](#)
power of arrest, [1](#) , [2](#) , [3](#)
Powers, Gary Francis, [1](#)
PPRR (prevention, preparation, response, and recovery), [1](#) , [2](#) , [3](#) , [4.1-4.2](#)
pretext, [1](#) , [2](#) , [3.1-3.2](#) , [4](#) , [5.1-5.2](#)
private detective See private investigator
private inquiry agent See private investigator
private intelligence agency/contractor, [1](#) , [2](#) , [3](#)
private investigator, [1](#) , [2](#) , [3](#) , [4](#) , [5](#) , [6](#) , [7](#) , [8](#) , [9](#) , [10](#) , [11.1-11.2](#) , [12](#)
psychoanalytic profile, [1](#)

Radio Shack, [1](#)
radio signals, fictitious, [1](#)
Rainbow Warrior, [1](#)
reconnaissance, [1](#) , [2](#) , [3](#) , [4](#) , [5](#) , [6](#) , [7](#) , [8](#) , [9](#) , [10](#) , [11](#)
contrast with observation 2.17
responsibility-to-provide principle See need-to-know principle

right-to-know principle See need-to-know principle

risk, term defined, [1](#)

risk analysis, [1.1-1.2](#)

safe house, [1](#), [2.1-2.2](#), [3](#)

safes, [1.1-1.2](#)

Sandhurst, [1](#)

Sawers, Sir (Robert) John, [1](#), [2](#)

SCIF, [1.1-1.2](#)

Scotland Yard, [1](#)

secondary data, use of in intelligence, [1](#)

secure containment, [1.1-1.2](#)

security lighting, [1.1-1.2](#)

sensitive compartmentalized information facility See SCIF

sensor lights, [1.1-1.2](#)

sleepers, [1](#), [2](#), [3](#), [4.1-4.2](#), [5](#)

Sony PlayStation, [1.1-1.2](#), [2](#)

Spanish secret police in WWII, [1](#)

special activities See black operations

speed styles, [1.1-1.2](#)

spy and spying, defined, [1](#)

spy-for-hire See private investigator

stakeout, term defined, [1](#)

static surveillance, term defined, [1](#)

strong rooms and keeps, [1.1-1.2](#)

sub rosa, [1.1-1.2](#)

Taliban, [1.1-1.2](#), [2.1-2.2](#), [3](#)

tangle-foot wire, [1.1-1.2](#)

target, term explained, [1](#), [2](#)

technical surveillance countermeasures, [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7.1-7.2](#), [8.1-8.2](#), [9](#)

threat, logical model, [1.1-1.2](#)

threat-agent, [1](#), [2.1-2.2](#)

threat analysis, [1.1-1.2](#)

threat communities, [1](#), [2.1-2.2](#)

threat profile, [1](#), [2](#)

traffic analysis, [1](#)

traffic light protocol, [1](#)

U2, [1](#)

Ulasewicz, Tony, [1](#)

United Kingdom, [1](#), [2](#), [3](#)

See also Britain *See also* British

unmanned aerial vehicles See drones

vaults, [1](#)

von Clausewitz, Carl, [1](#), [2](#)

vulnerability analysis, [1.1-1.2](#)

vulnerability defined, [1](#)

Walsh, Patrick F., [1](#)

Washington, George, [1](#)

Watergate, [1.1-1.2](#), [2.1-2.2](#), [3](#), [4](#), [5](#), [6](#)

See also Deep Throat *See also* Ellsberg, Daniel *See also* Liddy, G. Gordon

See also plumbers *See also* Watergate

Welch, Richard, [1.1-1.2](#), [2](#)

West Point, [1](#)

White House plumbers See plumbers

WikiLeaks, [1.1-1.2](#), [2.1-2.2](#), [3](#), [4](#)

window controls, [1.1-1.2](#)

wiretaps, [1](#), [2](#), [3](#), [4.1-4.2](#)

Woodward, Bob, [1.1-1.2](#)

See also Bernstein, Carl *See also* Deep Throat *See also* Felt, W. Mark

Yardley, Herbert O., [1](#)

About the Author

Dr. Hank Prunckun, BS, MSocSc, PhD, is associate professor of intelligence analysis at the Australian Graduate School of Policing and Security, Charles Sturt University, Sydney. He specializes in the study of transnational crime—espionage, terrorism, and drugs and arms trafficking, as well as cybercrime. He is the author of numerous reviews, articles, chapters, and books, including: *Handbook of Scientific Methods of Inquiry for Intelligence Analysis* (Scarecrow Press, 2010); *Shadow of Death: An Analytic Bibliography on Political Violence, Terrorism, and Low-Intensity Conflict* (Scarecrow Press, 1995); *Special Access Required: A Practitioner's Guide to Law Enforcement Intelligence Literature* (Scarecrow Press, 1990); and *Information Security: A Practical Handbook on Business Counterintelligence* (Charles C Thomas, 1989). He is the winner of two literature awards and a professional service award from the International Association of Law Enforcement Intelligence Analysts. Dr. Prunckun has served in a number of strategic research and tactical intelligence capacities within the criminal justice system during his twenty-eight-year operational career, including almost five years as a senior counterterrorism policy analyst. In addition, he has held a number of operational postings in investigation and security. Dr. Prunckun is also a licensed private investigator and a radio engineer.