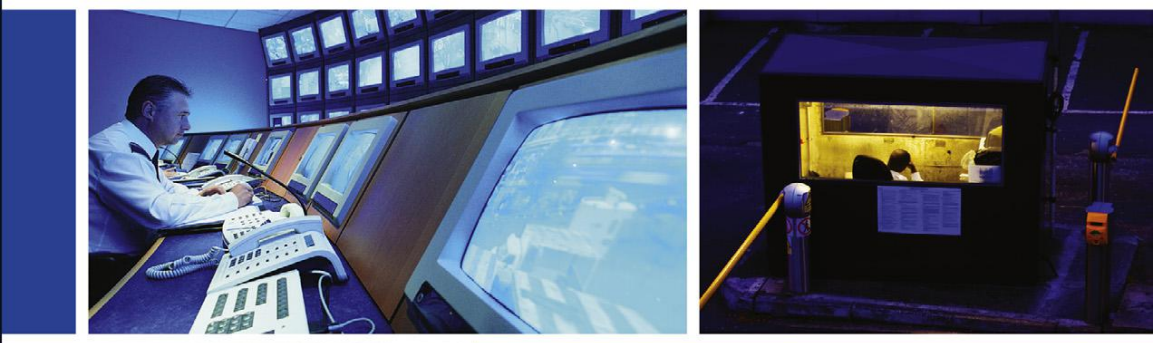
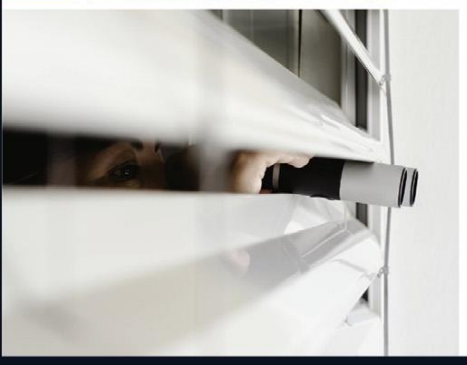
SURVEILLANCE AND THREAT DETECTION

Prevention versus Mitigation





Richard Kirchner, Jr.

B H

SURVEILLANCE AND THREAT DETECTION

This page intentionally left blank

SURVEILLANCE AND THREAT DETECTION

Prevention versus Mitigation

RICHARD KIRCHNER, JR.

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Butterworth-Heinemann is an imprint of Elsevier

Acquiring Editor: Brian Romer
Development Editor: Marisa LaFleur
Project Manager: Priya Kumaraguruparan
Designer: Matthew Limbert

Butterworth-Heinemann is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB UK

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloging-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-407780-5

CONTENTS

This page intentionally left blank

DIGITAL ASSETS

Thank you for selecting Butterworth Heinemann's *Surveillance and Threat Detection.* To complement the learning experience, we have provided a number of online tools to accompany this edition. Two distinct packages of interactive digital assets are available: one for instructors and one for students.

Please consult your local sales representative with any additional questions.

For the Instructor

Qualified adopters and instructors need to register at the this link for access: http://textbooks.elsevier.com/web/manuals.aspx?isbn=9780124077805

- **Test Bank** Compose, customize, and deliver exams using an online assessment package in a free Windows-based authoring tool that makes it easy to build tests using the unique multiple choice and true or false questions created for *Surveillance and Threat Detection.* What's more, this authoring tool allows you to export customized exams directly to Blackboard, WebCT, eCollege, Angel and other leading systems. All test bank files are also conveniently offered in Word format.
- **PowerPoint Lecture Slides** Reinforce key topics with focused PowerPoints, which provide a perfect visual outline with which to augment your lecture. Each individual

book chapter has its own dedicated slideshow.
- **Instructor's Guides** Design your course around customized learning objectives, discussion questions, and other instructor tools.

For the Student

Students will need to visit this link in order to access the ancillaries below. http://www.elsevierdirect.com/companion.jsp?ISBN=9780124077805

- **Self-Assessment Question Bank** Enhance review and study sessions with the help of this online self-quizzing asset. Each question is presented in an interactive format that allows for immediate feedback.
- **Case Studies** Apply what is on the page to the world beyond with the help of topic-specific case studies, each designed to turn theory into practice and followed by interactive scenario-based questions that allow for immediate feedback.

ACKNOWLEDGMENTS

In the course of the writing and research for this book, if I have failed to directly acknowledge the specific words of those who have written them, then it is not my intent to represent those words as my own and I happily provide acknowledgment to those who were original in their thoughts.

Portions of this book were written through the expert writing of Mark Graham and Mario Acevedo of Mark Graham Communications, Denver, Colorado. Thank you, gentlemen.

A special thank you to every member of the Pentagon Force Protection Agency—Office of Threat Detection past and present, particularly Ken "Mad Dog" Maddrey and Chaka Smith; Mr. Jim Pelkofski; the PFPA CI Shop; my friend(s) at the Threat Management Unit—CIA; John Reale for his cheerleading and keen business insights; Dan Botsch (and his professional staff) of TrapWire, Inc.; the Hon. George P. Shultz; editor extraordinaire Mary Jane Peluso with honorable mention to Amber Hodge for her latitude with deadlines; my loving parents; then oldest to youngest—Taddy, Sean, Skyelar, Liam, Emma, Christopher, and Lauren; and a very special thank you to my wife Kathleen, who, over and above the mothering of the aforementioned seven, is always at my side and shows me all things are possible through faith and our true love.

This page intentionally left blank

1

PREFACE AND INTRODUCTION

CHAPTER OUTLINE

Surveillance & Threat Detection. http://dx.doi.org/10.1016/B978-0-12-407780-5.00001-4

Abstract: *Surveillance and Threat Detection Methodology* is the most definitive resource to date addressing threat detection and attack prevention. This book contains never-before-published information from a subject-matter expert in the growing field of threat detection. The author shares a wealth of practical information on surveillance detection in the physical security realm. You are offered the opportunity to recognize a paradigm shift in modern-day security—one that goes from the reactive to the proactive—with details on how to protect yourself from terrorist and criminal attacks *before* they reach your doorstep! You will learn how to train your security force with the techniques and tactics necessary to recognize hostile surveillance and thwart an attack. This book is ideal for the professional physical security officer who wants a tooth-to-tail understanding of surveillance and threat detection.

Keywords: audience, detection, deterrence, normal, surveillance, territory, threat

1.1 Definitions

Actionable information: Information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process.

Anarchist: A person who rebels against any authority, established order, or ruling power.

Countersurveillance: All measures, active or passive, taken to counteract hostile surveillance.

Criminal enterprise: All illegal activity committed.

Emotionally disturbed persons: Individuals found within an administrative site assessed as either temporarily or permanently psychologically or mentally impaired to a degree that the person is gravely disabled or presents a clear danger to that person or another.

Foreign intelligence entity: Any foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service.

Hostile civil disturbance entities: Identified organizations known to target Department of Defense personnel, facilities, and assets through violence and other destructive and disruptive means.

If You See Something, Say Something: Trademarked public access program for individual reporting of suspicious activity to law enforcement.

Illegal imaging: The act of taking photos or recording video footage without prior authorization as outlined in jurisdictional law.

Measuring: Actively measuring distances of physical locations or objects by individuals located at that site through simple pacing, ground still photography, and/or commercially obtained overhead still photography. Measuring is a key step in the planning phase of attack/exploitation cycles, as the collection of such information assures the accuracy of plans, logistics, and execution.

Observation: Also regarded as "physical surveillance," this is systematic and deliberate observation of a person by any means on a continuing basis or acquisition of a nonpublic communication by a person not a party thereto or visibly present threat through any means not involving electronic surveillance.

Operational security: A protective and proactive discipline implemented to mitigate the risk of inadvertent exposure of personnel, methods, and means falling under surveillance detection (SD) purview. SD ensures and manages the continuous implementation of this discipline as to safeguard assigned personnel from potential negative or lethal actions having terrorism, antigovernment, foreign intelligence, and/or criminal nexus.

Presidential Executive Order 12333: President Ronald Reagan signed Presidential Executive Order 12333 on December 4, 1981 (U.S. President 1981, 1). The directive delineated the duties and responsibilities of the various U.S. intelligence agencies. This directive was also designed to protect the United States, its national interests and citizens, from foreign security threats. It also prohibited assassinations by stating, "No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination" (U.S. President 1981, 18).

Querying: The acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. A technique of human source intelligence collection, generally overt, unless the collector is other than he or she purports to be.

Surveillance: The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means.

Surveillance detection: Measures taken to detect and/or verify whether an individual, vehicle, or location is under surveillance.

Surveillance operation specialist: These personnel possess specialized advanced skills, training, and experiences in surveillance, surveillance detection, and countersurveillance methodologies.

Suspicious activity: Observed behavior indicative of criminal activities, intelligence gathering, or other preoperational planning related to national security or public safety.

Terrorism: The unlawful use of violence or threat of violence to instill fear and coerce governments and/or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and is committed in the pursuit of goals that are usually political.

Terrorist-related suspicious activity: Observed behavior consistent with preoperational targeting relating to a potential terrorist threat(s) to national security interests. Furthermore, any activity or behavior related to planning, preparation (including probes), and attack execution.

Test of security: Any attempt to measure reaction times and actions by police, security personnel, and/or other first responders. A simple mistake such as a vehicle approaching

a security barrier and then turning around or an attempt to circumvent access control procedures in order to assess strengths and weaknesses of police and equipment can disguise acts of test of security.

Timing: A subset of observation or "physical surveillance" with the intent of identifying the precise moment in which gaps of security appear; associated patterns of life or reoccurring patterns set by individuals of interest, assets, and critical mission functions. Adversarial planners require this information in support of the analysis, collection management, and dissemination targeting cycle.

1.2 Scope

Surveillance and Threat Detection Methodology is the most definitive resource to date addressing threat detection and attack prevention. This book contains never-before-published information from a subject-matter expert in the growing field of threat detection. The author shares a wealth of practical information on surveillance detection in the physical security realm. You are offered the opportunity to recognize a paradigm shift in modern-day security—one that goes from the reactive to the proactive—with details on how to protect yourself from terrorist and criminal attacks *before* they reach your doorstep! You will learn how to train your security force with the techniques and tactics necessary to recognize hostile surveillance and thwart an attack. This book is ideal for the professional physical security officer who wants a tooth-to-tail understanding of surveillance and threat detection.

The persistent stream of suspicious activity reports is proof that the "bad guys" are conducting surveillance of valuable targets in the United States and abroad. Such surveillance indicates preattack planning by terrorists and criminals and demands attention by security officers at all levels. To stop these attacks, security officers must understand terrorist and criminal surveillance and planning—to know what the "bad guys" are looking for and how they gather intelligence. Key to this understanding is that security officers learn how to distinguish "normal" from "not normal" behavior that will alert you to hostile surveillance and preattack planning. With this knowledge, security officers can implement protective countermeasures to detect, deter, disrupt, and defend against future attacks.

Whether you are responsible for a local storage facility, a bank, a mass-transit depot, or a nuclear reactor, introduction of a proactive threat detection program will increase your chances of preventing any attack dramatically. Such a program will align your security assets precisely to where they are needed and give you the tools to recognize if you are the target of criminal or terrorist surveillance. This first edition includes a historical overview of surveillance and an in-depth analysis of terrorist preattack and attack methodologies—illustrated with relevant real-world case studies. It describes how to incorporate threat detection into both a fixed-site physical security program and toward the protection of high-risk personnel. It discusses the counterintelligence and business intelligence arena and reviews the latest technologies in threat

detection and how they may integrate into your operations.

You will come to understand preattack and attack surveillance methodology and, more importantly, learn how to recognize hostile surveillance so you can *prevent* an attack.

1.3 Audience and Use Case Assumptions

For most of the individuals in the security and force protection ecosystem, "surveillance detection" is used commonly to describe the act of taking measures to detect and/or verify whether an individual, vehicle, or location is under surveillance. Throughout this book the words "threat detection" are utilized with and in place of "surveillance detection," as surveillance detection fails to capture the full scope of threats; threat detection fully encompasses the entire process of recognizing "threat" not just "surveillance." With many years working on and around the U.S. Pentagon Reservation we were looking for the enemy we wanted (Al Qaida, Hezbollah, Lone Wolves, etc.), yet we found the enemy we had (Russia, China, emotionally disturbed persons, etc.) all "threats" in and of themselves. This methodology rests on the proven historical understanding that the common element across the threat spectrum—regardless if it's internationally state-sponsored actors, homegrown violent extremists, extremist militia groups, intelligence operations, everyday criminals, or the emotionally disturbed person—has been, and will continue to be, that bad actors routinely

observe and record their target's activities to discover vulnerabilities and collect preoperational attack intelligence.

It should also be explained that the term "surveillance detection" is a misnomer. The word *surveillance* is the French word for "watching over"; "sur" means "from above" and "veiller" means "to watch." The word *surveillance* may be applied to observation from a distance by means of electronic equipment [such as closed-circuit television (CCTV) cameras] and usually of people for the purpose of influencing, managing, directing, or protecting. Therefore, detecting surveillance or "surveillance detection" could infer simply looking up to see a CCTV camera. The inverse of surveillance is sousveillance ("to watch from below") or the recording of an activity from the perspective of a participant in that activity or from ground level by an individual actor or even a small group. This is more to what threat detection methodology is seeking to discover, as this is the norm for bad actors collecting attack intelligence. However, and furthermore, simply looking for sousveillance is only a part of the requirement to capture actors conducting hostile preplanning and preoperational activity. The full spectrum of the threat (i.e., probing, querying, dry runs, and signaling) must be included to better define this evolving security strategy.

Threat detection programs are designed to exploit these risks by creating a mechanism to detect preoperational surveillance, report sightings, and disrupt an attack. The full threat detection program outlined in this book may

not be conducive to all organizations. Parts of the program can be extracted and suited to the needs of each organization's security plan. Before developing a threat detection program, organizations should ensure that their program will be in legal accordance with host country laws.

Disclaimer: The contents of this book are to provide rudimentary threat detection methodologies, much of which can be found as an open source with research. It is not intended as an advanced practical guide. To make such a textbook on advanced practices available publicly would certainly be studied by nefarious actors and would not be in the best interest of national public security. It is recommended for security practitioners that recognize the security and business value of threat detection, and desire a full scope program, to reach out to threat detection professionals for one-on-one consultations.

1.4 Executive Summary

Stopping attacks by terrorists and criminals against federal, state, local government, and corporate targets must include a new and proactive approach: *prevention* through the identification and disruption of preattack planning and surveillance activities. Because terrorists and criminals must conduct surveillance of their intended targets—often over a period of weeks, months, or even years—the detection of suspicious events and the correlation of these events can reveal the threat of an impending attack.

Surveillance and Threat Detection Methodology provides one of the most effective protective measures to prevent such an attack and does so by offering a paradigm shift in security thinking—one that is *proactive* versus *reactive*. This book shows how proactive measures can detect hostile surveillance and *prevent* an attack. Security officers will be taught the systematic steps of the criminal and terrorist preattack methodology and learn how to recognize suspicious behavior that signals preattack surveillance and planning. Incredibly, most in the public and private security industries have never heard of this methodology and so do not understand how to institute such a preventative program. With the information in this book, security officers can learn how to identify "bad guys" and employ appropriate countermeasures. This information encompasses how to detect terrorist and criminal surveillance and preattack planning, analyze suspicious activity reports, and develop an effective threat detection program. The results will increase the probability of preventing an attack dramatically while streamlining protection assets and costs.

The current model used to portray the security and protection of a facility is as concentric circles of physical security. In this model, we think of hardening the facility to provide warning and defend against an attack. The outermost ring represents where we would first detect a threat and adopt a heightened security posture. Security at this outer ring would be provided by long-range observation from within the facility and by patrolling the surrounding area. The middle ring represents where we begin screening access to the facility. Entry into the

facility would be channeled for control. It is here that we would rely on CCTV and active surveillance by security officers. The inner ring represents detection devices and physical barriers, such as metal detectors, alarms, dogs, fences, bollards, Jersey barriers, and guards to prevent unauthorized entry into the facility. The problem with this model is that it is reactive to a threat. Terrorists and criminals will surveil your facility to find the vulnerabilities in your security measures and penetrate even the most hardened of perimeters.

A better model is to think of security as concentric models of suspicious behavior. In the outermost ring, terrorists and criminals conduct cursory surveillance of your facility. At this point, their objective is twofold: (1) to see if an attack on your facility meets their strategic goal and (2) to gauge your facility's protective measures. Is it a hard or a soft target? The bad guys will engage in very-low profile behaviors as they observe your facility. They may simply walk by, watch, and take notes. If terrorist and criminals decide that an attack on your facility would still meet their strategic goal, then they will adopt more aggressive behaviors to gather intelligence; that is, they will move into the middle ring of suspicious behavior. Expect extensive documentation using photography, video, and hand-drawn maps. The bad guys will scout for surveillance zones where they can linger and observe unobtrusively. They will gain detailed information about your "pattern of life" and report the findings to their high-level operatives. If your facility has been designated as the target, then expect even more aggressive behaviors from the surveillants as they move

into the inner ring of suspicious behavior. Keep in mind that the bad guys will be clever in their methods, as they do not want to get caught and compromise their mission. They seek to get as much information as they can about the vulnerabilities of your security measures and to gauge the ability to meet their attack objectives (inflict maximum causalities, destroy the building, break into the vault, etc.). At this point, they will confront your security officers personally to ask questions, test your defenses and responses, gain entry into your facility, and find the lapses and gaps in your security measures. On the eve of the attack—the bull's eye of our rings of suspicious behavior—the bad guys will be present in full force to conduct last-minute surveillance and dress rehearsals to assure a successful operation, despite physical defenses.

1.4.1 Why Threat Detection

1.4.1.1 Territorial Dominance

When humans have their own territory, there is an impulse to defend this territory against others seeking to "invade" it. Territoriality is the attempt by an individual or group to affect, influence, or control people, phenomena, and relationships by delimiting and asserting control over a geographic area.[1]

1.4.1.2 Territorial Integrity

Your organization should *own* its operating environment and defend its territory effectively against acts of violence by another. KIRIK's

[1] Robert D. Sack. *Human Territoriality: Its Theory and History* (Cambridge Studies in Historical Geography). Cambridge University Press, November 1986.