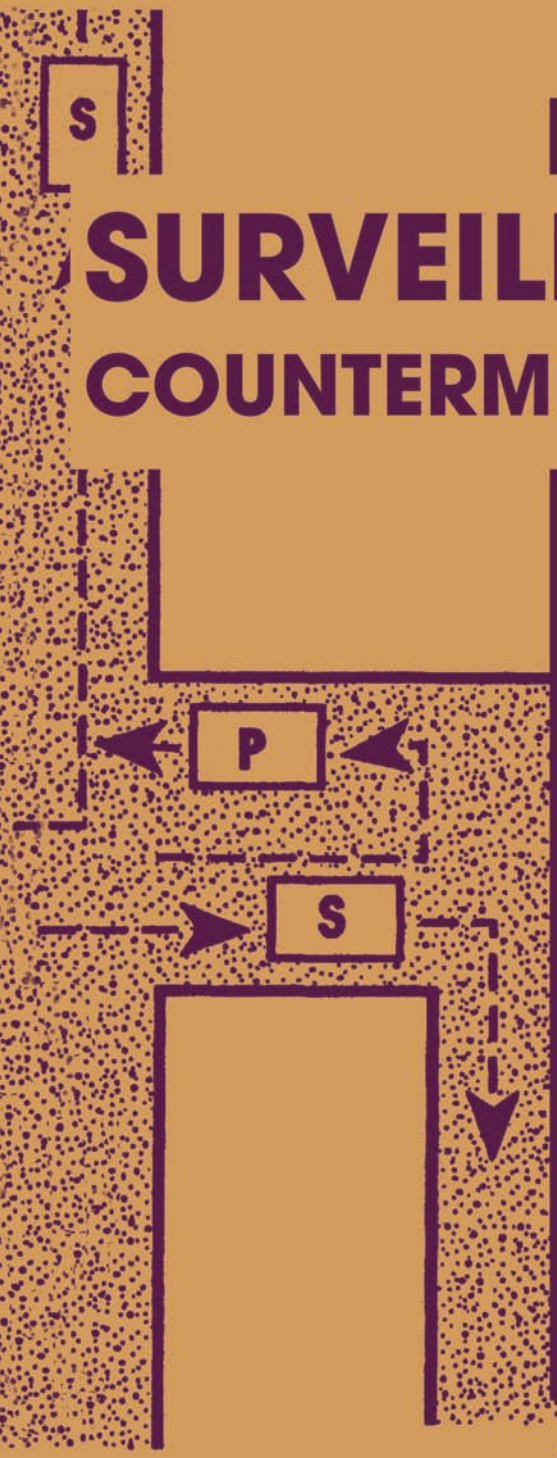

SURVEILLANCE COUNTERMEASURES

A Serious Guide to Detecting, Evading, and Eluding Threats to Personal Privacy

ACM IV SECURITY SERVICES

CONTENTS

CHAPTER 1

INTRODUCTION TO SURVEILLANCE COUNTER-MEASURES

This book was originally published during the last decade of the 20th century. Since that time, there has been an unanticipated proliferation of hostile covert elements that has significantly increased the threat to citizens, businesses, and national security interests of the United States and other democratic nations, both at home and abroad. For this reason, this book's applicability has broadened significantly from the original target audience of a small core of security professionals to virtually everyone.

The techniques in this work were documented shortly after the conclusion of the Cold War and were in large part intended as a tribute to the legacy of the cloak-and-dagger intrigue that characterized that era. In those bipolar days, adversaries generally exercised mutual protocols in a high-stakes gentlemen's game of spy versus spy. Even in the world of international terrorism during the previous era, there was a relatively rigid distinction between what were considered "legitimate" targets and off-limit targets (such as innocent civilians) that would result in negative sentiments toward the terrorist cause.

Today, terrorist and espionage operatives are less discriminate about the individuals they target, and criminal organizations have become less restrained in order to compete in the increasingly unscrupulous global crime market. These factors, coupled

with the dynamics of globalization, are responsible for a much more dangerous world for many more people. As a general rule, there are no rules, and no one is exempt.

The new reality of the contemporary environment is characterized by a wide range of unconstrained and asymmetric threats that act with relatively less regard to consequence. In the past 15 years, we have experienced the development of a much more pervasive and dangerous "underworld"—one that threatens a much broader stratum of society. Now there is a plethora of acute threats to the personal privacy and security of average citizens, including common criminals and stalkers, private and corporate investigative elements, international crime and terrorist organizations, government-sponsored espionage agencies, and, of course, radical Islamic terrorists who view all nonbelievers of Islam as infidels and enemies and therefore legitimate targets.

In virtually all cases, the elements that threaten individual, corporate, or national security conduct surveillance operations to further their objectives or as the primary means to an end. In today's hazardous environment, security professionals must understand the threat and be able to advise clients regarding the appropriate countermeasures to protect against a hostile surveillance effort. The average citizen, too, has a vested interest in understanding the concepts of surveillance countermeasures that can enhance personal security.

At the most basic level, criminals will "case" potential targets to develop information to maximize their probability of success in committing a crime. Sophisticated criminal organizations will conduct more extensive surveillance efforts to develop information on individuals they intend to intimidate, exploit, or terminate. Terrorist organizations conduct comprehensive preoperational surveillance to maximize the probability of successful attacks. In preparation for criminal or terrorist acts, surveillance is employed to determine when and where the target is most vulnerable.

Methods of international espionage have become much more aggressive toward nonmilitary and nongovernment targets. To a large degree, the intelligence services of foreign countries, both friend and foe, are competing in a global war based on economics. With less emphasis on military advantage and more on economic strength, the number of individuals who are vulnerable to espionage

because of business affiliations is vastly increased. This expanding threat is further compounded by the ever-increasing practice of industrial espionage conducted between competing businesses.

Criminal, terrorist, and espionage organizations also employ surveillance in support of efforts to recruit or coerce individuals to provide information or other types of support. To this end, surveillance is employed to develop exploitable information on unwitting individuals. Those confronted with exploitable evidence developed through surveillance may be forced to cooperate rather than risk having the information disclosed to their families, employers, or the public. Attributes and vices such as infidelity, homosexuality, alcoholism, and drug abuse are some common examples of the limitless options possible for such blackmail operations. As a corollary, the majority of surveillance activities conducted by private investigative agencies are undertaken to confirm or deny whether an individual is conducting similar types of activities. Even individuals with no readily exploitable attributes can be manipulated into compromising situations to develop the leverage necessary for coercion.

Regardless of the nature of the threat, surveillance can be detected and defeated through the effective use of surveillance countermeasures. This book addresses the principles that have developed into time-proven methods of countering the most sophisticated surveillance techniques. Importantly in this age of terrorism, the very same surveillance countermeasures that are applicable to the detection of preoperational surveillance can prove critical when hostile elements are actually in the act of a crime or attack. This is the point when operators must expose themselves and are consequently most vulnerable to detection. Proficiency in the techniques of observation and surveillance countermeasures is an effective means to prevent the act or enable individuals to avoid the threat when in harm's way.

Surveillance countermeasures can be categorized as either surveillance detection or antisurveillance. The former is employed to detect the presence of a possible or suspected surveillance, while the latter is employed to elude a suspected or detected surveillance. Both methods are further categorized into distinct disciplines.

In general terms, surveillance can be categorized as either physical or technical. Accordingly, surveillance countermeasures can be either physical or technical, based on the nature of threat. Physical

surveillance requires the direct involvement of the human element, which simply means that it must involve physical observation of the target by an individual or a team of surveillants. For this reason, physical surveillance assumes a degree of exposure of the effort to the individual under surveillance. Surveillance countermeasures are employed to maximize this exposure or to force surveillance operators to terminate contact in order to avoid exposure. Technical surveillance uses such equipment as remotely monitored video cameras, listening devises or "bugs," telephone monitors or "taps," and motion-monitoring beaconing devices to observe, monitor, or record the target's activities. Technical surveillance devices are vulnerable to both physical inspection and technical detection.

While the technical-surveillance concepts detailed in this book are still largely relevant, based on the emergent threat environment the physical surveillance countermeasures addressed herein have become invaluable. Many elements that conduct surveillance activities are either unable or unwilling to rely heavily on technical surveillance means, primarily because of the sophistication of technical detection capabilities and the unacceptable risk of compromise. For this reason, the majority rely exclusively on the time-tested physical techniques that involve human operators who can think, react, and terminate the surveillance if necessary rather than compromise an operation.

Again, based on the new reality, the techniques documented in this book are more widely applicable to security professionals and vulnerable citizens than when originally presented in 1994. In fact, the U.S. National Intelligence Council's 2020 Project, titled "Mapping the Global Future," predicts a steady increase in threats to a wide range of individuals based on the disturbing trend of "pervasive insecurity"—one that is expected to continue well into the second quarter of the 21st century. As a parting and practical example, in May 2000, an al Qaeda terrorist organization training manual was seized in a safe house in Europe. One of the manual's chapters is dedicated to covert surveillance and addresses the development and utilization of exploitable information as a primary method of coercing individuals into support of the cause. As a testament to the enduring relevance of this text, each of the surveillance techniques addressed in the terrorist training manual are detailed in this book, with corresponding and exacting countermeasures.