Book Review

The quiet threat: Fighting industrial espionage in America

Ronald L. Mendell
Charles C. Thomas Publisher Ltd., *Springfield*, *IL*, *2010*, *2nd edn.*, *272pp.*, *$59.95*,
ISBN: *978-0398079628*

Security Journal (2012) **25,** 90–93. doi:10.1057/sj.2011.26

In a world where intellectual property crime and victimization are becoming more prevalent because of mass communication and technological advances, Ronald L. Mendell's updated contribution to the world of industrial espionage is particularly timely and important. Since Charles C. Thomas Publisher Ltd. first published *The Quiet Threat: Fighting Industrial Espionage in America* (*2nd edition*) in 2003, great advancements have been made with respect to information technology, corporate outsourcing and the transience, as well as erosion, of intellectual capital. As a result, real-time data management and security concerns have emerged as a clear and present danger to corporations and governments alike. Similarly, intellectual property crime and industrial espionage have garnered increasing interest among criminologists and researchers, particularly because the incidence and prevalence of these crimes are heavily influenced by fast-paced changes in technology.

The Quiet Threat is a book that appears to be particularly focused on introducing readers to the concept of industrial espionage as a silent, enigmatic foe, which poses a significant threat to the competitive position of modern corporations and economic strength of powerful nations. Throughout the text, Mendell discusses several different facets of industrial espionage from both a historical and practical point of view. However, the book is not laid out chronologically from past to present, following a clear or linear path. Instead, the book presents and discusses practical concepts that are relevant to acts of industrial espionage and those who are entrusted with providing information security. Later, the text circles back on important concepts through an examination of information gathering tactics and techniques, which have been used throughout history, along with some of the processes that are related to the pervasiveness of espionage at present. Discussion topics, exercises and questions, as well as a list of further readings, can also be found at the end of each chapter to extend each reader's experience beyond the pages of the text. These additions to each chapter present the reader with an opportunity for further reflection on and guided preparation for prevailing security concerns.

After a brief introductory discussion of the paradoxical nature of information security in the modern era, Chapter 1 begins by familiarizing readers with the use of visual observations as a general technique of gathering data, through either legal or illegal channels. Mendell implicates individual powers of observation in the important process of detecting, identifying and deconstructing the meaning behind various types of information. Throughout this

chapter, Mendell reveals a number of historical examples of factory observations conducted throughout history on various companies and enterprises, which were attempts to obtain a competitive marketplace advantage. Then, he proposes a number of exercises that readers may engage in to hone their observational skills.

Chapter 2 is dedicated to a discussion of how knowledge can be constructed and attained through research and information gathering, particularly open-sources of Competitive Technical Intelligence. Mendell likens the process of knowledge construction to sorting 'through a dense thicket of facts', which originate with a seed and grow into the branches of a tree. This knowledge construction tactic involves learning as much as possible about one's competitors and industry through legitimate, accessible sources, thereby fostering one's greater understanding of a target's points of weakness. Utilizing this process allows the information gatherer to use knowledge as a point of leverage against specific targets.

Evidence of knowledge construction can be seen in Chapter 3, for example, where Mendell traces the roots of espionage techniques to the Elizabethan Age in England and follows them through periods of industrialism in eighteenth and nineteenth century England. From this point, much of Mendell's subsequent analyses of industrial espionage through the twenty-first century (Chapters 4 and 5) are also grounded in quite interesting and informative historical accounts of spying and intellectual property crime, both in the United States and abroad.

Chapter 4 continues Mendell's initial discussion of observation to include a wider array of observation techniques which are aimed at discovering sources of data. Accordingly, he suggests that paths to observation and information gathering may be accessible through many different sources: computer and mobile technology (networks, operating systems, e-mail, laptops, disks, drives, printers and so on), electronic eavesdropping (bugging, wiretapping and so on), infiltration (impersonation, vendors and so on), sales forces (divulging information) and sifting through trash or public records. Mendell slightly changes course in Chapter 5 to address the evolution of industrial espionage techniques throughout history, particularly with respect to the changing nature of business in the United States. In particular, the text is dedicated to revealing how a more comprehensive, multi-pronged approach to information gathering and spying, not taken in years past, will act as a 'stepping stone' to acquiring secrets.

Mendell provides additional evidence of multi-pronged espionage techniques in the next chapter. Consistent with the notion of acquiring trade or business secrets, Chapter 6 examines various elements of politics and power that are implicit in most cases of industrial espionage. In particular, Mendell seems to suggest that having political savvy and fortitude is necessary not only for the spy looking to obtain information, but also for those entrusted with protecting a corporation's intellectual property. Some of the techniques he discusses include acquiring access to data through higher-education research, engaging in bribery, providing disinformation to targets, and engaging in ruses and deceptive tactics. He later provides evidence of these tactics in examples of patent infringement, theft of trade secrets and the failure of US intelligence efforts during the Vietnam War.

Chapter 7 provides an in-depth discussion of the countermeasures historically taken to protect sensitive information, but from the perspective of a spy trying to circumvent those protections. In this case, the 'spy' is referred to as an information predator, and he provides a first-hand account of how he has, or might, go about bypassing traditional security measures. This chapter provides a refreshing segue into Chapters 8 and 9, which reveal

a number of internal and external methods of supplementing traditional security measures. In this regard, Mendell suggests that organizations fail to do enough to secure their information, even from their own employees. As a result, he argues that internal security may be bolstered by providing clear objectives, goals, and training for security staff, by patrolling more effectively, and by engaging in intelligence building through the gathering of information. Similarly, building an intelligence gathering operation to focus on information outside of the organization can help stifle external threats to security.

In Chapter 10, Mendell discusses the process of investigating cases of industrial espionage, namely the theft of trade secrets occurring following the passage of the Economic Espionage Act of 1996. Through this exploration, the author provides a general description of what constitutes trade secret theft, in addition to providing a number of suggestions and checklists that investigators may follow in order to build evidence, bolster security and combat industrial espionage.

The final two chapters of the main body of text are devoted to a discussion of spy tradecraft, also known as 'tricks of the trade', and data mining. In Chapter 11, where Mendell refers to tradecraft as both an art and science, the importance of human relations, social adaptation and manipulation, keen observational skills and the use of photographic information are highlighted as necessary characteristics of the effective spy. Mendell concludes in Chapter 12 with a detailed discussion of how data can be so readily accessed in today's modern era of communication. He also reveals the various techniques that can be used to discover and identify useful databases and other sources of information, which may be of interest to intelligence seekers and security specialists.

Although each chapter provides plenty to consider with respect to industrial espionage, the primary body of text is also supplemented by a collection of readings and blueprints found after the final chapter. These supplementary items include a Chapter Notes section, a Master Checklist, a brief Chronology of important events concerning industrial espionage throughout history, a section detailing how to plan for an intelligence operation against a target, a sample intelligence gathering report and a glossary of terms that are important/relevant to any discussion of industrial espionage. The Chapter Notes offer a thorough description of the origins of various perspectives found in the book, whereas the Master Checklist provides a summary of each important security proposal that is discussed. Considered together, all of these readings provide additional supporting information, as well as a greater level of detail not found in the main body of the text. For this reason, Mendell's primary audience here appears to be those who are in positions to apply information security techniques to real-world settings, as well as those entrusted with providing security for their agency or enterprise. Thus, practitioners may find the supplementary information quite useful as a means of more deeply exploring the topic.

Generally, *The Quiet Threat* is a book targeted at students of information security or individuals in certificate programs, as well as information security professionals actively working in either the public or private sector. In fact, according to Mendell, 'the text's primary aim is practical advice'. The book may be well suited for information security practitioners or possibly even corporate executives looking to gain a competitive advantage. There is certainly enough information for students and security professionals to gain additional insight into the phenomena of industrial espionage. However, beyond individuals in security professions, the book may have less practical utility, particularly for those only looking to achieve a basic understanding of the subject. Because of the book's hands-on

approach, chapters often read more like texts for college coursework or instruction manuals for vocational training programs. In this regard, there are simply far too many checklists and bullet points for the casual reader to follow.

Nevertheless, Mendell's book does provide a thought-provoking discussion of industrial espionage within the context of the prevailing era. With awareness of intellectual property crime and industrial espionage becoming more widespread, this book does represent an important contribution to the growing body of literature focused on intelligence gathering and the dissemination of intellectual capital.

William A. Stadler
Department of Criminal Justice and Criminology,
University of Missouri, Kansas City, USA