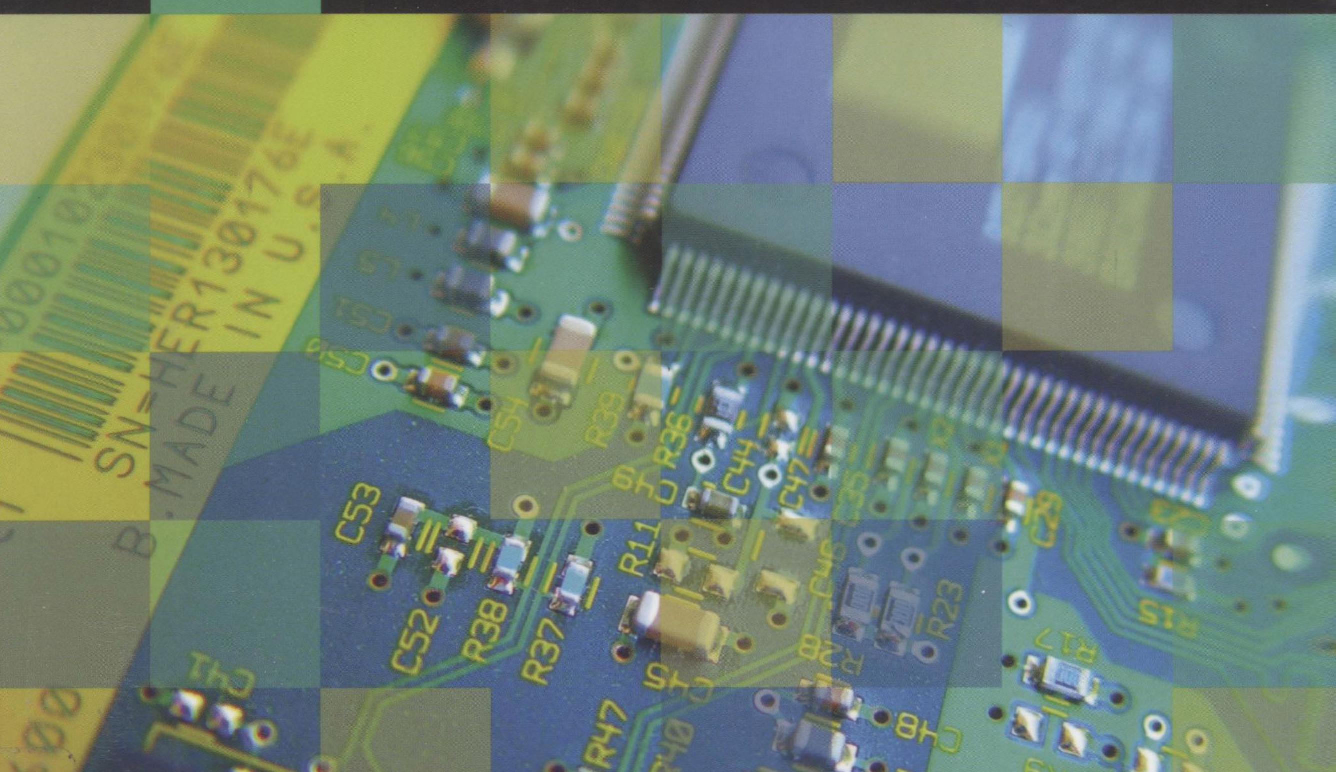
CYBERCRIME

investigating high-technology computer crime



Robert Moore

second edition

anderson publishing

CYBERCRIME

INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME

SECOND EDITION

ROBERT MOORE

ELSEVIER

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

ap

Acquiring Editor: Shirley Decker-Lucke
Development Editor: Ellen S. Boyne
Project Manager: Sarah Binns
Designer: Dennis Schaefer

Anderson Publishing is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Elsevier, 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, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments 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 Control Number: 2010935324

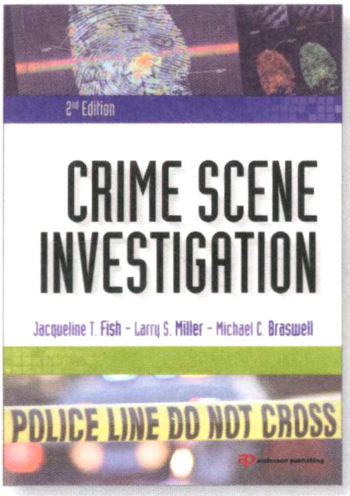
British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-1-4377-5582-4

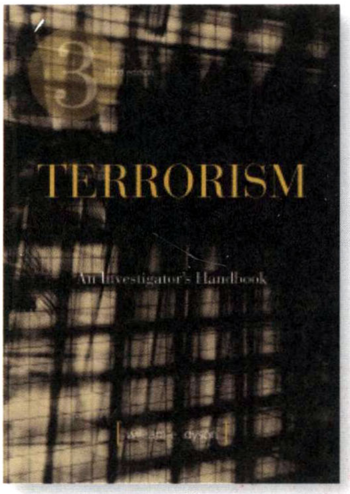
For information on all Anderson Publishing publications
visit our Web site at www.andersonpublishing.com

Printed in The United States of America
10 11 12 13 9 8 7 6 5 4 3 2 1

Other Titles of Interest from Anderson Publishing®


2nd Edition
CRIME SCENE INVESTIGATION
Jacqueline T. Fish - Larry S. Miller - Michael C. Braswell
POLICE LINE DO NOT CROSS
anderson publishing

Crime Scene Investigation 2e
Jacqueline T. Fish, Larry S. Miller, Michael C. Braswell
978-1-4224-6331-4



Terrorism: An Investigator's Handbook 3e
William E. Dyson
978-1-59345-530-9

Criminal Investigation: A Method for Reconstructing the Past 6e
James W. Osterburg, Richard H. Ward
978-1-4224-6328-4

Police Photography 6e
Larry S. Miller, Richard T. McEvoy Jr.
978-1-4377-5580-0

Report Writing for Criminal Justice Professionals 4e
Larry S. Miller, John T. Whitehead
978-1-4377-5584-8

Interviewing and Interrogation for Law Enforcement 2e
John E. Hess
978-1-4224-6325-3

Legal Guide for Police: Constitutional Issues 9e
Jeffery T. Walker, Craig Hemmens
978-1-4377-5588-6

Civil Liability in Criminal Justice 5e
Darrell L. Ross
978-1-4224-6139-6

Crisis Negotiations 4e
Michael J. McMains, Wayman C. Mullins
978-1-4224-6323-9

Effective Police Supervision 6e
Harry W. More, Larry S. Miller
978-1-4377-5586-2

ap anderson publishing www.andersonpublishing.com

Professors and Instructors only: 1-877-374-2919 | criminaljustice@elsevier.com

To place an order with Anderson Publishing at Elsevier Science & Technology books:
1-800-545-2522 or log on to www.elsevierdirect.com

Introduction

The topic of high-technology crime and cybercrime is discussed much more today than it was five years ago when the first edition of this text was released. Computers have become integral parts of the daily lives of citizens around the world. The number of individuals who gain access to the World Wide Web, both for legitimate and for illegitimate reasons, continues to increase every day. Criminal activities involving computers and technology continue to be a problem for the criminal justice system. It is worth noting that while crime numbers have increased over the last five years, the criminal justice response has also increased. Today there are more criminal justice agencies staffing cybercrime-related investigators. Additionally, there are more computer forensics services available for investigators. However, there is still a continuing need to increase awareness and understanding of cyber-related crime.

There is an incredible amount of literature on the topic of cybercrime, ranging from works on cybercrime in general to more specific works that focus on particular cyber-related crimes. However, the current work seeks to continue its original goal—to provide an introductory level of coverage to a rapidly changing field of the criminal justice system. This work is written for those who have limited or no knowledge of how computers work and/or computer networking principles. Readers are introduced to various complex topics in an easy-to-understand format. It is the hope of the author that these materials can be of use not just to university students but also to those who are currently working in the criminal justice field.

The book is divided into three sections. The first section consists of an introduction to high-technology crime, which is also commonly referred to as *cybercrime*. The second section addresses investigative issues associated with the investigation and prosecution of these crimes. The final section provides readers with some insight into the future of study in the area of high-technology crime, including current issues and an introduction to the emerging field of cybercriminology.

It is not the intent of this work to make the reader an expert in the area of high-technology crime, for no single work could accomplish this. The field is complex and constantly changing, as the technology used by both the criminals and the criminal justice system continues to evolve. Instead, the reader should view this work as a starting point for future study and research on the topic. To assist in this process each chapter concludes with a series of review questions designed to highlight the important terminology and concepts presented within each chapter. Each chapter also contains reference to related books, articles, or court cases that have been selected to provide interested readers with a means of continuing their education in this area. There are also a variety of websites and organizations that maintain a virtual presence on the World Wide Web, many of which provide up-to-date information on many of the topics discussed in this work. Therefore, each chapter will contain a brief listing of relevant websites that readers may visit in order to continue learning about the topics addressed in each chapter. Finally, every chapter except the final one will contain a brief spotlight on a news story that addresses how the materials discussed in the chapter are used or encountered in practice. These news stories are relatively recent; the stories come from news sources within the previous two to three years, with the majority published in the year before press time. The final chapter covers the new and exciting area of cybercriminology. Scholars in this area of study are working to gain a better understanding of what causes individuals to engage in the many cyber-related crimes that are discussed in this work. While there are few news articles that address these studies, numerous academic journal articles and textbooks are being developed on the topics, and readers are provided with information on these works.

As with the first edition, it is the hope of this author that this work will motivate readers to become more involved in the areas of research and training in the high-technology crime field.

Table of Contents

Chapter 10
Executing a Search Warrant for Digital Evidence 205

Chapter 11
An Introduction to Computer Forensics 229

Chapter 1

An Introduction to High-Technology Crime

When discussing crimes that involve computers and technology it is possible that prior to this reading the term *high-technology crime* may not have been heard by the reader. The term *technology* is often used to refer to mechanical or electrical devices that assist individuals in their day-to-day activities, but what does it mean to discuss *high technology*? As this is a work designed for those who are either interested in or currently involved in the field of criminal justice, let us take the standard equipment of a law enforcement officer as an example. Today, most all law enforcement personnel carry a firearm of some type, regardless of whether they elect to utilize a revolver or a semi-automatic. Is the officer's firearm a piece of technology? Of course. The firearm is a highly mechanical device, with the revolver having been developed by Samuel Colt in 1836. Therefore, the firearm is a piece of technology and one that has been around for more than a 100 years. Now, is the firearm a piece of high technology? This could be debatable, as some would consider the complex designs and manufacturing components of the firearm to make it a highly sophisticated piece of technology. But does being highly sophisticated equate to being considered high technology? Probably not. In the eyes of this author, the term *high technology* invokes images of highly developed electronic devices—more in line with the components that make up a cellular telephone than the components of a firearm.

It is worth noting that for many people what they consider to be a computer—the large electronic device that we type our research papers on and use to browse the Internet—is not the limitation for the technology. A computer is an electronic device that allows the user to input information, process that information, and then receive

DOI: 10.1016/B978-1-4377-5582-4.00001-7

results that are based on the information provided by the user. Many of these devices do not come with monitors or keyboards. For example, many of us now commonly use a debit card at the local convenience store, thereby saving us the time and effort it takes to write out a check. To complete our financial transactions, the cashier merely takes our debit card and swipes the magnetic strip through a small machine, returning our card to us when he or she is finished. The small device attached to the cashier's cash register will obtain our account number from the magnetic strip on the back of the debit card. We as users then enter our PIN onto the keypad, and the transaction is either approved or rejected. The machine that reads our debit cards is a miniature computer. Furthermore, the debit card scanner would meet our earlier established criteria for being considered an example of a high-technology device. Another example of technological devices seeing increased use in our society would be cellular telephones. In the five years since the first edition of this text was published, a number of cellular phone manufacturers continue to release phones containing increasingly advanced software applications. Today's cellular phone can allow users from around the world to input information, process information, and send or receive information almost instantaneously. Each of these devices is a highly sophisticated electronic device that would therefore meet the previously discussed definition of a high-technology device. Now that we have a basic understanding of some examples of high-technology devices, questions that remain involve gaining a better understanding of high-technology crime and determining whether such criminal behavior is a serious problem that truly warrants examination and consideration.

What Is High-Technology Crime?

In keeping with the definition of high technology previously noted, *high-technology crime* refers to any crime involving the use of high-technology devices in its commission. These are crimes that involve the use of computers, telephones, check-reading machines, credit card machines, and any other device that meets the previous definition of high technology. There are numerous forms of high-technology crime, ranging from traditional crimes committed prior to technological advances, to newer crimes that rely on high-technology devices to commit crimes. In the past, there have been several different ways of referring to crimes involving high-technology devices. Perhaps the two best-known classifications used to distinguish these crimes are computer crimes or cybercrimes.

Computer Crimes

Traditionally, the term *computer crime* has been used to refer to criminal activities involving a computer that are made illegal through statute. The definition espoused by Eoghan Casey, one of the most well-known researchers in the area of computer-related crime, is used here because of the clarity of his focus. Accordingly, a computer crime would be a crime that involves a computer in one of the following ways:

- *The computer as an instrument of the crime.* Here, the computer is used as a means of engaging in the criminal activity. Under this category, the crime cannot be committed without the computer being turned on and used in the commission of the act. An example here would be the individual who uses a company computer to embezzle funds from a company account.
- *The computer as the focus of a crime.* Here, the computer is the intended target of criminal activity and is not necessarily used in the commission of the act. The best example of this is the individual who breaks into a computer supply store after hours with the intention of stealing computers and computer peripheral equipment.
- *The computer as a repository of evidence.* Here, the individual involved in a criminal act has not stolen the computer and has not used the computer as a means of committing the criminal act, but he or she has stored evidence on the machine. A good example of this is the individual who stores his or her illegally copied music files on his or her home computer. Note then that for this category to be applicable, the storage computer could not have been involved in the criminal activity. However, the generalizations are of minor concern because regardless of which category or categories the individual's actions fall under, she or he is still guilty of a computer crime under this definition.

This definition is a good means of addressing criminal activities that involve computer technology. Let us examine one of the more famous and commonly read about computer crimes: hacking. *Hacking* refers to the unauthorized access of another person's computer, and would be considered a computer crime under the preceding definition for several reasons. First, the crime involves a computer that was used as an instrument of the crime. To be guilty of hacking, one must actually type in commands to penetrate the security of a second computer. Second, both computers will probably maintain some form(s) of evidence that could be used to confirm the identity of the hackers. As such, computers involved in hacking would meet the third definition above, whereby computers are repositories of evidence related to a crime—in this case, the crime of hacking into the target computer.

Cybercrime

Cybercrime, returning to a definition provided by Casey, refers to any crime that involves a computer and a network, where a computer may or may not have played an instrumental part in the commission of the crime. The term *cybercrime* would be used to refer to a criminal act like that of identity theft, which involves the theft of someone's personal information such as their credit card number or Social Security number. When an individual commits the crime of identity theft, there are several methods of obtaining a target's personal information. Many of the techniques involve the use of a computer or a network, but many more techniques have nothing to do with computers other than information stored in text files on a computer's hard drive.

In reading the discussion above it becomes clear that the term *cybercrime* actually refers to computer-related crime; however, some consider computer crime to be a subdivision of cybercrime that warrants its own definition and understanding. The determining factor between the two appears to be little more than the issue of whether a statute is present to criminalize the use of the computer in the criminal act. Because of the fact that more crimes today are relying on the Internet, there has been a significant effort by legislators to expressly criminalize these acts in the statutes. For example, as recently as 10 years ago, many states did not criminalize online harassment. Apparently, the reigning thought at the time was that harassment via the computer did not have the necessary psychological or physical impact necessary to show harm to an individual. Legislators and criminal justice professionals today are beginning to understand the dangers of such crimes. Prior to the enactment of these statutes, individuals guilty of harassing someone over the Internet were prosecuted under other statutes that were, for lack of a better term, "stretched out" to include the crime under investigation. Now that more of the crimes are being made illegal through express statutes, the question arises as to whether there is a need to differentiate between the two forms of crime. Should computer crime be considered separately from cybercrime? After all, over the last five years the term *cybercrime* has superseded that of *computer crime*. A quick search for book and journal articles on the topic of cybercrime versus the topic of computer crime would result in a confusing number of articles as more researchers and professionals are utilizing the term *cybercrime* as an umbrella term for all crime involving computers and technology.

Consolidating High-Technology Crimes

It could be argued that criminal behavior is criminal behavior regardless of the terminology used to describe the behavior. Therefore, a strong argument could be made that the distinction between a computer crime and a cybercrime is trivial. Both activities are crimes, and both activities involve technology in the commission of the acts. The majority of hacking attacks, with hacking being the most historically well known of computer crimes, are now reliant on the Internet and network connections. Because of this fact, the definition of a computer crime is now beginning to blur into the definition of a cybercrime—being that the worldwide network, the Internet, is now involved in many criminal activities that rely on computer technology.

In this work, I hope to provide information on several crimes that may involve only limited influence of computers and networks, as well as acts that rely almost entirely on the use of a computer and a network. These crimes most often involve highly developed technology in the commission of the crime, and as such the term *high-technology crime* is utilized for the purposes of this work. By utilizing this term I am referring to criminal activities that may have at one time been considered a computer crime or a cybercrime, with some of the crimes being considered a combination of both. Semantics regarding whether the act is a computer crime versus a cybercrime versus a high-technology crime is not important. Gaining a better understanding of the problem and the need to develop a strong response is more important.

How Serious Is the High-Technology Crime Problem?

With the term *high-technology crime* we are now referring to many diverse criminal activities such as hacking, digital child pornography, identity theft, intellectual property theft, and online fraud. The rate of each of these crimes has been steadily increasing in recent years and, when examined as a whole, amounts to a very serious problem. It should also be noted that the problem is not isolated to the United States. Problems associated with high-technology crimes have become increasingly more discussed in every country around the world—even in countries not known for their high levels of technological development and skill. Technology has played a key role in globalization, but this shrinking of the world has also led to many difficulties in terms of criminal activity. The worldwide nature of high-technology crime has developed problems involving such considerations as jurisdiction. In some cases it is now very difficult to determine who has the authority to investigate a high-technology crime. For example, an individual living in Russia is capable of transmitting an image of child pornography here to the United States. In this situation, who has