

Fourth Edition

CYBER CRIME AND CYBER TERRORISM

Robert W. Taylor

University of Texas at Dallas

Eric J. Fritsch

University of North Texas

John Liederbach

Bowling Green State University

Michael R. Saylor

University of Texas at Dallas

William L. Tafoya

University of New Haven



330 Hudson Street, NY NY 10013

Vice President, Portfolio Management: Andrew Gilfillan
Portfolio Manager: Gary Bauer
Editorial Assistant: Lynda Cramer
Field Marketing Manager: Bob Nisbet
Product Marketing Manager: Heather Taylor
Director, Digital Studio and Content Production: Brian Hyland
Managing Producer: Jennifer Sargunar
Content Producer: Rinki Kaur
Manager, Rights Management: Johanna Burke

Operations Specialist: Deidra Smith
Creative Digital Lead: Mary Siener
Managing Producer, Digital Studio: Autumn Benson
Content Producer, Digital Studio: Maura Barclay
Cover Designer: Studio Montage
Cover Images: Scanrail1/Shutterstock
Full Service Project Management: Ranjith Rajaram
Composition: Integra Software Services, Ltd.
Text Printer/Bindery: LSC Communications, Inc.
Cover Printer: Phoenix Color/Hagerstown
Text Font: TimesLTPro-Roman

Copyright © 2019, 2014, 2013, by Pearson Education, Inc. or its affiliates. All Rights Reserved. Manufactured in the United States of America. This publication is protected by copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights and Permissions department, please visit www.pearsoned.com/permissions/.

Acknowledgments of third-party content appear on the appropriate page within the text.

PEARSON and ALWAYS LEARNING are exclusive trademarks owned by Pearson Education, Inc. or its affiliates in the U.S. and/or other countries.

Unless otherwise indicated herein, any third-party trademarks, logos, or icons that may appear in this work are the property of their respective owners, and any references to third-party trademarks, logos, icons, or other trade dress are for demonstrative or descriptive purposes only. Such references are not intended to imply any sponsorship, endorsement, authorization, or promotion of Pearson's products by the owners of such marks, or any relationship between the owner and Pearson Education, Inc., authors, licensees, or distributors.

Library of Congress Cataloging-in-Publication Data

2013047759

1 17



ISBN-13: 978-0-13-484651-4
ISBN-10: 0-13-484651-6

*For my beautiful grandchildren: Madison, Olivia, and Brody; Kylie;
August, Axel, and Aero*
RWT

For Cheryl D. and my J-Kids (Jerod, Jacob, Joley, Jadyn, and Jaxon)
EJF

For Allyson and Ben
JL

*For the love of my Life, and my wonderful kids Shelbe, Kyla, Ayden, and
Knox for all their love and support*
MRS

*For the CyberCops and White Hat Hackers who have dedicated
themselves to making cyberspace a safer place for the rest
of us and the women in my life who make ours a better world:
Renee, Wendi, Samantha, and Ashley*
WLT



CONTENTS

Preface xv

Acknowledgments xxii

Section I The Etiology of Cyber Crime and Cyber Terrorism

Chapter 1 INTRODUCTION AND OVERVIEW OF CYBER CRIME AND CYBER TERRORISM 1

Chapter Objectives 1

Introduction 1

New Threats to the Information Age 2

Purpose and Scope of This Book 3

Defining the Terms 4

Overview 5

A Developmental Perspective on a Growing Problem 5

The Reality of Increased Cybervictimization 7

Changes to Cybervictimization and the Emergence of Cyber Terror 8

The Costs of Cybercrime 9

Classification of Computer Crime 12

Carter's Classification of Computer Crimes 13

Other Classification Schemes 17

Summary 18 • *Review Questions* 19 • *Critical*

Thinking Exercises 19 • *Endnotes* 19

Chapter 2 CYBER TERRORISM AND INFORMATION WARFARE 22

Chapter Objectives 22

Introduction 22

Defining the Concepts 24

Buzzwords: Information Warfare, Cyberterrorism, and Cybercrime 24

Risk and Critical Infrastructure Attacks 27

Low-Level Cyberwar 27

Infrastructure Reliance 28

Information Attacks 31

Web Site Defacement 32

Cyberplagues: Viruses and Worms 32

- Distributed Denial-of-Service Attacks 33
- Unauthorized Intrusions 35
- Cyber and Technological Facilitation 36*
 - Facilitation of Attack and Dissemination of Ideology 36
 - Data Hiding 37
 - Cryptography 37
- Propaganda and Promotion 38*
 - Funding and Financing Terrorist Groups 39
- Cyberterrorism as an Adjunct Attack 41*
 - Al Qaeda, the Islamic State, and Information Technology 41
- Perspectives on Information Warfare 43*
 - The Russian Perspective 43
 - The Chinese Perspective 44
 - Summary 45 • Review Questions 46 • Critical Thinking Exercises 46 • Endnotes 46

Chapter 3 THE CRIMINOLOGY OF COMPUTER CRIME 49

- Chapter Objectives 49*
- Introduction 49*
- Choice Theory 49*
 - Routine Activities 50
- Deterrence Theory 52*
- Psychological Theories 53*
 - Moral Development and Crime 53
 - Personality Disorders 54
 - Pedophiles and Psychological Theory 55
- Social Structure Theories 56*
 - Strain Theory 56
 - White-Collar Crime and Strain Theory 58
- Social Process Theories 59*
 - Learning Theory 60
 - Hackers and Learning Theories 67
 - Virus Writers and Learning Theories 69
 - Social Control Theory 70
- Terrorism and Political Theory 71*
 - Summary 74 • Review Questions 74 • Critical Thinking Exercises 74 • Endnotes 74

Chapter 4 HACKERS 77

<i>Chapter Objectives</i>	77
<i>Introduction: What Is a Hacker?</i>	77
Who and What Is a Hacker?	78
Today's Hackers	79
<i>Defining Hackers</i>	83
Cyber criminals Versus Hackers	83
Crackers	86
Script Kiddies	86
White Hat Versus Black Hat	87
Hacktivists	88
<i>The Origins and History of Hacking</i>	89
Hacking Changes	89
The Criminalization of Hacking	90
Challenges and Changes in Hacking	92
<i>The Hacker Subculture</i>	93
Technology	94
Knowledge	96
Commitment	98
Categorization	99
Law	102
<i>Summary</i>	105
<i>Review Questions</i>	105
<i>Critical Thinking Exercises</i>	105
<i>Endnotes</i>	106

Chapter 5 SOPHISTICATED CYBER CRIMINAL ORGANIZATIONS 109

<i>Chapter Objectives</i>	109
<i>Introduction</i>	109
<i>Espionage and the Theft of Intellectual Property</i>	111
<i>Insider Fraud</i>	115
Sabotage	118
<i>Sophisticated Criminal Organizations</i>	120
The Impact of Organized Crime	120
Use of Social Media by Organized Crime	121
African Criminal Enterprises	122
Asian Criminal Enterprises	123
Operation Avalanche	124
Balkan Criminal Enterprises	125
Eurasian Criminal Enterprises—Russian Organized Crime	126

Italian Organized Crime—La Cosa Nostra (LCN) Mafia 126
Middle Eastern Criminal Enterprises 128
Mexican and South American Drug Cartels 128
The Indiscriminant Underground Marketplace—The Deep Web or Tor Network 129
 Summary 135 • *Review Questions* 136 • *Critical Thinking Exercises* 136 • *Endnotes* 136

Section II Cyber Crime: Types, Nature, and Extent

Chapter 6 WHITE-COLLAR CRIMES 138

Chapter Objectives 138
Introduction 138
Embezzlement 139
Corporate Espionage 141
Money Laundering 144
Identity Theft 148
Internet Fraud Schemes 152
 Summary 156 • *Review Questions* 157 • *Critical Thinking Exercises* 157 • *Endnotes* 157

Chapter 7 VIRUSES AND MALICIOUS CODE 159

Chapter Objectives 159
Introduction 159
The Language of Malicious Software (Malware) 163
Viruses and Other Malware 164
 History and Development 166
 Viruses 167
 Worms 170
 Trojan Horses 172
 Adware and Spyware 177
 Denial-of-Service Attacks 178
 Blended Threats 178
Extent of Viruses and Malicious Code Attacks 181
Virus Writers and Virus Experts 184
 Summary 189 • *Review Questions* 190 • *Critical Thinking Exercises* 190 • *Endnotes* 191

Chapter 8 SEX CRIMES, VICTIMIZATION, AND OBSCENITY ON THE WORLD WIDE WEB 194

Chapter Objectives 194

Introduction 194

Nature of Exploitation on the Internet 195

Online Victimization of Young People 197

Cyberbullying 200

Stalking via the World Wide Web 201

The Mechanisms of Traditional Stalking and
Cyberstalking 202

Characteristics of Stalkers and Their Victims 204

Legislation Targeting Stalking 206

Obscenity on the World Wide Web 207

Laws and Legislation Protecting Children Online 208

Pedophilia and Child Pornography 211

The “New” Child Pornographers 214

Moving from Pornography to Molestation 216

Child Molestation 219

The Problem of Child Sexual Abuse 221

Prostitution and the Sex Trade 223

Massage Parlors 226

Pornography and Webcams 227

Online Dating Fraud 229

Sex Tourism 231

The Process of Sex Tourism 234

*Issues in the Investigation of Internet Exploitation,
Cyberstalking, and Obscenity* 239

Law Enforcement Initiatives 239

Overlapping Jurisdictions and Duplication of Effort 240

Identification of Suspects 241

Issues with Evidence and Detection 241

Summary 242 • *Review Questions* 243 • *Critical
Thinking Exercises* 243 • *Endnotes* 243

Chapter 9 ANARCHY AND HATE ON THE WORLD WIDE WEB 250

Chapter Objectives 250

Introduction 250

Digital Hate 251

White Supremacy, Hate, and the Internet 252

Terrorist Extremists from the Left 253
 ELF and ALF 254
Domestic Terrorists in Cyberspace 256
 Dehumanize, Desensitize, and Demonize 256
 Internet Cartoons 257
Storage and Dissemination of Information 258
 Publishing Information on Potential Victims 261
 Fund-Raising 264
Terrorism, Intelligence Gathering, and the USA PATRIOT Act 265
 A Short History of Intelligence in the United States 265
 Domestic Intelligence and Policing 265
 Conflicting Roles 266
 Defining Intelligence 266
 U.S. Intelligence Weaknesses 267
The USA PATRIOT Act of 2001 268
 The Reauthorized PATRIOT Act of 2006 269
 The Reauthorized PATRIOT Act of 2011 269
 Constitutional Rights and the USA PATRIOT Act 269
 Summary 271 • *Review Questions* 271 • *Critical Thinking Exercises* 271 • *Endnotes* 271

Section III Controlling Cyber Crime: Legislation, Law Enforcement, and Investigation

Chapter 10 DIGITAL LAWS AND LEGISLATION 274

Chapter Objectives 274
Introduction 274
Search and Seizure Law for Digital Evidence 274
 Searches with Warrants 275
 Searches Without Warrants 277
Federal Statutes 280
 The Pen/Trap Statute 18 U.S.C. §3121-27 281
 The Wiretap Statute (Title III) 18 U.S.C. §2510-22 281
 Electronic Communications Privacy Act (ECPA)
 18 U.S.C. §§2701-11 282
USA PATRIOT Act/USA Freedom Act 284
 Communication Assistance for Law Enforcement Act 285
 Federal Criminal Statutes 285

<i>Admitting Evidence at Trial</i>	288
Authentication	288
Hearsay	289
The Best Evidence Rule	289
<i>Significant Court Cases</i>	290
Summary	292
Review Questions	292
Critical Thinking Exercises	293
Endnotes	293

Chapter 11 LAW ENFORCEMENT ROLES AND RESPONSES 294

<i>Chapter Objectives</i>	294
<i>Introduction</i>	294
<i>Federal Roles and Responses</i>	294
The Department of Justice	295
The Federal Bureau of Investigation	296
The National Security Agency	298
The Federal Trade Commission	298
The Postal Service	300
The Department of Energy	301
The Department of Homeland Security	302
U.S. Immigration and Customs Enforcement	303
The U.S. Secret Service	305
<i>State and Local Roles</i>	306
Critical Needs at the State and Local Levels of Enforcement	307
Summary	308
Review Questions	309
Critical Thinking Exercises	309
Endnotes	309

Chapter 12 THE INVESTIGATION OF COMPUTER-RELATED CRIME 311

<i>Chapter Objectives</i>	311
<i>Introduction</i>	311
<i>Investigator Roles and Responsibilities</i>	312
First Responders	312
Investigators	313
Digital Analysts	313
Corporate Security	313
Subject Matter Experts	314
Single-Location Crime Scenes	314
<i>Search Warrants and Electronic Evidence</i>	315
Computer Systems	316
External Storage Media	316

- Handheld Devices 316
- Other Electronic Devices 317
- Networking Equipment 317
- Executing the Search Warrant 317
- Examining the Crime Scene 319
- Multiple-Location and Network Crime Scenes 324
- Identifying Network Architectures 325
- Modeling Network Transactions 325
- Locating Evidence 326
- Key Information for Locating Network Trace Evidence 327
- Collecting Network Trace Evidence 329
- Presenting Digital Evidence at Trial 329*
 - The Hearsay Rule 330
 - Using Notes on the Witness Stand 330
 - Business Records 331
 - Presenting Best Evidence 331
 - Challenges to Forensic Analysis Strategies 332
 - Chain of Custody 333
 - Expert Testimony 334
 - Summary 334 • Review Questions 334 • Critical Thinking Exercises 334 • Endnotes 334*

Chapter 13 DIGITAL FORENSICS 337

- Chapter Objectives 337*
- Introduction 337*
- The Basic Process of Storage Forensics 338*
- Preparation for Forensic Analysis 338*
 - Acquisition of Data 339
 - Authentication of Data 340
 - Imaging of the Evidence Drive 341
 - Wiping the Analysis Drive 342
 - Restoring 343
- Forensic Analysis 346*
- The Forensic Analyst as Expert Witness 348*
- Computer Storage Systems 348*
 - Volatile Storage Systems 348
 - Nonvolatile Storage Systems 350
- File Systems 352*
 - FAT: File Allocation Table 352
 - NTFS: New Technology File System 353

<i>Application: Defragmenting a Disk</i>	355
<i>Evidence Recovery from Slack Space</i>	356
<i>Commercial Forensic Packages</i>	357
Extended Analysis and Searching	359
User Interface	359
Centralized Report Writing and Auditing	360
Validation and Support	360
<i>Summary</i>	361
<i>Review Questions</i>	361
<i>Critical Thinking Exercises</i>	361
<i>Endnotes</i>	362

Section IV The Future of Cyber Crime and Cyber Terrorism: Prevention and Trends

Chapter 14 INFORMATION SECURITY AND INFRASTRUCTURE PROTECTION 363

<i>Chapter Objectives</i>	363
<i>Introduction</i>	363
<i>Mastering the Technology and the Environment</i>	364
Personal Computers and Intruders	364
The Internet Explosion	365
<i>Principles of Risk Analysis</i>	366
Assessment and Evaluation	366
Threats	367
Cost-Effective Security	369
<i>Security Technologies</i>	369
<i>Backups</i>	369
Wireless Networks and Security	370
Firewalls	370
Limitations of Firewalls	373
Encryption	373
Password Discipline	376
<i>Security Vendor Technologies</i>	377
Home Users	378
<i>A Recap of the Evolution of Cyberattacks</i>	379
The Early Attacks (1980–2000)	381
New Century Attacks (2000 to Present)	383
<i>Summary</i>	386
<i>Review Questions</i>	387
<i>Critical Thinking Exercises</i>	387
<i>Endnotes</i>	387

Chapter 15 CYBER CRIME AND TERRORISM: A FORECAST OF TRENDS AND POLICY IMPLICATIONS 389

Chapter Objectives 389

The Impact of Cyber Crime 389

The Future of Cyber Crime and Cyber Terrorism: Forecasts 392

Forecast 1: Computer Crime Will Significantly Impact the Police and Courts 393

Forecast 2: Fraud and Identity Theft Will Be the Largest Computer Crime Problem Impacting the Police 397

Forecast 3: Virtual Crimes Will Continue to Rapidly Increase 399

Forecast 4: The Threat from Computer Hacker Groups Will Increase 400

Forecast 5: Organized Crime Groups Will Increasingly Adopt Computerization as a Criminal Instrument 401

Forecast 6: Terrorist Groups Will Increasingly Use Global Networking 407

Forecast 7: The Character of Espionage Will Continue to Broaden 409

Forecast 8: Criminals Will Increasingly Use Technology-Based Instruments and Methodologies to Carry Out Attacks 410

Summary 414 • Review Questions 415 • Critical Thinking Exercises 415 • Endnotes 415

Index 420

PREFACE

NEW TO THIS EDITION

Each chapter includes new pedagogical features to aid students and instructors in comprehending the complex subject matter discussed in each chapter. These include the following:

Chapter Objectives at the beginning of each chapter identifying the core elements students need to learn.

Boxes throughout the chapters highlight interesting topics that are relevant to the chapter subject matter. In many cases, these box items highlight case studies or examples of the subject matter under discussion in the chapter.

Quick Facts boxes provide unique tidbits of information related to the chapter topics and enhance student learning.

Summaries are organized around chapter objectives and provide a clear and concise discussion of each chapter subject matter.

Review Questions at the end of each chapter pose a series of questions to test students recall of the chapter information.

Critical Thinking Exercises at the end of each chapter require students to go further and think on the analytic level. Most of the exercises involve our research and discussion.

It is the authors' shared experience that there is little in the way of introductory textbooks covering the issues of cyber crime and cyber terrorism. We have found numerous books covering the details of the technical side of these issues and others that cover the legal side. However, there are very few works that attempt to provide a summary introduction and overview of these issues. In this vein, we have tried to approach the various topics covered in this book in a nontechnical and nonjargon style. Criminal justice students and practitioners will find the technical components quite readable and understandable. Computer science students and practitioners will find the criminal justice material bereft of jargon and written in a readable and understandable style as well. In sum, we specifically tried to bridge the gap between criminal justice knowledge and competence and the technical issues that arise during investigations of the crimes and acts we cover. It is our fervent hope that the techie will get as much out of this book as the criminal justice student.

Cyber Crime and Cyber Terrorism is written for students and practitioners with a beginning interest in studying cybercrimes, cyberterrorism, and information warfare committed using computer and computer network technology. The text is written in a user-friendly fashion, designed to be understandable by even the most technologically challenged reader. Issues addressed in the book include descriptions of the types of crimes and terrorist acts committed using computer technology; theories addressing hackers and other types of digital criminals; an overview of the legal strategies and tactics targeting this type of crime; and in-depth coverage of investigating and researching cyber crime, cyber terrorism, and information warfare. Readers will find a conversational tone to the writing designed to convey complex technical issues

as understandable concepts and issues. Additionally, upon completion of the text, readers should find themselves better prepared for further study into the growing problems of crime, terrorism, and information warfare being committed using computer technology.

The first section of the book covers the etiology of the cyber crime, cyber terrorism, and information warfare problem. The focus in this section is on the types of crimes, acts of terrorism and information warfare that are committed using computers, networks, and the Internet. Additionally, the reasons why offenders commit these types of crimes are examined in relation to current criminological theories and explanations. As the reader will find, applying criminological theory to cyber crime, cyberterrorism, and information warfare is a relatively recent endeavor. This section includes a chapter dedicated to hackers, and concludes with a new chapter focused on threats from sophisticated cybercriminal organizations. Chapter 1 provides an introduction and overview of computer crime. In particular, a categorization of computer crimes is presented. Chapter 2 provides a definition and overview of two key areas of concern in regard to computer crimes, specifically “information warfare” and “cyberterrorism.” Chapter 3 reviews criminological theories that can explain cyber crime. Since few theories have been applied directly to cyber crime, this chapter focuses on the criminological theories that can be applied to cyber crime. In other words, the theories explained in this chapter were developed to explain crime in general, not cyber crime specifically. Chapter 4 presents an overview of hackers. Finally, Chapter 5 focuses on new threats from sophisticated cybercriminal organizations operating in a worldwide venue.

The second section of the book details the various types of crimes that are committed using digital technology. Chapter 6 describes the ways in which the computer revolution has altered the techniques used to commit some of the most common white-collar offenses, including embezzlement, corporate espionage, money laundering, and fraud. In addition to these traditional white-collar offenses, the chapter provides an overview of the emerging area of identity theft crimes. Chapter 7 discusses viruses and other types of malicious code. The chapter takes an etiological approach with an emphasis on the description, examples, and categorical analysis of these various threats. Chapter 8 focuses on crimes against persons committed over the Internet, including exploitation, stalking, and obscenity. The chapter goes into detail on the etiology of these types of offenses and the offenders who commit them. Finally, Chapter 9 provides the reader with an introduction to the issues surrounding the growth of the Internet and the dissemination of extremist ideologies over the World Wide Web.

The third section of the book discusses the law, law enforcement, and investigation of cyber crime and cyber terrorism. Chapter 10 reviews the law and legislation as it applies to the collection of evidence and prosecution of cyber crime. First, search and seizure law for digital evidence is discussed, including searches with warrants and numerous searches without warrants. Second, the major federal statutes governing the collection of digital evidence, especially electronic surveillance law, are discussed along with federal criminal statutes that forbid certain types of computer crime. Third, issues related to the admission of digital evidence at trial, including authentication and hearsay, are reviewed. Finally, significant U.S. Supreme Court cases in the area of cyber crime are discussed. Chapter 11 then discusses the primary role of the many

federal agencies involved in detecting and enforcing computer crimes. The chapter continues with a discussion concerning the role of local agencies, with an emphasis on detailing the myriad of limitations associated with the local agencies' response to computer crime. Chapter 12 highlights the role that investigators play in the enforcement of cyber crime laws. Techniques for acquiring investigative information are presented in this chapter, along with conceptual tools that allow an investigator to communicate with computer experts. Finally, Chapter 13 reviews the collection of evidence and evidentiary issues related to cyber crime and terrorism.

The final section of the book covers prevention of cyber crime and terrorism and an overview of what the future might hold in these areas. Chapter 14 presents the problems associated with information security and infrastructure protection. The chapter discusses at length the problems and prospects presented by the USA PATRIOT Act as well as other laws designed to protect the information infrastructure. The concluding chapter of the book, Chapter 15, uses research developed by Carter and Katz as a framework to present an analysis of what the future of cyber crime, cyber terrorism, and information warfare might look like. The results of the research led to the development of eight forecasts for the future. Each prediction is accompanied by examples, trends, and analysis of what the future may hold.

CHAPTER 1 INTRODUCTION AND OVERVIEW OF CYBER CRIME AND CYBER TERRORISM

- Reorganization of text throughout the chapter
- Updated text, scholarship, and statistics on the costs of cybercrime
- Updated and new text on the classification of computer crime including extensive overviews of more recent computer crime classification schemes
- New material on recent major distributed denial-of-service attacks
- New material that underscores how the emergence of dangers regarding online victimization influenced popular culture during the dawn of the twenty-first century

CHAPTER 2 CYBER TERRORISM AND INFORMATION WARFARE

- New material on Low-Level Cyber war including discussion on *Stuxnet* and *Flame*
- Update material on Viruses and Worms with new material on the Global “WannaCry” malware infections of 2016–2017
- New box items throughout the chapter, including new material on the encryption of terrorist iPhones, recruitment videos from the Islamic State, and the burgeoning cyber threats stemming from hackers in North Korea

CHAPTER 3 THE CRIMINOLOGY OF COMPUTER CRIME

- Updated theoretical research relating to computer crime
- Significant update to routine activities theory
- Added new and modern box items throughout the chapter

CHAPTER 4 HACKERS

- New material on hacker subculture, the classification of hackers, and their views on the role of prosocial hacking in the protection of consumers and businesses in the fight against computer crime
- New material that describes and identifies the Internet of Things as a prime target of hackers, computer criminals, and cyber terrorists
- New material on hacktivism and the continued prominence of the hacktivist group Anonymous

CHAPTER 5 SOPHISTICATED CYBER CRIMINAL ORGANIZATIONS

- Updated statistical data throughout the chapter
- New case material on espionage
- New and more contemporary box items throughout the chapter
- Updated material on the “Deep Web” or Tor Network

CHAPTER 6 WHITE-COLLAR CRIMES

- Updated statistics and cases throughout the chapter
- New material on the problem of intellectual piracy and the origins of these crimes within American history
- New section on proposed strategies to mitigate identity theft and the concept of “fractured identities”

New text regarding the largely ignored phenomenon of Trade Based Money Laundering and how this crime threatens global international trade and commerce.

CHAPTER 7 VIRUSES AND MALICIOUS CODE

- New statistical information throughout the chapters
- Updated material on ransomware, viruses, worms, Trojan horses, and other malware
- New discussion on viruses and malicious code attacks, with updated information regarding attack trends, vulnerability trends, malicious code trends, and spam trends

CHAPTER 8 SEX CRIMES, VICTIMIZATION, AND OBSCENITY ON THE WORLD WIDE WEB

- New material on the role of social media as a facilitator of cyberstalking with detailed discussion of the threats posed by child predators using “Snapchat” and other online social media software platforms
- Updated case studies on cyberstalking victimization and updated statistical data throughout the chapter
- New material on the size and scope of child pornography on the Internet
- Updated material on laws and legislation protecting children online
- New material on prostitution and the sex trade online with discussions relating to the “Ashley Madison” scandal, unique online sites that review sex workers

(“providers”), massage parlors, new types of porn sites, such as webcams and streaming services that focus on a world-wide audience

- New material on online dating scams (ODS) and the tragedy of child sex trafficking

CHAPTER 9 ANARCHY AND HATE ON THE WORLD WIDE WEB

- Updated references and material throughout the chapter
- Expanded the section on “U.S. Intelligence Weaknesses”
- Added new material on the Dark Web; updating other material in Chapter 5 on the “Deep Web”
- Augments and distinguishes “Black Market” and other “Fake Trade” discussed in Chapters 6 and 15
- Added new material on WikiLeaks
- Added new material on “Fake News”

Updated discussion of right-wing hate groups

- Updated coverage of the Earth Liberation Front (ELF)
- New section on the Reauthorized PATRIOT Act (2011)

CHAPTER 10 DIGITAL LAWS AND LEGISLATION

- Significant revision and update of federal statutes applicable to cyber crime and cyber terrorism
- Added new and modern box items throughout the chapter
- New coverage of recent U.S. Supreme Court cases

CHAPTER 11 LAW ENFORCEMENT ROLES AND RESPONSES

- New material and box items throughout the chapter
- Revision and update of federal law enforcement agencies tasked with the investigation of cyber crime and cyber terrorism

CHAPTER 12 THE INVESTIGATION OF COMPUTER-RELATED CRIME

- Updated material and references throughout the chapter
- Added new commentary on the current state-of-the-domain of computer crime investigation
- Add new material that distinguishes “corporate security” from “private police”
- Augmented the landmark case *Frye v. United States*
- Augmented the landmark case *Daubert v. Merrell Dow Pharmaceutical* hence, updating “the *Daubert Test*”

CHAPTER 13 DIGITAL FORENSICS

- Minor update of this strong chapter focusing on the art and science of digital forensics with new material on digital forensics and mobile devices operating outside the Windows operating systems, such as cell phones, PDAs, and tablet devices

- Updated and new material on addressing mobile devices using Android OS, Apple's iOS, and Windows Mobile systems
- New material on commercial forensic packages used by law enforcement to analyze digital evidence for the arrest and prosecution of suspects
- New material on the use of technology in solving high-profile cases, including the infamous BTK (Blind-Torture-Kill) serial murder case in Kansas

CHAPTER 14 INFORMATION SECURITY AND INFRASTRUCTURE PROTECTION

- Minor update on this chapter focusing on information security and infrastructure protection
- Updated material on deep packet inspection (DPI), DPI firewalls, and RSA SecurID
- Updated section on the evolution of cyberattacks discussing how cyberattacks have become more sophisticated, polymorphic, and multi-vector in their approach to defeating security, presenting challenges to both the home user and the advanced cybersecurity professional

CHAPTER 15 CYBER CRIME AND TERRORISM: A FORECAST OF TRENDS AND POLICY IMPLICATIONS

- Updated statistical information and new research regarding patterns and trends in computer crime and cyber terrorism
- Added new material on big data trends, cyber threat trends, ransomware, electromagnetic pulse (EMP), the Faraday cage, drones, and artificial intelligence
- Updated new policy implications relating to the growing need for transparency in cybercrime investigations, particularly at the international level

INSTRUCTOR SUPPLEMENTS

Instructor's Manual with Test Bank. Includes content outlines for classroom discussion, teaching suggestions, and answers to selected end-of-chapter questions from the text. This also contains a Word document version of the test bank.

TestGen. This computerized test generation system gives you maximum flexibility in creating and administering tests on paper, electronically, or online. It provides state-of-the-art features for viewing and editing test bank questions, dragging a selected question into a test you are creating, and printing sleek, formatted tests in a variety of layouts. Select test items from test banks included with TestGen for quick test creation, or write your own questions from scratch. TestGen's random generator provides the option to display different text or calculated number values each time questions are used.

PowerPoint Presentations. Our presentations offer clear, straightforward outlines and notes to use for class lectures or study materials. Photos, illustrations, charts, and tables from the book are included in the presentations when applicable.

To access supplementary materials online, instructors need to request an instructor access code. Go to www.pearsonhighered.com/irc, where you can register for an instructor access code. Within 48 hours after registering, you will receive a confirming

email, including an instructor access code. Once you have received your code, go to the site and log on for full instructions on downloading the materials you wish to use.

ALTERNATE VERSIONS

eBooks. This text is also available in multiple eBook formats including Adobe Reader and CourseSmart. CourseSmart is an exciting new choice for students looking to save money. As an alternative to purchasing the printed textbook, students can purchase an electronic version of the same content. With a CourseSmart eTextbook, students can search the text, make notes online, print out reading assignments that incorporate lecture notes, and bookmark important passages for later review. For more information, or to purchase access to the CourseSmart eTextbook, visit www.coursesmart.com.

ACKNOWLEDGMENTS

First and foremost, we want to thank our wives, significant others, children, extended family, and friends for their support and patience with all of us as we compiled the fourth edition of this book. As is the case with many of these types of projects, we locked ourselves in our offices, missed family functions, worked during vacations, delayed retirement, and, in general, put out our loved ones while writing this book. Thank you for your love, patience, and support during these times.

Since our first edition, time has presented us with a new set of authors. Dr. D. Kall Loper has left academia to pursue a career as an expert in digital forensics, a field that he helped found and develop. And quite sadly, our good friend and colleague Dr. Tory J. Caeti was killed in a terrible traffic accident in August 2006 while serving as a consultant with Bob Taylor to the U.S. Department of State Anti-Terrorism Assistance Program in Kenya. Tory and Bob were to present material to the Kenyan National Police on digital terrorism. We miss Tory, and he will be forever in our thoughts. Dr. Tom Holt joined us for the second edition, but has subsequently moved on to focus his work on cybercrime. For this edition, we are fortunate to have the services of Mike Saylor, from the Cyber Defense Labs located on the campus of the University of Texas at Dallas as a valuable coauthor. Further, retired-FBI agent Bill Tafoya now professor, and a long-time friend and colleague, has also joined us as a coauthor for this edition. As the “father of police futuristics,” Bill was an early participant in defining and recognizing digital crime and digital terrorism as major threats to the future of our society. To a great extent, our understanding of the threats posed by cybercrime and digital terrorism were first discussed in the early years of the development of the *Society for Police Futurists International* (PFI), an organization started by Bill back in the early 1990s. Bob was one of the first educators to join Bill in presenting at the first “International Symposium on the Future of Law Enforcement” at the FBI Academy in Quantico (April, 1991) featuring Alvin Toffler as the keynote speaker. It was Bill’s hard work that began serious study on the future of policing, and Bob’s early paper presented at this conference that became the first outline for this book. We also express our sincere appreciation and a heartfelt “thank you” to several graduate students who have assisted us on this project. Specifically, Jennifer Davis-Lamm worked tirelessly for Dr. Taylor in researching various aspects of the cyberworld. Alexandra Jones assisted Dr. Fritsch in compiling recent theoretical research applicable to computer crime. Dr. Tafoya expresses a special thank you to Meredith Emigh and Gabriella Palmeri for their dedication unearthing the many current references used in this book, and pays a heartfelt homage to Dr. Richard H. Ward (deceased) for his vision and contribution to the discipline of Criminal Justice. Thanks too, to Bernard “Bud” Levin and Shawn Henry for their important insight into several chapters of this edition. We would like to thank Tamara Lynn, Fort Hays State University and Priscilla Montagna, Bunker Hill Community College for reviewing the fourth edition of this book. We would also like to thank the hundreds of students in our classes who have purchased and used previous editions of the book. Their suggestions on text revisions have been invaluable, and have been incorporated within this most recent edition of the text.

Finally, we would like to thank our editorial staff at Pearson. Gary Bauer’s guidance and assistance was instrumental in getting this book to press. We also want to thank all other Pearson staff involved in this project. They epitomize patience and understanding in dealing with slow academics who take forever to return phone calls and e-mails.