Foreword *xvii*
Acknowledgments *xix*
About the Author *xxi*

CHAPTER 1 INTRODUCTION 1

I. Introduction 2
II. Cyberspace and Criminal Behavior 3
III. Clarification of Terms 4
IV. Traditional Problems Associated with Computer Crime 5
a. Physicality and Jurisdictional Concerns 6
b. Perceived Insignificance, Stereotypes, and Incompetence 7
c. Prosecutorial Reluctance 8
d. Lack of Reporting 9
e. Lack of Resources 10
f. Jurisprudential Inconsistency 13
V. Extent of the Problem 14
VI. The Emergence of e-Cash: A New Problem for Law Enforcement 17
a. Prepaid Cards 17
b. Stored Value Cards 17
c. Mobile Payments 17
d. Internet Payment Services 17
e. Digital Precious Metals 18
VII. Conclusions 19

CHAPTER 2 COMPUTER TERMINOLOGY AND HISTORY 21

I. A Brief History of Computers 23
II. Computer Language 24
a. Understanding Data 25
III. Computer Hardware 25
a. Input Devices 25
b. Output Devices 26
c. Hard Drives and Other Mass Storage Devices 28
IV. Computer Software 29
V. Boot Sequence 29
VI. Operating System 29

VII. Alternatives to DOS: Popular Operating Systems 30
a. Microsoft Windows 30
b. Macintosh 32
c. UNIX 32
d. LINUX 32
e. Application Software 33
VIII. A Brief History of the Internet 35
IX. Network Language 36
a. Commonly Used Terms 36
X. Realms of the Cyberworld 38
XI. Data Bandwith Transfer Rates 39
XII. Categorizing Internet Communications 40
a. World Wide Web 40
b. Newsgroups/Bulletin Boards (Usenet Groups) 40
c. Internet Relay Chat 42
XIII. Future Issues and Conclusions 43

CHAPTER 3 TRADITIONAL COMPUTER CRIME: EARLY HACKERS AND THEFT OF COMPONENTS 46

I. Introduction 47
II. Traditional Problems 47
III. Recognizing and Defining Computer Crime 51
IV. Three Incidents 52
V. Phreakers: Yesterday's Hackers 56
a. What is Phreaking? 56
b. The War on Phreaking 57
VI. Hacking 60
a. Defining Hacking 60
b. Evolution in the Hacking Community 60
c. Contemporary Motivation 62
d. Hierarchy of Contemporary Cyber-Criminals 65
VII. Computers as Commodities 67
a. Hardware 67
VIII. Theft of Intellectual Property 69
a. Software 69
b. Film Piracy 70
IX. Conclusions 71

CHAPTER 4 CONTEMPORARY COMPUTER CRIME 74

I. Neo-Traditional Crime 75
a. Fraud and Fraudulent Instruments 76

II. Web-based Criminal Activity 76
a. Interference with Lawful Use of Computers 77
b. Malware 78
c. DoS (Denial of Service) and DDoS (Distributed Denial of Service) Attacks 82
d. Spam 84
e. Ransomware and the Kidnapping of Information 86
f. Theft of Information, Data Manipulation, and Web Encroachment 87
g. Dissemination of Contraband or Offensive Materials 93
h. Online Pharmacies 96
i. Online Gambling 99
j. Threatening and Harassing Communications 102
k. Online Fraud 105
l. Securities Fraud and Stock Manipulation 108
III. Ancillary Crimes 109
a. Money Laundering 109
IV. Conclusions 113

CHAPTER 5 IDENTITY THEFT AND IDENTITY FRAUD 117

I. Introduction 118
II. Typologies of Internet Theft/Fraud 120
a. Assumption of Identity 120
b. Theft for Employment and/or Border Entry 120
c. Criminal Record Identity Theft/Fraud 121
d. Virtual Identity Theft/Fraud 122
e. Credit Identity Theft/Fraud 122
III. Prevalence and Victimology 125
a. Victims and the Costs Associated with Victimization 127
b. Future Increases 128
IV. Physical Methods of Identity Theft 129
a. Mail Theft 129
b. Dumpster Diving 130
c. Theft of Computers 131
d. Bag Operations 132
e. Child Identity Theft 133
f. Insiders 133
g. Fraudulent or Fictitious Companies 133
h. Card Skimming and ATM Manipulation and Fraudulent Machines 135
V. Virtual or Internet Facilitated Methods 136
a. Phishing 137
b. Spyware—Generally 138

c. Trojans 138
d. Keyloggers and Password Stealers 139
VI. Crimes Facilitated by Identity Theft/Fraud 140
a. Insurance and Loan Fraud 141
b. Immigration Fraud and Border Crossings 142
VII. Conclusions and Recommendations 144

CHAPTER 6 TERRORISM AND ORGANIZED CRIME 148

I. Terrorism 149
a. Defining Terrorism 150
b. Classification Through Motivation 151
c. Roots of Contemporary Terrorism 153
d. Terrorism as a Stage 154
e. Cyberterrorism as a Concept 155
II. Terror Online 157
a. Propaganda, Information Dissemination, Recruiting, and Fundraising 157
b. Training 158
c. Research and Planning 159
d. Communication 160
e. Attack Mechanism 161
III. Terrorism and Crime 162
a. Criminal Activities 162
b. Criminalizing Terrorist Acts 163
c. Government Efforts 163
d. Conclusions 165
IV. Organized Crime 166
a. Defining Organized Crime 167
b. Distinguishing Organized Crime from CyberGangs 172
V. Organized Crime and Technology 173
a. Extortion 173
b. Cargo Heists and Armed Robbery 175
c. Fraud 175
d. Money Laundering 176
e. The Sex Trade 176
f. Confidence Scams 177
g. Fencing of Stolen Property 178
h. Data Piracy and Counterfeit Goods 180
i. Human Smuggling 180

VI. Confronting Contemporary Organized Crime 181
VII. The Intersection of Organized Crime and Terrorism 181

CHAPTER 7 AVENUES FOR PROSECUTION AND GOVERNMENT EFFORTS 185

I. Introduction 186
II. Traditional Statutes 187
III. The Evolution of Computer-Specific Statutes 187
a. Computer Fraud and Abuse Act of 1986 190
b. National Information Infrastructure Protection Act of 1996 (NIIPA) 191
IV. Evolving Child Pornography Statutes 193
V. Identity Theft and Financial Privacy Statutes 194
a. Identity Theft and Assumption Deterrence Act of 1998 (Appendix A) 194
b. The Financial Modernization Act of 1999 (Appendix B) 195
c. Fair and Accurate Credit Transactions Act of 2003 (FACTA) 195
d. Identity Theft Penalty Enhancement Act of 2004 197
e. Additional Efforts to Protect Personal Information 197
VI. Federally Funded Initiatives and Collaborations 198
VII. Law Enforcement Operations and Tools in the United States 201
a. Packet Sniffers and Key Loggers 201
b. Data Mining 203
c. Collaborations and Professional Associations 207
VIII. International Efforts 209
a. OECD and the Select Committee of Experts on Computer-Related Crime of the Council of Europe 209
b. Council of Europe's (CoE) Cybercrime Conventions 211
IX. Conclusions 214

CHAPTER 8 APPLYING THE FIRST AMENDMENT TO COMPUTER-RELATED CRIME 217

I. Introduction and General Principles 218
II. Obscenity in General 218
III. Traditional Notions of Decency 219
IV. Emerging Statutes and the Availability of Obscene Material to Children 220
V. Defining Child Pornography 222

VI. Applying Case Law to Child Pornography Statutes 222
VII. Technology-Specific Legislation—Contention in the Courts 225
VIII. Internet Gambling 229
IX. Conclusions 230

CHAPTER 9 THE FOURTH AMENDMENT AND OTHER LEGAL ISSUES 233

I. Introduction 234
II. History of the Fourth Amendment 235
III. The Expectation of Privacy and Electronic Surveillance 236
a. Types of Recognized Privacy 237
IV. Electronic Surveillance and the Right to Privacy 238
V. Private v. Public-Sector Searches 238
VI. Application of *Ortega* to E-Mail: The Cases of *Simons* and *Monroe* 239
VII. The Electronic communications Privacy Act and The Privacy Protection Act of 1980 240
a. Electronic Communications Privacy Act of 1986 240
b. Three Titles Under ECPA 241
c. Privacy Protection Act 243
d. Defining Interception Under ECPA and the PPA 245
e. Communications Assistance for Law Enforcement Act 245
f. Challenges to the CALEA 246
g. Applying the Wiretap Act to E-mail Interceptions—*U.S.* v. *Councilman* 246
VIII. The Patriot Act 247
a. Enhanced Presidential Authority 248
b. Electronic Surveillance and Criminal Investigations 249
c. National Security Letters and Other Fourth Amendment Issues 251
IX. Current State of Privacy 252
a. Challenges to Warranted Searches 252
b. Warrantless Searches 256
X. Other Legal Considerations 260
a. Vicinage 260
b. Undercover Techniques 260
c. Sentencing Guidelines 260
XI. Conclusions 261

CHAPTER 10 FORENSIC TERMINOLOGY AND DEVELOPING FORENSIC SCIENCE CAPABILITIES 264

I. Forensic Computer Science—An emerging discipline 266
II. Traditional Problems in Computer Investigations 266

a. Inadequate Resources 267
b. Lack of Communication and Cooperation Among Agencies 268
c. Over-reliance on Automated Programs and Self-Proclaimed Experts 268
d. Lack of Reporting 269
e. Evidence Corruption 269
III. Computer Forensic Science and Disk Structure 269
a. Disk Structure and Data Storage 271
b. Data Location 273
c. Partition Table 273
d. Data Management–Operating Instructions 274
e. Data Integrity 275
IV. Developing computer Forensic Science Capabilities 275
V. Minimum Housing Requirements 277
VI. Minimum Hardware Requirements 278
VII. Minimum Software Requirements 281
a. Data Preservation, Duplication, and Verification Tools 281
b. Data Recovery/Extraction Utilities 284
VIII. A Sampling of Popular Forensic Software 290
a. Maresware 290
b. Guidance Software 290
c. Ultimate Toolkit 291
d. Other Forensic Utilities 292
IX. Conclusions 293

CHAPTER 11 SEARCHING AND SEIZING COMPUTER-RELATED EVIDENCE 296

I. Traditional Problems Associated with Finding Digital Evidence 297
II. Pre-Search Activities 299
a. Warrant Preparation and Application 300
b. Plan Preparation and Personnel Gathering 303
c. Preparing a Toolkit 306
III. On-Scene Activities 309
a. Knock, Notice, and Document 309
b. Securing the Crime Scene 309
c. Determining the Need for Additional Assistance 310
d. Scene Processing 311
e. Locating Evidence 316
f. Seizure and Documentation of Evidence 317

g. Bagging and Tagging 319
h. Interviewing Witnesses 322
i. Scene Departure and Transportation of Evidence to Lab 322
IV. Conclusions 323

CHAPTER 12 PROCESSING OF EVIDENCE AND REPORT PREPARATION 325

I. Aspects of Data Analysis 326
a. Establish Forensically Sterile Conditions 327
b. Ensure Legitimacy and Capabilities of Analysis Tools 328
c. Physical Examination 329
d. Creation and Verification of Image 329
e. Jumping the CMOS Password 331
f. Short Circuiting the Chip 331
g. Pulling the Battery 331
h. Default Passwords 332
i. Social Engineering/Brute Force 332
j. Key Disks 332
k. Image Verification 332
l. Logical Examination 333
m. Restoration of Files 333
n. Listing of Files 334
o. Examine Unallocated Space for Data Remnants 335
p. Unlocking Files 336
q. Brute Force/Social Engineering 337
r. Program Defaults and Program-Specific Crackers 337
s. Examination of User Data Files 337
t. Piping of Evidence 338
u. Examination of Executable Programs 338
v. Evidence from Internet Activity 340
II. Non-Windows Operating Systems 341
a. Macintosh Operating System 341
b. Linux/Unix Operating Systems 342
III. PDA Forensics 343
IV. Report Preparation and Final Documentation 343
V. Conclusions 345

CHAPTER 13 CONCLUSIONS AND FUTURE ISSUES 349

I. Traditional Problems and Recommendations 350
a. Establishing Technology-Neutral Legislation 350
b. Establishing Accountability for Internet Users 351

c. Increasing Public Awareness and Research Capabilities 351
d. Increasing Inter-Agency and Intra-Departmental Cooperation 351
e. Developing Relationships Between Investigative Agencies and the Private Sector 352
f. Developing International Cooperation 352
g. Standardization of Accreditation or Expertise 353
h. Miscellaneous 354
II. Additional Approaches to Internet Crime 354
III. Future Trends and Emerging Concerns 357
a. Wireless Communications 357
b. Data Hiding: Remote Storage, Encryption, and the Like 358
c. Governing Decency and Virtual Pornography 360
d. Data Mining and Increased Interoperability 360
IV. Conclusions 362
References *365*
Index *375*