

Contents

List of Figures.....	xiv
List of Tables.....	xvi
List of Boxes.....	xvii
1 TECHNOLOGY AND CYBERCRIME	1
Introduction.....	2
The Importance of Technology in Modern Society.....	3
Technology as a Landscape for Crime.....	5
A Typology of Cybercrime.....	19
Overview of the Textbook.....	24
2 LAW ENFORCEMENT, PRIVACY, AND SECURITY IN DEALING WITH CYBERCRIME	35
Introduction.....	36
Role of Municipal Police Departments and Sheriff Offices in Investigating Cybercrime.....	38
State Agencies' Roles in Investigating Cybercrime.....	42
Federal Law Enforcement and Cybercrime.....	44
Civil Investigation and Application of Digital Evidence.....	45
Extralegal Agencies and Nongovernmental Organizations.....	49
International Enforcement Challenges.....	51
The Tension Between Security and Privacy.....	53

3	COMPUTER HACKERS AND HACKING	67
	Introduction	68
	Defining Computer Hacking	69
	Non-Nation-State Actors vs. Nation-State Actors.....	72
	The Human Aspects of the Hacker Subculture	75
	Hacking History	79
	The Contemporary Hacker Subculture	96
	Legal Frameworks to Prosecute Hacking.....	103
	Enforcing and Investigating Hacker Activity	110
4	MALWARE AND AUTOMATED COMPUTER ATTACKS	125
	Introduction	126
	The Basics of Malware.....	127
	Viruses, Trojans, and Worms	129
	Blended Threats and Ancillary Tools	139
	The Global Impact of Malware	145
	Hackers and Malware Writers.....	148
	Legal Challenges in Dealing with Malware	150
	Coordination and Management in Addressing Malware	154
5	DIGITAL PIRACY AND INTELLECTUAL PROPERTY THEFT	163
	Introduction	164
	What Is Intellectual Property?	167
	The Theft of Corporate IP Relative to Pirated Content.....	169
	Counterfeiting, E-Commerce, and Intellectual Property Theft	171
	The Evolution of Piracy and Pirating Methods.....	177
	The Subculture of Piracy	183
	The Evolution of Legislation to Deal with Intellectual Property Theft	185
	The Law Enforcement and Industry Response	194
6	ONLINE FRAUD	209
	Introduction	210
	Fraud and Computer-Mediated Communications	213
	Identity Theft.....	214
	Email-Based Scams.....	217
	Phishing Emails	221

Data Breaches and Identity Crimes	231
Identity Theft and Fraud Laws.....	233
Investigating and Regulating Fraud Globally.....	237
7 PORNOGRAPHY, IMAGE-BASED SEXUAL ABUSE, AND PROSTITUTION	253
Introduction	254
Pornography in the Digital Age.....	256
Image-Based Sexual Abuse.....	261
Prostitution and Sex Work.....	265
The Clients of Sex Workers.....	267
Dealing with Obscenity and Pornography Online.....	269
8 CHILD SEXUAL EXPLOITATION MATERIAL OFFENSES	287
Introduction	288
Defining and Differentiating Child Pornography and CSEM from Obscene Content.....	290
The Role of Technology in Child Sexual Exploitation Material.....	295
Explorations of the Pedophile Subculture Online	299
Typologies of CSEM Use and Consumption	302
The Legal Status of CSEM Around the Globe	309
Nonprofit Organization Efforts.....	315
Law Enforcement Efforts to Combat CSEM	317
9 CYBERBULLYING, ONLINE HARASSMENT, AND CYBERSTALKING	331
Introduction	332
Defining Cyberbullying	334
The Prevalence of Cyberbullying	336
Predictors of Bullying Online and Offline	338
Differentiating Online Harassment and Stalking	340
Rates of Harassment and Stalking	342
Understanding Victims' Experiences of Cyber-Violence	344
Reporting Online Bullying, Harassment, and Stalking	347
Regulating Cyberbullying.....	349
Regulating Online Harassment and Stalking	352
Enforcing Cyber-Violence Laws and Norms.....	356

10 ONLINE EXTREMISM AND CYBERTERROR	371
Introduction	372
Defining Terror, Hacktivism, and Cyberterror.....	374
The Use of the Internet in the Indoctrination and Recruitment of Extremist Groups	380
Electronic Attacks by Extremist Groups.....	390
The Radical Far Right Online	393
The E-Jihad.....	396
Legislating Extremism and Cyberterror.....	399
Investigating and Securing Cyberspace from the Threat of Terror	403
11 CYBERWARFARE AND INFORMATION OPERATIONS ONLINE	417
Introduction	418
Defining Warfare and Cyberwarfare.....	420
The Role of Nation-State Actors in Cyberattacks	425
Offensive and Defensive Cyber-Operations.....	427
Information Warfare Campaigns Online.....	433
Securing Cyberspace from the Threat of Cyberwar.....	439
12 ILLICIT MARKET OPERATIONS ONLINE	451
Introduction	452
Differentiating Physical and Virtual Markets.....	453
The Development and Evolution of Illicit Markets Online	460
Contextualizing the Practices of Illicit Market Participants.....	466
Debunking Claims Related to Illicit Market Operations.....	469
13 CYBERCRIME AND CRIMINOLOGICAL THEORIES	479
Introduction	480
Applying Criminological Theories to Cybercrime Offending.....	482
Applying Criminological Theories to Cybercrime Victimization.....	502
Need for New Cyberspace Theories?	511
14 EVOLUTION OF DIGITAL FORENSICS	533
Introduction	534
From Computer Forensics to Digital Forensics.....	535
Stages of Digital Forensic Investigation	550

The Role of Digital Evidence	555
Types of Hardware, Peripherals, and Electronic Evidence	558
Evidence Integrity.....	564
15 ACQUISITION AND EXAMINATION OF FORENSIC EVIDENCE	575
Introduction	576
Data Preservation.....	577
Digital Forensic Imaging Tools	583
Uncovering Digital Evidence.....	593
Data Analysis.....	605
Reporting of Findings	608
16 LEGAL CHALLENGES IN DIGITAL FORENSIC INVESTIGATIONS	619
Introduction	620
Constitutional Issues in Digital Investigations	622
Admissibility of Evidence in Court.....	648
Admissibility of Digital Forensics as Expert Testimony.....	659
17 THE FUTURE OF CYBERCRIME, TERROR, AND POLICY	671
Introduction	672
Considering the Future of Cybercrime	674
How Technicways Will Shift with New Technologies.....	677
Social Movements, Technology, and Social Change.....	680
Need for New Cyber Criminological Theories?	684
Shifting Enforcement Strategies in the Age of the Internet.....	686
Considering the Future of Forensics	690
The Challenge to Policy-Makers Globally	692
Glossary.....	703
Index	759