

• Detailed Contents •

Preface	xv
Acknowledgments	xix
Chapter 1 • Cyberspace, the Internet, and the World Wide Web	1
• CASE STUDY 1.1: The Dark Side of the Internet	3
The Beginning of the Internet and Cyberspace	4
• CASE STUDY 1.2: The First-Ever Web Server	5
The Purpose of the Internet	6
Operations and Management Aspect	6
Social Aspect	7
Commercialization Aspect	7
• LEGAL ISSUE 1.1: Napster: The First File Sharing Program	8
Vulnerabilities of the Internet	8
What Is a Vulnerability?	9
<i>Time and Space</i>	9
<i>Lack of Barriers to Entry</i>	9
<i>Anonymity/Identity</i>	10
<i>Asymmetries of Cyberspace</i>	11
<i>1s and 0s</i>	12
• THINK ABOUT IT 1.1	12
What Distinguishes Cyberspace, the Internet, and the World Wide Web?	12
• LEGAL ISSUE 1.2: Is It a Crime to Link to Infringed/Illegal Content?	14
• WHAT CAN YOU DO? PREPARING FOR THE JOB OF THE FUTURE:	14
Careers in Cybercrime and Cybersecurity	14
➤ Summary	15
➤ Key Terms	15
➤ Discussion Questions	16
➤ Internet Resources	16
➤ Further Reading	16
Chapter 2 • What Is Cybersecurity?	17
• THINK ABOUT IT 2.1: What Is Cybersecurity and Why Is It Important?	18
Origins and Nature of Cybersecurity	19
• THINK ABOUT IT 2.2: War Games	20
Definitions	20
Definition of Cybersecurity	21
• CASE STUDY 2.1: The Original Hacker: Kevin Mitnick	23

Cybersecurity Policies	24
• CASE STUDY 2.2: FusionX	25
Overview of Cyberspace Intrusions	25
Network-Based Attacks	26
• CASE STUDY 2.3: Vitek Boden	27
Wireless Attacks	27
Man-in-the-Middle Attacks	28
• LEGAL ISSUE 2.1: Hacking . . . With a Body Count?	30
➤ Securing Your Wi-Fi in a Wireless World	31
➤ Summary	31
➤ Key Terms	32
➤ Discussion Questions	32
➤ Internet Resources	32
➤ Further Reading	32
➤ Appendix 2A	34
Chapter 3 • Threat Factors—Computers as Targets	37
• CASE STUDY 3.1: The Top 10 Data Breaches	38
The Evolution of Cybercrime	39
Phases of Convergence	39
Main Targets in Information Technology	39
• THINK ABOUT IT 3.1: Russian Cyberspies and the 2016 Presidential Election	40
Computers as a Target	42
Threats to Mobile Devices	43
• CASE STUDY 3.2: Democratic Election Campaign—Hackers Steal Campaign Information	44
Viruses, Worms, and Trojan Horses	44
Viruses	44
<i>Risks Created by Viruses</i>	47
<i>Risks to Mobile Devices</i>	48
• CASE STUDY 3.3: The First Viruses	50
Worms	50
• LEGAL ISSUE 3.1: The Morris Worm	51
<i>Risks Created by Worms</i>	52
Trojan Horses	53
<i>Risks Created by Trojan Horses</i>	54
• CASE STUDY 3.4: The U.S. Government Firewall Virus	55
Preventing Malware Intrusions	56
Antivirus Software	56
Firewall	57
Thoughtful User Behavior	57
• THINK ABOUT IT 3.2: Pokémon Go, Cybercriminals, and Cybersecurity	58
Encryption	58
• WHAT CAN YOU DO? ENCRYPTING YOUR COMPUTER	60
Future Developments	61

➤ Summary	61
➤ Key Terms	62
➤ Discussion Questions	62
➤ Internet Resources	62
➤ Further Reading	63

Chapter 4 • Threats to Cybersecurity by Criminals and Organized Crime 65

Cybercrimes	65
• NORSE ATTACK MAP	66
Why Do People Commit Cybercrimes?	66
Fraud and Financial Crimes	66
Consumer Crimes	66
<i>Identity Theft</i>	66
• WHAT CAN YOU DO? COUNTER MEASURES—PROTECTING YOUR IDENTITY	67
<i>Phishing Scams</i>	68
• CASE STUDY 4.1: Advance Fee Fraud—Nigerian Phishing Scam	70
• WHAT CAN YOU DO? COUNTERMEASURES TO PHISHING SCAMS	71
<i>Spam</i>	71
Banks and Financial Corporations	72
<i>Botnets</i>	72
<i>Logic Bombs</i>	73
<i>Viruses</i>	74
Internet-Initiated Sexual Offending and Exploitation	74
<i>Internet-Initiated Sexual Offending</i>	74
<i>Child Pornography</i>	75
• LEGAL ISSUE 4.1	77
<i>Snuff Films</i>	77
<i>Trafficking in Persons</i>	78
• THINK ABOUT IT 4.1: Countermeasures to Child Pornography—Operation Predator and Operation Globe	80
Mail-Order Brides	80
Cyberbullying	82
Cyberharassment	82
Cyberstalking	83
Online Denigration	84
Online Impersonation	84
Online Exclusion	84
Tools Used	84
<i>Social Media</i>	84
<i>YouTube</i>	85
Gaming	85
• CASE STUDY 4.2: Cyberbullying and Suicide	86
➤ Summary	87
➤ Key Terms	87
➤ Discussion Questions	87

➤ Internet Resources	88
➤ Further Reading	88
Chapter 5 • Threats to Cybersecurity by Hacktivists and Nation-States	89
• THINK ABOUT IT 5.1: Cyberattacks on the Power Grid	89
Threats to Cybersecurity	90
Local Threats	91
<i>Types of Insider Threats</i>	91
• LEGAL ISSUE 5.1: Corporate Espionage—Inside Security Breach at AMSC	93
National Threats	93
<i>Displeasure With the Government</i>	93
<i>Specific Causes</i>	94
• CASE STUDY 5.1: Edward Snowden—Going Dark	95
International Threats	95
• CASE STUDY 5.2: The Hacked Company Graveyard	97
• CASE STUDY 5.3: Inside the Office of Personnel Management Cyber Attack	99
• THINK ABOUT IT 5.2: Setting Up a Cyberheist	99
Hackers	100
<i>Evolution of the Term Hacker</i>	100
<i>The Hacker Community</i>	101
<i>“Black Hats,” “White Hats,” and “Gray Hats”</i>	102
<i>The Internet and the Transparent Citizen</i>	103
• LEGAL ISSUE 5.2: Privacy Versus Security	104
What Motivates Hackers?	104
• THINK ABOUT IT 5.3: Why Do People Have a House Alarm?	105
• LEGAL ISSUE 5.3: California’s Breach Notification Statute	107
➤ Summary	108
➤ Key Terms	108
➤ Discussion Questions	108
➤ Internet Resources	109
➤ Further Reading	109
Chapter 6 • National Security: Cyberwarfare and Cyberespionage	111
Cyberwarfare	113
Nation-State Threats by Region	113
Syrian Electronic Army	114
Chinese	114
Russia and Eastern Europe	115
• CASE STUDY 6.1: North Korea and the Sony Hack	116
Cyberespionage	116
<i>Economic Cyberespionage</i>	119
• LEGAL ISSUE 6.1: Misappropriation of Information or Espionage?	120
<i>Political Cyberespionage</i>	120
<i>The Threat of Insiders</i>	120

• CASE STUDY 6.2: GhostNet	121
• LEGAL ISSUE 6.2: The Fourth Amendment	121
Cyberintelligence	122
Cybersabotage	122
<i>Denial-of-Service Attacks</i>	124
• CASE STUDY 6.3: Rutgers State University—DDoS Attack	124
➤ Summary	125
➤ Key Terms	125
➤ Discussion Questions	125
➤ Internet Resources	126
➤ Further Reading	126
Chapter 7 • Cyberterrorism	127
• THINK ABOUT IT 7.1: The Future of Terrorist Attacks	127
Cyberterrorism Defined	128
The Role of the Media	130
• CASE STUDY 7.1: Defining Cyberterrorism Within the Academic Context	130
• LEGAL ISSUE 7.1: The Role of Violence	132
Evolution of the Threat	133
Technology Use by Extremists	134
Al-Qaeda	134
Boko Haram	134
The Islamic State (also known as ISIS/ISIL/Daesh)	134
Targets of Cyberterrorism	135
Probable Versus Possible	135
• CASE STUDY 7.2: The 2003 New York City Blackout	136
Vulnerability of Critical Infrastructures	137
Risk Management	138
<i>Risk = Threat × Asset × Vulnerability</i>	138
<i>Asset Value Assessment</i>	138
<i>Threat Assessment</i>	139
<i>Vulnerability Assessment</i>	139
Damage Potential	139
• THINK ABOUT IT 7.2: Critical Infrastructure Risk Assessment	140
➤ Summary	141
➤ Key Terms	141
➤ Discussion Questions	141
➤ Internet Resources	142
➤ Further Reading	142
Chapter 8 • An Evolving Threat: The Deep Web	143
• THINK ABOUT IT 8.1: Surface Web and Deep Web	144
The Surface Web	144
The Deep Web and Darknets	145
Accessibility	146

The Onion Router	147
Products Available	149
• THINK ABOUT IT 8.2: Black Market Blood	149
<i>The Hidden Wiki</i>	150
<i>The Silk Road</i>	150
• THINK ABOUT IT 8.3: Dread Pirate Roberts and the Silk Road	152
Payment: Cryptocurrency	153
Bitcoins (BTC or ₿)	153
Dash	154
Law Enforcement Response	154
Operation Onymous	155
Anonymous and "Vigilante Justice"	155
• THINK ABOUT IT 8.4: Online Vigilante Justice	156
Terrorist Presence on the Deep and Dark Web	157
• CASE STUDY 8.1: ISIS and the Threat of the Darknet	158
Legal Issues	158
• LEGAL ISSUE 8.1: Anonymity and the First Amendment	160
➤ Summary	160
➤ Key Terms	161
➤ Discussion Questions	161
➤ Internet Resources	161
➤ Court Cases	161
Chapter 9 • Cybersecurity Operations	163
Theoretical Operations	163
Routine Activity Theory	164
<i>Role of Guardianship</i>	164
Learning Theory	165
Differential Association Theory	165
Subculture Theory	166
The Hacker Subculture	167
DEF CON Convention	168
• CASE STUDY 9.1: The Hacker's Manifesto	168
Law Enforcement Operations	169
Federal Agencies	169
<i>National Security Agency (NSA)</i>	169
<i>Department of Homeland Security</i>	170
<i>Federal Bureau of Investigation</i>	170
Local Agencies	171
Cyberterrorism Prevention Training	172
Private-Sector Collaboration	173
• CASE STUDY 9.2: One Hat, Two Hat, White Hat, Red Hat . . .	174
Interagency Operations	175
Target Hardening	176
Firewalls	176
SCADA Systems	176

Honeypots, Nets, and Tokens	176
• THINK ABOUT IT 9.1: The Honeynet Project	178
• LEGAL ISSUE 9.1: The Fourth Amendment	178
➤ Summary	179
➤ Key Terms	179
➤ Discussion Questions	179
➤ Internet Resources	180
➤ Further Reading	180
Chapter 10 • Cybersecurity Policies and Legal Issues	181
• THINK ABOUT IT 10.1: Mirai: A Shot Across the Bow— Distributed Denial-of-Service Attack	182
• CASE STUDY 10.1: A Holistic Approach to Cybersecurity	183
National Cybersecurity Policies	184
Comprehensive National Cybersecurity Initiative, 2008	184
Cybersecurity Workforce Act of 2014	185
• CASE STUDY 10.2: Ransomware—California Hospital Pays \$17,000	186
National Cybersecurity and Critical Infrastructure Protection Act of 2014	186
• THINK ABOUT IT 10.2: Ransomware	187
International Cybersecurity Policies	188
• LEGAL ISSUE 10.1: The Cyberwars in the Middle East	189
Legal Issues	190
Civil Rights	190
Security Versus Privacy	191
USA PATRIOT Act	192
• LEGAL ISSUE 10.2: <i>United States v. Warshak</i>	193
Jurisdictional Issues	194
<i>Universal Jurisdiction</i>	194
<i>Budapest Convention on Cybersecurity (2001)</i>	195
<i>Network and Information Security Directive (2016)</i>	195
Issues With Enforcement/Jurisdiction	195
• LEGAL ISSUE 10.3: Law of the Sea	197
➤ Summary	198
➤ Key Term	198
➤ Discussion Questions	198
➤ Internet Resources	199
➤ Further Reading	199
Chapter 11 • What the Future Holds	201
• THINK ABOUT IT 11.1: Pizzeria “Comet Ping Pong” Is a Child Pornography Ring	201
Data Is the New Oil	202
Data Mining	202
Dataveillance	203

Google	204
Manipulation of Data: The Screen Is Always Right	206
Censorship	207
Spoofing	208
E-Mail Spoofing	209
Stock Market Spoofing	209
• CASE STUDY 11.1: High-Frequency Trading—"Flash Boys"	210
Emerging Threats	210
Internet of Things	210
Real-Time Location Services	211
Vulnerable Targets	212
GPS Jammers and Spoofers	212
Naval System	213
Aircraft	214
Army Bases	214
Women's Shelters	214
• THINK ABOUT IT 11.2: Dangerous Criminal or Researcher Trying to Save Lives?	215
• LEGAL ISSUE 11.1: Health Care Records Are Worth Millions	216
Potential/Emerging Perpetrators	216
Man in the Middle	216
Swatting	217
Crime Inc.	218
The Organizational Structure of Crime Inc.	218
➤ Summary	219
➤ Key Terms	219
➤ Discussion Questions	220
➤ Internet Resources	220
➤ Further Reading	220
Appendix: Cybersecurity-Related Organizations	221
Glossary	225
Notes	231
Index	255
About the Authors	273