

Table of Contents

	Preface and Acknowledgement	IX
	Acknowledgement.....	XI
	Dedication	XI
	Foreword	XIII
Chapter 1	Cybercrime and Cybersecurity Issues: Stakes and Challenges for the 21st Century	1
	1.1 Understanding the context.....	1
	1.2 The risks and the needs	8
	1.3 Supporting and developing the digital society	14
	1.4 Cybersecurity expectations	16
	1.5 Summary	20
	1.6 Exercises.....	20
Chapter 2	Cyberspace and Internet: a New Paradigm for Crime and Conflicts.....	23
	2.1 Understanding the context.....	23
	2.2 The characteristics of cybercrimes	28
	2.3 The Internet: empowering criminals	36
	2.4 Summary in 10 tips	52
	2.5 Exercises.....	54

Chapter 3	Cybercrimes Against Persons.....	55
	3.1 Understanding the context.....	55
	3.2 Affecting people's dignity and integrity.....	55
	3.3 Swindles and frauds over the Internet	64
	3.4 Identity crimes.....	74
	3.5 Privacy related offences	81
	3.6 Technological innovation and responsibility.....	86
	3.7 Summary	87
	3.8 Exercices	89
Chapter 4	Cybercrimes Against Assets.....	91
	4.1 Understanding the context.....	91
	4.2 The typology of the main crimes against assets	100
	4.3 Frauds and scams	107
	4.4 Summary of offences from a technological perspective	119
	4.5 Case study from the FBI	121
	4.6 Exercises.....	124
Chapter 5	Cybercrimes Against States	125
	5.1 Understanding the context.....	125
	5.2 Examples of cybercriminal activities that can affect states.....	127
	5.3 Cyberthreats against states.....	135
	5.4 Summary	140
	5.5 Exercises.....	141
Chapter 6	Cyberconflicts, Cyberwars and Cyberpower	143
	6.1 Understanding the context.....	143
	6.2 From cybercrime to cyberwar	149
	6.3 Cyberwar.....	156
	6.4 Information war	160
	6.5 Cyberterrorism: a particular kind of cyberconflict.....	168
	6.6 Cybercrime or cyber conflict?	173
	6.7 Summary	175
	6.8 Exercises.....	176
Chapter 7	Understanding Cybercriminals	177
	7.1 Understanding the context.....	177
	7.2 Towards a classification of cybercriminals	178
	7.3 About hacking and hackers.....	186
	7.4 Hackers' conventions, contests, and school	192
	7.5 Portraits of hackers.....	194
	7.6 Summary	202
	7.7 Exercices	203

Chapter 8	The Cybercriminal's Toolkits.....	205
8.1	Understanding the context.....	205
8.2	Fundamental principles and constant factors of cyberattacks	206
8.3	Spam and phishing: assets for criminals.....	210
8.4	Means of obtaining connection parameters to access systems.....	216
8.5	Some basic attacks.....	221
8.6	The black market of cybercriminality	239
8.7	Summary	250
8.8	Exercises.....	252
Chapter 9	The Fight Against Cybercrime	255
9.1	Understanding the context.....	255
9.2	Strengthening legislation is not enough.....	257
9.3	An integrative approach and a global strategy	262
9.4	The principal challenges in combating cybercrime at the international level.....	275
9.5	Some privacy related considerations	285
9.6	Summary	290
9.7	Exercises.....	292
Chapter 10	The Global Cybercrime Ecosystem and Cybercriminal Investigation.....	295
10.1	Understanding the context.....	295
10.2	The place of the struggle against cybercriminality in the cybercriminal ecosystem	301
10.3	Cybercriminal investigation	302
10.4	The idea of digital evidence	304
10.5	Fundamental concepts in computer crime investigation	312
10.6	Investigating computer crimes within organizations.....	317
10.7	Summary	327
10.8	Exercises.....	328
Chapter 11	A Global Approach to Cybersecurity.....	329
11.1	Understanding the context.....	329
11.2	The evolution of information security.....	331
11.3	Avoiding the cybersecurity gap.....	336
11.4	A systemic approach to cybersecurity	343
11.5	Summary	352
11.6	Exercises.....	354
Chapter 12	Cybersecurity Governance and Security Measures	357
12.1	Understanding the context.....	357
12.2	Managing the risks.....	362

12.3	Defining a security policy.....	370
12.4	Understanding ICT security from a technical point of view	376
12.5	A functional approach to generic security tools	381
12.6	Cyber security as a competitive advantage.....	396
12.7	Summary	397
12.8	Exercises.....	399

Chapter 13	Cyberconflict & Cybercrime:	
	Prospects for a Global Response	401
13.1	Understanding the context.....	401
13.2	Some complex and global questions.....	402
13.3	For an international treaty: a contribution to stability in cyberspace	407
13.4	Connecting the world responsibly	417
13.4	Summary	422
13.5	Exercises.....	423
	 Glossary of main cybercrime and cybersecurity related terms	 425
	 Annex: Some references	 443
	 Index	 447