

Contents

1	The Global Cybercrime Industry and Its Structure:	
	Relevant Actors, Motivations, Threats, and Countermeasures	1
1.1	The Rapidly Rising Global Cybercrime Industry	1
1.1.1	Cybercrime: Definitional Issues	3
1.2	Economic, Social, and Political Impacts of Cybercrimes	4
1.2.1	Social Impacts	5
1.2.2	Political and National Security Impacts	6
1.3	Methodological, Conceptual, Logical, and Statistical Problems in Estimating Cybercrime	7
1.4	Trends in Cybercrimes	9
1.4.1	Social Engineering Skills	10
1.5	Types and Classification of Cybercrimes	10
1.5.1	Targeted vs. Opportunistic Attacks	11
1.5.2	Predatory Cybercrimes vs. Market-Based Cybercrimes	13
1.6	Relevant Actors Associated with Cybercrimes	14
1.6.1	Cyber-Criminals, Cyber-Terrorists, and State Actors Involved in Cyberattacks	14
1.6.2	Cybercrime Victims and Targets	15
1.6.3	Regulators and Governments	16
1.6.4	Supranational Organizations	18
1.6.5	Voluntary, Nonprofit, and Non-government Organizations	20
1.7	Motivations Associated with Cybercrimes	21
1.7.1	Intrinsic Motivation	22
1.7.2	Extrinsic Motivation	23
1.7.3	Combination of Motivations	23
1.7.4	Trend Toward Extrinsically Motivated Crimes	23
1.8	Businesses' Countermeasures to Combat Cybercrimes	24
1.9	Concluding Comments	25
	Notes	26
	References	27

2	Simple Economics of Cybercrime and the Vicious Circle	35
2.1	Introduction	35
2.2	Economic Factors Affecting Crimes	36
2.2.1	Target Attractiveness	36
2.2.2	Economic Conditions Facing an Offender	37
2.3	Economic Processes Motivating a Cyber-Criminal's Behavior	37
2.3.1	Selection of Targets	38
2.4	Structure of Cybercrimes: The Vicious Circle	38
2.4.1	The Cybercrime Market	39
2.4.2	Law-Enforcement Agencies	40
2.4.3	Cyber-Criminals	41
2.4.4	Cybercrime Victims	42
2.4.5	Inter-jurisdictional Issues	44
2.5	A Cyber-Criminal's Cost-Benefit Calculus	45
2.5.1	The Benefit Side	46
2.5.2	The Cost Side	46
2.6	Concluding Comments	49
Note		50
References		50
3	An Institutional Perspective on Cybercrimes	57
3.1	Introduction	57
3.2	Institutional Theory	58
3.2.1	Regulative Institutions	58
3.2.2	Normative Institutions	59
3.2.3	Cognitive Institutions	59
3.2.4	Interrelationships Among Institutional Pillars	59
3.2.5	Exogenous and Endogenous Institutions	60
3.2.6	Neoinstitutionalism	60
3.2.7	Institutions Operating at Various Levels	61
3.3	Viewing Cybercrimes Through the Prism of the Literature on Institutions	62
3.3.1	Formal Constraints and Crimes	62
3.3.2	Informal Constraints and Crimes	62
3.4	Institutions at Different Levels Influencing Cyberattacks	63
3.4.1	International-Level Institutions and Cyberattacks	63
3.4.2	National-Level Institutions and Cyberattacks	64
3.4.3	Institutions at the Industry/Professional/Inter-organizational Level and Cyberattacks	66
3.4.4	Institutions at the Network Level and Cyberattacks	67
3.4.5	Institutions at the Intra-organizational Level and Cyberattacks	68
3.5	Concluding Comments	69
Notes		69
References		69

4	Increasing Returns and Externality in Cybercrimes	75
4.1	Introduction	75
4.2	Increasing Returns and Feedback Loops in Cybercrimes	76
4.2.1	Economic Feedback	76
4.2.2	Sociopolitical Feedbacks	77
4.2.3	Cognitive Feedback	78
4.3	Mechanisms Associated with Externality in Cybercrimes	78
4.3.1	Path Dependence and Externality	78
4.4	Inefficiency and Congestion in the Law-Enforcement System	81
4.5	Diffusion of Cybercrime Know-How and Technology	84
4.6	Increased Predisposition Toward Cybercrime	86
4.7	Concluding Comments	88
	Notes	88
	References	89
5	Institutional Field Evolved Around Cybercrimes	95
5.1	Introduction	95
5.2	The Theoretical Framework: Institutional Field	97
5.3	Institutional Field Change Mechanisms	100
5.3.1	Exogenous Shocks	100
5.3.2	Changes in Organizational Logics	101
5.3.3	Gradual Change in Field Structure	101
5.4	Institutional Evolution	102
5.4.1	Regulative Pillar Related to Cybercrime	102
5.4.2	Normative and Cognitive Pillars Related to Cybercrime	102
5.5	Institutional Field Formed Around Cybercrimes	103
5.5.1	The Formation of Regulative Pillar Around Cybercrime	103
5.5.2	The Formation of Normative Pillar Around Cybercrime	107
5.5.3	The Formation of Cognitive Pillar Around Cybercrime	109
5.6	Concluding Comments	110
	Notes	111
	References	112
6	Information and Communications Technologies, Cyberattacks, and Strategic Asymmetry	119
6.1	Introduction	119
6.2	Strategic Asymmetry and ICTs	123
6.3	Institutional and Organizational Factors Linked with Positive and Negative Asymmetries	126
6.3.1	Institutions, ICTs, and National Security	127
6.3.2	Ability to Create Positive Asymmetry and Minimize Vulnerabilities of Negative Asymmetry	131

6.4	Concluding Comments	133
	Notes	134
	References	134
7	Global Heterogeneity in the Pattern of the Cybercrime Industry . .	139
7.1	Introduction	139
7.2	The Global Digital Security Threat: A Brief Survey	140
7.3	Pattern of the Global Cyber-War and Crime: A Proposed Model	142
7.3.1	Characteristics of the Source Nation	142
7.3.2	Profile of Target Organization	154
7.4	Concluding Comments	156
	Notes	158
	References	159
8	Structure of Cybercrime in Developing Economies	165
8.1	Introduction	165
8.2	A Brief Survey of Cybercrimes in Developing Countries	168
8.2.1	Broadband Connections and Increase in Cybercrimes	169
8.3	Economic and Institutional Factors Related to Cybercrimes in Developing Economies	170
8.3.1	Formal Institutions: Permissiveness of Regulatory Regimes	170
8.3.2	Informal Institutions: Social Legitimacy and Cybercrime	172
8.3.3	Defense Mechanisms Against Cybercrimes	173
8.3.4	Concentration of Crimes	175
8.3.5	Path Dependence Externalities Generated by Conventional Crimes and Cybercrimes	176
8.3.6	Cybercrime Business Models in Developing Economies	177
8.3.7	Motivations Behind Cybercrimes	178
8.4	Concluding Comments	179
	Notes	183
	References	183
9	Institutional and Economic Foundations of Cybercrime Business Models	189
9.1	Criminal Entrepreneurship and Business Models in the Digital World	189
9.2	Business Model and Their Components: Applying in the Context of the Cybercrime Industry	191
9.2.1	Configuration of Competencies	191
9.2.2	Company and Firm Boundaries	194
9.3	The Internet and Organized Crime Groups' Reinvention of Business Models	196

9.4	Cybercrime Operators and Legitimate Businesses: Selling Concept vs. Marketing Concept	197
9.4.1	Marketing Mix of C2C vs. C2V Operators	198
9.5	Quality Uncertainty, Technological Information, and Market Information	198
9.5.1	The Problem of Quality Uncertainty in an e-Marketplace	198
9.5.2	Technological Information and Market Information in an e-Marketplace	199
9.6	Development of Dynamic Capabilities	200
9.7	Concluding Comments	201
	References	202
10	The Global Click Fraud Industry	207
10.1	Introduction	207
10.2	Clicks and Value Creation in the Internet Economy	208
10.3	A Survey of Click Fraud	209
10.4	A Click Fraudster's Cost-Benefit Calculus	212
10.4.1	The Offenders	212
10.4.2	The Victims	219
10.5	Concluding Comments	221
	References	222
11	Concluding Remarks and Implications	227
11.1	Where Do We Go from Here?	227
11.2	Implications for Businesses	228
11.2.1	All Firms Are Not Equally Susceptible to the Vulnerability of Various ICT-Created Security Risks	229
11.2.2	Some Firms Are More Affected by the Government's Measure	229
11.2.3	Consideration of Security Risks in ICT and Competitive Strategies	229
11.2.4	The Rank Effect	230
11.2.5	Importance of Reporting	230
11.2.6	Measures to Avoid Positive Feedbacks to Cyber-Criminals	230
11.2.7	Combining Technological and Behavioral/Perceptual Measures	231
11.2.8	Managing Market Information	231
11.2.9	Collaborating with Government Agencies	231
11.2.10	Harnessing the Power of Attachment in Online Communities	232
11.2.11	Employing Online Security as a Competitive Advantage Tool	232

11.3	Implications for Consumers	233
11.3.1	Revisiting a Cognitive Framework Related to Cybercrimes	233
11.3.2	Tracking the Performance Indicators Frequently	234
11.3.3	Minimizing Activities, Websites, Channels, and Networks Associated with Cybercrimes	234
11.3.4	Understanding Communication Modes of Legitimate and Criminal Enterprises	234
11.3.5	Need to Be Watchful for e-Commerce Activities That Have Relatively High Incidence of Cybercrimes and Cyber-frauds	234
11.3.6	Staying Safe Offline	235
11.3.7	Monitoring Children's Online Activities	235
11.3.8	Assessing the Credibility and Reputation of Parties Involved in Economic Transactions	235
11.3.9	Knowing About How Information Is Handled by Parties Involved in Various Transactions	236
11.4	Implications for Policy Makers	236
11.4.1	Cooperation and Collaboration Among National Governments, Computer Crime Authorities, and Businesses	236
11.4.2	Paying Attention to Wider Institutional Fields	237
11.4.3	Measures to Increase Reporting Rate	237
11.4.4	Certainty vs. Severity of Punishment	237
11.4.5	Developing Economies' Negative International Image and Exclusion from the Digital World	238
11.4.6	Helping Small and Poor Countries Develop Anti-cybercrime Capabilities	239
11.4.7	Collaborations with Businesses	239
11.4.8	Measures to Educate Consumers and Increase the Distribution of and Access to Information	240
11.4.9	Broadband Penetrations and Cybercrime in Developing Economies	240
11.4.10	Dealing with Various Types of Online Communities	241
11.5	Directions for Future Research	241
11.5.1	Institutional Analysis of Cybercrime	241
11.5.2	Empirical Analysis	243
11.5.3	Inter-organizational Studies	243
11.5.4	ICT-Created Positive and Negative Asymmetries	243
11.5.5	Modus Operandi of Various Types of Cyber-Criminals	244
11.5.6	Examination of Non-state Actors	245
11.5.7	Longitudinal Analysis of Hackers	245

11.5.8	The Nature of Hot Products	245
11.5.9	Portability in Cybercrimes	245
11.5.10	Applying a Game-Theoretic Approach	245
11.5.11	Developing a Typology of Cybercrimes	246
11.5.12	Country-Level Case Studies of Cybercrimes	246
11.5.13	Cybercrime Operations as a Born Global Phenomenon	246
11.6	Final Thought	247
References		247