

# Table of Contents

<b>I</b>	<b>Introduction</b>	<b>15</b>
	<i>Wytske van der Wagen, Jan-Jaap Oerlemans &amp; Marleen Weulen Kranenbarg</i>	
1.1	Cybercrime as a new field in criminology	15
1.2	What is cybercrime?	16
1.3	Objective of the book	18
1.4	Structure of the book	20
<b>2</b>	<b>Cybercrime in a criminological perspective</b>	<b>21</b>
	<i>Wytske van der Wagen, Jan-Jaap Oerlemans &amp; Marleen Weulen Kranenbarg</i>	
2.1	Introduction	21
2.2	Cybercrime in historical perspective	21
2.2.1	The period 1970-1989	22
2.2.2	The period 1990-1999	24
2.2.3	The period 2000-2009	25
2.2.4	The period 2010-2021	27
2.3	Cybercrime in a theoretical perspective: the ‘old wine, new bottles’ discussion	28
2.3.1	The removal of barriers of time and space	28
2.3.2	Automation and amplification	29
2.3.3	Innovation and transformation	30
2.3.4	Social and commercial interconnectivity	30
2.3.5	Anonymity and fluidity of identity	31
2.3.6	Virtualisation and hybridisation	32
2.4	Cybercrime in a methodological perspective	33
2.4.1	Questionnaires and interviews	33
2.4.1.1	Online and offline questionnaires	33
2.4.1.2	Online and offline interviews	36
2.4.2	Online and offline participatory observation	39
2.4.2.1	Hacker forums	39
2.4.2.2	Telegram	41
2.4.2.3	Other websites	41

	2.4.2.4	Dark web and criminal marketplaces	42
	2.4.3	Documents and registration data	43
	2.4.3.1	Registration data	43
	2.4.3.2	Case law	44
	2.4.3.3	Police files	45
	2.4.3.4	Reports from public and private organisation	47
	2.4.3.5	(Social) media content	47
	2.4.4	General trends and developments in cybercrime research	48
2.5		To conclude	50
2.6		Discussion questions	50
2.7		Core concepts	51
<b>3</b>		<b>Types of cybercrime and their criminalisation</b>	<b>53</b>
		<i>Jan-Jaap Oerlemans &amp; Wytse van der Wagen</i>	
3.1		Introduction	53
3.2		Cyber-dependent crime	53
	3.2.1	Hacking	55
	3.2.1.1	Computer hacking	55
	3.2.1.2	Ethical hacking	58
	3.2.2	Malware	59
	3.2.2.1	Ransomware	60
	3.2.3	Botnets	65
	3.2.4	Ddos attacks	67
3.3		Cyber-enabled crime	70
	3.3.1	Cyber-enabled fraud	70
	3.3.2	Online drug trafficking	73
	3.3.3	Money laundering and virtual currency	76
	3.3.4	Online sex offences	79
	3.3.4.1	Child pornography	79
	3.3.4.2	Sexting	82
	3.3.4.3	Grooming	83
	3.3.4.4	Sextortion	85
	3.3.4.5	Revenge porn	87
	3.3.5	Content crimes	88
3.4		Future developments	90
	3.4.1	Increased involvement of state actors	90
	3.4.2	The ‘internet of things’	91
	3.4.3	The use of artificial intelligence by cybercriminals	92

3.5	To conclude	93
3.6	Discussion questions	93
3.7	Core concepts	94
<b>4</b>	<b>Cyber offenders</b>	<b>99</b>
	<i>Wytske van der Wagen &amp; Marleen Weulen Kranenburg</i>	
4.1	Introduction	99
4.2	Prevalence and development of cybercrime offending	100
4.2.1	Prevalence rates	100
4.2.2	Trends	102
4.3	Typologies of cyber offenders	103
4.3.1	Hacker taxonomies	104
4.3.2	General classifications of cyber offenders	106
4.3.3	Typologies targeting organised crime offenders	107
4.4	Background characteristics of cyber-dependent offenders	108
4.4.1	Socio-demographic characteristics	109
4.4.1.1	Age	109
4.4.1.2	Gender	109
4.4.1.3	Ethnicity	110
4.4.1.4	Family composition and socio-economic background	111
4.4.2	Education, work and leisure	111
4.4.2.1	Education(s)	111
4.4.2.2	Work	112
4.4.2.3	Leisure activities	113
4.4.3	Social network (offline and online)	114
4.4.4	Psychological characteristics and personality	115
4.4.4.1	Autism	115
4.4.4.2	Self-control	116
4.5	Motivations	116
4.5.1	Intellectual motivations	117
4.5.2	Sensation-related motivations	117
4.5.3	Status-related motivations	117
4.5.4	Financial motivations	118
4.5.5	Vindictive motivations	118
4.5.6	Ideological motivations	118
4.6	Contextual factors that play a role in cyber offending	119
4.6.1	Family context	119
4.6.2	School context	120
4.6.3	Social context (offline and online)	125

	4.6.4	Legal context	126
	4.6.5	Digital context	127
4.7		To conclude	128
4.8		Discussion questions	129
4.9		Core concepts	129
<b>5</b>		<b>The organisation of cybercrime</b>	<b>131</b>
		<i>Thomas J. Holt &amp; Rutger Leukfeldt</i>	
5.1		Introduction	131
5.2		Assessing the nature of organised crime and cybercrime	133
	5.2.1	Qualitative research on organisational structures	133
	5.2.2	Quantitative research on organisational structures	135
5.3		The role and structure of online markets on cybercrime	136
	5.3.1	Differentiating shops, forums and cryptomarkets	137
	5.3.2	The social relationships structuring online markets	139
5.4		To conclude	140
5.5		Discussion questions	142
5.6		Core concepts	143
<b>10</b>	<b>6</b>	<b>Victims of cybercrime</b>	<b>145</b>
		<i>Take Sipma, Rik Beerthuisen, Wylske van der Wagen &amp; André van der Laan</i>	
	6.1	Introduction	145
	6.2	International developments in cybercrime victimisation	146
	6.3	The extent and development of cybercrime victimisation in the Netherlands	147
	6.3.1	Cybercrime victimisation among the general public	147
	6.3.1.1	Malware	148
	6.3.1.2	Hacking	149
	6.3.1.3	Identity fraud	149
	6.3.1.4	Online sales and purchase fraud	150
	6.3.1.5	Online threats	150
	6.3.1.6	Other forms of cybercrime	151
	6.3.1.7	Shift from offline to online victimisation	152
	6.3.1.8	Victimisation in police records	153
	6.3.2	Cybercrime victimisation of companies and governmental institutions	154

6.4	Risk and protective factors of cybercrime victimisation	155
6.4.1	Internet use	155
6.4.2	Accessibility and protection measures	156
6.4.3	Personality traits	158
6.4.4	Socio-demographic characteristics	159
6.5	Reactions to and consequences of victimisation of cybercrime	160
6.5.1	Readiness to report	160
6.5.2	Financial and emotional consequences	160
6.5.2.1	Financial implications	160
6.5.2.2	Emotional consequences	161
6.5.3	Change in online activities	163
6.6	Measures against victimisation of cybercrime	163
6.7	To conclude	165
6.8	Discussion questions	166
6.9	Core concepts	167
<b>7</b>	<b>Criminological theories and cybercrime</b>	<b>169</b>
	<i>Marleen Weulen Kranenborg &amp; Wytse van der Wagen</i>	
7.1	Introduction	169
7.2	Classical criminological theories and their applicability to cybercrime	170
7.2.1	Routine activity theory	170
7.2.1.1	Opportunity theories	170
7.2.1.2	Suitable target	171
7.2.1.3	Absence of capable guardianship	172
7.2.1.4	Convergence in time and space	173
7.2.2	Social control theory	174
7.2.3	Social learning theory	175
7.2.3.1	Differential association	176
7.2.3.2	Deviant definitions	176
7.2.3.3	Imitation	177
7.2.3.4	Differential reinforcement	177
7.2.4	Neutralisation techniques	178
7.2.5	Strain theory	179
7.2.6	Labelling theory	181
7.3	Criminological theories and organised cybercrime	183
7.3.1	How organised and digital are cybercriminal networks?	183

	7.3.2	Pros and cons of online collaboration, a unique opportunity?	185
7.4		Cybercriminological concepts and approaches	186
	7.4.1	Online disinhibition	186
	7.4.1.1	Distinguishing the online from the offline self	188
	7.4.2	Digital drift	189
	7.4.3	Affordance theory	190
	7.4.4	Cyborg crime and actor-network theory	192
7.5		To conclude	194
7.6		Discussion questions	195
7.7		Core concepts	195
<b>8</b>		<b>Cybercrime investigations</b>	<b>197</b>
		<i>Jan-Jaap Oerlemans &amp; Maša Galič</i>	
8.1		Introduction	197
8.2		Digital investigations and criminal procedure law	198
	8.2.1	Regulating investigative methods	198
	8.2.2	Jurisdiction and cybercrime	203
8.3		IP addresses as digital leads	207
	8.3.1	Data production and preservation orders	209
	8.3.2	Seizing and analysing data on computers	217
	8.3.3	Network computer searches	220
8.4		The challenge of anonymity	222
	8.4.1	Proxy and VPN services	222
	8.4.2	Tor	223
	8.4.3	Open source investigations	225
	8.4.4	Online undercover operations	228
8.5		The challenge of encryption	236
	8.5.1	Encryption in storage	237
	8.5.2	Encryption in transit	239
	8.5.3	Hacking as an investigative method	240
8.6		Disrupting cybercrime	243
8.7		To conclude	247
8.8		Discussion questions	248
8.9		Core concepts	249
<b>9</b>		<b>Interventions for cyber offenders</b>	<b>255</b>
		<i>Elina van 't Zand, Sifra Matthijsse, Tamar Fischer &amp; Wytke van der Wagen</i>	
9.1		Introduction	255

9.2	Perspectives on interventions	256
9.2.1	Three approaches	256
9.2.2	Applicability of the approaches to cyber offenders	257
9.3	The rational choice approach	258
9.3.1	Deterrence and situational crime prevention	258
9.3.2	Reactive interventions in line with the rational choice approach	260
9.3.2.1	Incarceration	260
9.3.2.2	Financial penalties	261
9.3.3	Preventive interventions in line with the rational choice approach	262
9.3.3.1	Cease-and-desist-visits	262
9.3.3.2	Online policing	263
9.3.3.3	Education in schools	265
9.4	The What Works approach	266
9.4.1	What Works and effective treatment	266
9.4.2	Interventions in line with the What Works approach	267
9.4.2.1	Strengthening cognitive and social skills	267
9.4.2.2	Reducing pro-criminal attitudes and increasing awareness of criminality and harm	269
9.4.2.3	Manipulating criminogenic opportunity factors	270
9.4.2.4	Diversion	271
9.5	The desistance approach	272
9.5.1	Why people stop offending	272
9.5.2	Interventions in line with the desistance approach	274
9.5.2.1	Ethical hacking	274
9.5.2.2	Role models	276
9.5.2.3	Talent development	277
9.5.2.4	Career perspectives	279
9.6	To conclude	280
9.7	Discussion questions	282
9.8	Core terms	282
<b>References</b>		<b>285</b>
<b>Index</b>		<b>337</b>
<b>Case law</b>		<b>347</b>

