

TABLE OF CONTENTS

Abbreviations		XV
One	Cybercrime Jurisdiction – an Introduction – <i>Bert-Jaap Koops and Susan W. Brenner</i>	1
1.1	Substantive and Procedural Cybercrime Jurisdiction	2
1.2	Traditional Bases for Jurisdiction	3
1.3	Diverging Views	6
1.4	Aim and Structure of This Book	7
	Bibliography	7
Two	Jurisdiction in the Cybercrime Convention – <i>Henrik W.K. Kaspersen</i>	9
2.1	Introductory Remarks	9
2.2	Jurisdiction Rules in the Cybercrime Convention	10
2.2.1	Territoriality principle	10
2.2.2	Ubiquitous nature of cybercrimes	11
2.2.3	Substantial link	12
2.3	Other Jurisdiction Principles	12
2.3.1	High seas and outer space	13
2.3.2	Nationality principle	13
2.3.3	Universality principle	14
2.4	Rights of the Defendant	15
2.5	International Law: a Matter of Pragmatism?	15
2.5.1	Extradition	15
2.5.2	International co-ordination	16
2.6	Positive Jurisdiction Conflicts and the Need for Flexibility	17
2.7	Obligation to Prosecute?	18
2.8	Jurisdiction Principles and Extraterritorial Criminal Investigations	19
2.9	Concluding Observations	21
	Bibliography	22
Three	International Co-operation as a Promise and a Threat – <i>Gus Hosein</i>	23
3.1	Questioning International Co-operation	24
3.2	Traversing a History of Jurisdiction	25
3.2.1	‘New bottles’: Everything is different	26
3.2.2	‘Old wine’: Nothing new	27

3.3	Reaching for Harmonization: International Co-operation in Criminal Matters	29
3.3.1	Co-operation as a response to terrorism	29
3.3.2	Case: Maher Arar and the international co-operation in intelligence	30
3.4	Harmonization and International Co-operation Involving Information Technology	34
3.4.1	Co-operation as a necessity for cybercrime	34
3.4.2	Case: Investigating Indymedia	37
3.5	Can International Co-operation Be Regulated?	44
	Bibliography	46
Four	Cybercrime and Jurisdiction in Australia – <i>Gregor Urbas and Peter Grabosky</i>	47
4.1	Introduction	47
4.2	National Cybercrime Legislation	49
4.2.1	Jurisdictional overview	49
4.2.2	Historical overview of computer-crime laws	50
4.2.3	Specific cybercrime provisions	51
4.2.4	Relevant case law	56
4.3	Legal Provisions on Jurisdiction for Cybercrimes	60
4.3.1	Commonwealth legislation	61
4.3.2	State and territory legislation	64
4.4	Co-operation Arrangements	64
4.5	Cross-Border Investigation	65
4.6	Conclusion	68
	Bibliography	68
Five	Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty Is at Stake? – <i>Paul de Hert</i>	71
5.1	Introduction	71
5.2	‘Sovereignty’, ‘Jurisdiction’, an ‘Territoriality’	72
5.3	Cybercrime Legislation: Old and New	76
5.3.1	The strength of existing criminal-law instruments	76
5.3.2	Deconstruction of the threat analysis at the national level	79
5.3.3	Cross-border investigation powers	80
5.4	International Co-operation and the European Arrest Warrant	84
5.4.1	Today’s possibilities	84
5.4.2	The 2002 framework decision on the European arrest warrant	85
5.4.3	Implications of the EAW for cybercrime	87
5.4.4	Illustration: the case of Holocaust denier Siegfried Verbeke	88
5.5	Enlarged Jurisdiction	92

5.5.1	Territoriality and Belgian and Dutch jurisdiction provisions	92
5.5.2	Two developments with regard to enlarged jurisdiction	94
5.6	Jurisdiction and the Flexibility of International Law	97
5.6.1	The <i>Lotus</i> case	97
5.6.2	<i>Yerodia</i> does not correct <i>Lotus</i> but proves my point	99
5.7	Extraterritorial Investigation	102
5.7.1	<i>Lotus</i> and the legality of extraterritorial law enforcement	102
5.7.2	The legality of transborder access to stored computer data	106
5.8	Conclusion	109
	Bibliography	110
Six	Cybercrime and Jurisdiction in Brazil. From Extraterritorial to Ultraterritorial Jurisdiction? – <i>Roberto Chacon de Albuquerque</i>	111
6.1	Introduction	111
6.2	Cybercrime Legislation	113
6.2.1	Substantive law	113
6.2.2	Procedural law	118
6.3	Cross-Border Cyber-Investigation	119
6.4	Substantive Cybercrime Jurisdiction	122
6.5	Extraterritorial Jurisdiction and Jurisdiction Conflicts	125
6.6	Pitfalls of Extraterritorial Jurisdiction	128
6.7	Extraterritorial Jurisdiction in Brazil	131
6.7.1	Unconditional extraterritorial jurisdiction	131
6.7.2	Conditional extraterritorial jurisdiction	133
6.8	Ultraterritorial Jurisdiction	134
6.9	Conclusion	138
	Bibliography	139
Seven	Cybercrime and Jurisdiction in Chile – Rodrigo Zúñiga and Fernando Londoño	141
7.1	Introduction	141
7.2	Brief Legislative History	142
7.2.1	Material provisions	142
7.2.2	Procedural provisions	142
7.3	Material Provisions on Relevant Cybercrimes	143
7.3.1	Provisions within the law	143
7.3.2	Relevant case law	146
7.4	Procedural Provisions Applicable to Cybercrime Investigations	147
7.5	Material Jurisdiction	149
7.5.1	Legal provisions on jurisdiction concerning cybercrimes	149
7.5.2	The reasonableness of claiming jurisdiction for cybercrimes	152
7.6	Procedural Jurisdiction	154

7.7	Conclusion	154
	Bibliography	155
Eight	Cybercrime and Jurisdiction in Denmark – <i>Henrik Spang-Hanssen</i>	157
8.1	Introduction	157
8.2	Substantive Cybercrime Legislation	157
8.2.1	General issues	157
8.2.2	Provisions relating to cybercrimes	159
8.3	Procedural Provisions	167
8.3.1	Investigation powers	167
8.3.2	International co-operation	169
8.3.3	Co-operation with EU countries	170
8.3.4	Co-operation with the Nordic countries	172
8.4	Jurisdiction Concerning Cybercrime	173
8.5	Analysis and Opinion	174
8.5.1	What is a cybercrime?	175
8.5.2	Cybercrime jurisdiction and public international law	177
8.5.3	Cyber-investigation jurisdiction	179
8.5.4	Conflict in cybercrime jurisdiction	180
8.6	Conclusion	181
	Bibliography	181
Nine	Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions – <i>Ulrich Sieber</i>	183
9.1	Introduction	183
9.1.1	The new challenges of cybercrime	183
9.1.2	The new responses of the international community	183
9.1.3	The situation in Germany	184
9.1.4	The need for new solutions in the field of jurisdiction	186
9.2	Traditional Approaches in German Criminal Law	187
9.2.1	The need for differentiation	187
9.2.2	The traditional approaches to action crimes and abstract endangerment offenses	189
9.3	New Solutions	193
9.3.1	The autonomous interpretation of the concept of result	193
9.3.2	Dissemination of illegal content: distinction between push and pull	198
9.3.3	The BGH decision in the <i>Toben</i> case	201
9.4	Results and Consequences	204
9.4.1	Result with respect to present law	204
9.4.2	Evaluation of the present legal situation	205

9.4.3	Basic principles for the future development of jurisdiction in cyberspace	207
9.4.4	Conclusions for legal policy	208
	Bibliography	209
Ten	Cybercrime and Jurisdiction in India – Pavan Duggal	211
10.1	Introduction	211
10.2	Indian Cybercrime Legislation	212
10.2.1	Substantive law	213
10.2.2	Procedural law	214
10.3	Cybercrime Jurisdiction	217
10.3.1	Legal provisions	217
10.3.2	Jurisprudence	220
10.4	Evidentiary Issues	222
10.5	Analysis and Opinion	223
10.6	Conclusion	224
	Bibliography	225
Eleven	Cybercrime and Jurisdiction in Italy – Giovanni Ziccardi	227
11.1	Substantive Cybercrime Law	227
11.1.1	The Constitution of 1948	227
11.1.2	The first real informatic provisions	228
11.1.3	Copyright law	228
11.1.4	The Italian Computer Crimes Act of 1993	229
11.1.5	The Data Protection Acts of 1996 and 2003	232
11.2	Procedural Cybercrime Law	233
11.2.1	Network wiretapping	233
11.2.2	Search, seizure, and network searches	233
11.2.3	Data retention	234
11.3	Jurisdiction: The Applicability of Italian Criminal Law	234
11.3.1	The <i>Locus Commissi Delicti</i> Issue	234
11.3.2	The obligatory nature of Italian criminal law	235
11.3.3	The principle of territoriality	235
11.3.4	Applicability of the principle of territoriality	236
11.3.5	Applicability of the principle of defense	237
11.4	A Typical Case: An Attack from ‘Outside’	237
11.5	Conclusion	238
	Bibliography	239
Twelve	Cybercrime and Jurisdiction in Japan – Pauline C. Reich	241
12.1	Introduction	241
12.2	Cybercrime Legislation	243
12.2.1	Substantive law	243

12.2.2	Procedural law	246
12.2.3	Japan and the Cybercrime Convention	247
12.3	Jurisdiction in Cybercrime Cases	250
12.3.1	Jurisdictional provisions	250
12.3.2	Case law on cross-border cybercrime	251
12.3.3	Cyber-investigation and international co-operation	252
12.4	Conclusion	254
	Bibliography	254
Thirteen	Cybercrime and Jurisdiction in the Republic of Korea – <i>Jeong-Hoon Lee</i>	257
13.1	Introduction	257
13.2	Substantive Cybercrime Legislation	258
13.2.1	The Criminal Act	258
13.2.2	The Information and Communications Network Act	260
13.3	Criminal Jurisdiction over Cybercrime	262
13.3.1	Principles of criminal jurisdiction	262
13.3.2	Application of the principles of criminal jurisdiction	264
13.4	Evidence and International Mutual Assistance Concerning Cybercrime	268
13.4.1	Investigation of evidence	269
13.4.2	Search and seizure	269
13.4.3	Admissibility of evidence	270
13.4.4	International mutual assistance	270
13.5	Conclusion	271
	Bibliography	272
Fourteen	Cybercrime and Jurisdiction in New Zealand – <i>Noel Cox</i>	273
14.1	Introduction	273
14.2	National Cybercrime Legislation	274
14.2.1	Brief history	274
14.2.2	Provisions on various cybercrimes	274
14.2.3	Investigation powers	278
14.3	Jurisdiction for Cybercrimes	280
14.3.1	Provisions in law	280
14.3.2	Case law	283
14.4	Policy Considerations	285
14.4.1	Claiming jurisdiction for cybercrimes	285
14.4.2	Dealing with cyber-investigation jurisdiction	288
14.4.3	Positive and negative jurisdiction conflicts	289
14.5	Conclusion	290
	Bibliography	290

Fifteen	Cybercrime and Jurisdiction in the United Kingdom – <i>Ian Walden</i>	293
15.1	Introduction	293
15.2	Material Jurisdiction	294
15.2.1	Statutory rules	295
15.2.2	Extraterritorial criminal law	299
15.3	Procedural Jurisdiction	301
15.3.1	Investigating cybercrime	302
15.3.2	Moving evidence	305
15.3.3	Moving people	308
15.4	Concluding Remarks	311
	Bibliography	311
Sixteen	Cybercrime and Jurisdiction in the United States – <i>Jessica R. Herrera-Flanigan</i>	313
16.1	Introduction	313
16.2	Cybercrime Substantive Laws	314
16.2.1	Computer Fraud and Abuse Act of 1986	314
16.2.2	Other relevant laws	315
16.3	Cybercrime Procedural Laws	317
16.4	United States Determination of Jurisdiction	319
16.5	United States Determination of Venue, Once Jurisdiction is Established	320
16.6	Jurisdictional Issues with Cybercrime Investigations	321
16.6.1	Ivanov-Gorshkov, McKinnon, and Zezev cases	322
16.6.2	Procedures for searching computers internationality and providing assistance	324
16.7	Conclusion	325
	Bibliography	325
Seventeen	The Next Step: Prioritizing Jurisdiction – <i>Susan W. Brenner</i>	327
17.1	Jurisdictional Conflicts	327
17.2	Prioritizing Jurisdictional Claims: Lack of Guidance	329
17.3	Factors in Prioritizing Jurisdictional Claims	330
17.3.1	Place of commission of the crime	331
17.3.2	Custody of the perpetrator	333
17.3.3	Harm	337
17.3.4	Nationality	338
17.3.5	Strength of the case against the perpetrator	343
17.3.6	Punishment	344
17.3.7	Fairness and convenience	346
17.4	Conclusion	346
	Bibliography	349

About the editors and authors

351
