

Table of Contents

Editor	v
Contributors	vii
Preface	xvii
Introduction to the Second Edition <i>Ioannis Iglezakis</i>	1
CHAPTER 1	
Attacks Against Information Systems: Technical Definitions <i>Lilian Mitrou</i>	3
§1.01 “Information Systems” and Surrounding Concepts	4
§1.02 The Notions of “Attacks” and Threats	6
§1.03 Security of Information Systems	8
§1.04 Cybersecurity	10
§1.05 Cybercrime and Cyberwar	11
CHAPTER 2	
Criminalization of Attacks Against Information Systems <i>Philippe Jougleux, Tatiana-Eleni Synodinou & Lilian Mitrou</i>	15
§2.01 The Milestones of the European Legal Framework	16
[A] The Long Road to the Harmonization of Cybercrime Law	16
[1] Before the Budapest Convention	16
[2] The Budapest Convention on Cybercrime (2001)	17
[3] The Council Framework Decision of 2005	18
[4] Other Unilateral, Bilateral and Multilateral Approaches	19
[B] Directive 2013/40/EU	21
[1] The Adoption of the Directive	21
[2] Main Principles of the Directive 2013/40/EU	22

Table of Contents

[3]	Cyberwar and the Directive	24
[4]	The Protection of Critical Infrastructure Against Cyber Attacks and Cyber Terrorism	25
[5]	Next Steps after the Directive	27
§2.02	Criminal Offenses	27
[A]	Illegal Access to Information Systems	27
[1]	The Offense and Its Application	27
[2]	The Issue of Illegal Access with or Without Use of Technological Measures	29
[3]	Illegal Access and Theory of Information Goods	33
[B]	Illegal System Interference	33
[1]	Overview of the Offense	33
[2]	DDoS Attacks	36
[3]	Other Fields of Application	37
[C]	Illegal Data Interference	38
[1]	Overview of the Offense	38
[2]	New Forms of Malware and Repression	38
[3]	The States as Perpetrators of the Offense	40
[D]	Illegal Interception	41
[1]	Overview of the Offense	41
[2]	The Distinction Between Private and Public Communication	42
[3]	The Principles Guiding Lawful Interceptions	43
[4]	The Snowden Revelations and Their Lessons	44
[E]	Relationship of Cyber-Attack Offenses with Other Offenses	46
[1]	Consecutive and Concurrent Sentences	46
[2]	The Concurrent Application of “Computer-Related” Offenses with Cyber Attacks Offenses	47
[3]	The Legal Evolution of Cyber Fraud with the Directive 2019/713/EU	50
§2.03	Private Law Aspects of the Regulation of Cyber Attacks	52
[A]	Civil Liability for Cyber Attacks	52
[B]	The Calculation of Damages	54
[C]	The Negligent Protection of an Information System	56
§2.04	Forensic Issues	58
[A]	The Enforcement of Cybercrime Legislation and the Problem of Evidence	58
[B]	Digital Forensics and E-Evidence	59
[1]	Electronic Evidence	60
[2]	Principles	62
[3]	Problems and Shortcomings of Digital Evidences	65
[C]	Specific Forensics Categories	67
[1]	Network Forensics	67
[2]	Smartphone Forensics	68
[3]	Cloud Forensics	69

§2.05	[4] Internet of Things Forensics	71
	Personal Data Protection and the Legal Status of the IP Address	72
	[A] The Double Nature of the IP Address in EU Privacy Law	74
	[1] The IP Address and Personal Data Protection	74
	[2] The IP Address and the Secrecy of Communications	82
	[3] IP Address and Presumption of Liability in the CJEU's Case Law: An Alternative Approach?	90
	[B] The Processing of the IP Address as Evidence in Criminal Litigation	94
	[1] The IP Address in the Cybercrime Convention	94
	[2] Processing of IP Address in Cybercrime Cases under the Scope of EU Law	101
§2.06	Investigation and Prosecution of Cybercrime and Jurisdiction	106
	[A] The Issue	106
	[B] The Principles	109
	[1] Territoriality and Jurisdictional Conflicts	109
	[2] Jurisdictional Conflicts	110
	[C] Extraterritorial Jurisdiction	111
	[D] Transborder Access to Evidence under the Cybercrime Convention	112
	[E] Direct Contact to Service Provider	115
	[F] Transborder Access under the Directive 2013/40/EU	115
	[G] Jurisdictional Issues and Transborder Access under the Draft Regulation on European Production and Preservation Orders for E-Evidence in Criminal Matters	117

CHAPTER 3

Prevention of Cyber Attacks

	<i>Philippe Jouglex & Tatiana-Eleni Syndinou</i>	121
§3.01	The Obstacle: Crimes Legislation	122
	[A] Tools Used for Committing Offenses	122
	[1] Overview of the Offense of Hacking Tools Distribution	122
	[2] The Three Steps of Malicious Intention	123
	[3] The Black Market of Data	124
	[B] Incitement, Aiding and Abetting and Attempt	125
§3.02	The Role of ISPs in Cybercrime Prevention	126
	[A] ISPs as Gatekeepers of the Internet: The Debate about a More Active Role of ISPs in Cybercrime Prevention	126
	[B] The Big Challenge: Balancing ISP Subscribers' Rights with Law Enforcement Objectives	129
	[C] Cybercrime Prevention via Internet Filtering: Precedents and Controversies	132
	[D] The Role of ISPs in Cybercrime Prevention and Its Boundaries: An Interference with Fundamental Rights?	138

Table of Contents

[1] Illegal and Harmful Criminal Content in the EU and Freedom of Expression	138
[2] The Internet Connection as a Component of the Right of Expression	139
[a] The Recognition of Internet Access as a Fundamental Value in the Contemporary World	141
[b] The Guarantee of Internet Access as a Component of the Right of Freedom of Expression	145
[3] Site Blocking at an ISP Level in the CJEU's Case Law	150
 CHAPTER 4	
Legal Consequences of Cybercrime	
<i>Tatiana-Eleni Synodinou & Lilian Mitrou</i> 157	
§4.01 The Regime of Security and Data Breach Notification	157
[A] Security and Data Breach Notification as a Compliance and Transparency Tool	157
[B] The USA Breach Notification Model	159
[C] The Current European Framework	161
[1] The Electronic Communications Sector: The e-Privacy Directive	161
[2] Notification under the Framework Directive	163
[3] Notification under the Regulation 611/2013	164
[D] The Future: A Comprehensive Notification Regime?	166
[1] The General Data Protection Regulation (GDPR)	166
[2] The NIS Directive	168
§4.02 Cybercrime as a Tool for Committing Other Offenses	170
[A] Sociology of Hacking: The Enemy from Within	170
[B] Cybercrime as a Parallel Economy	177
Conclusion	181
Appendices	185
 APPENDIX I	
Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA	187
 APPENDIX II	
Convention on Cybercrime	203
 APPENDIX III	
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	229

Table of Contents

APPENDIX IV	
Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA	265
Bibliography	283
Index	299