

Table of Contents

Editor and Contributors	v
Preface	xv
Introduction <i>Ioannis Iglezakis</i>	1
CHAPTER 1 Attacks against Information Systems: Technical Definitions <i>Lilian Mitrou</i>	9
§1.01 “Information Systems” and Surrounding Concepts	10
§1.02 The Notions of “Attacks” and Threats	12
§1.03 Security of Information Systems	14
§1.04 Cybersecurity	16
§1.05 Cybercrime and Cyberwar	17
CHAPTER 2 Criminalization of Attacks against Information Systems <i>Philippe Jougleux, Lilian Mitrou & Tatiana-Eleni Synodinou</i>	19
§2.01 The Milestones of the European Legal Framework	20
[A] The Long Road to the Harmonization of Cybercrime Law	20
[1] Before the Budapest Convention	20
[2] The Budapest Convention on Cybercrime (2001)	21
[3] The Council Framework Decision of 2005	22
[4] Other Unilateral, Bilateral and Multilateral Approaches	23
[B] Directive 2013/40/EU	25
[1] The Adoption of the Directive	25
[2] Main Principles of the Directive 2013/40/EU	26
§2.02 Criminal Offences	29

Table of Contents

	[A] Illegal Access to Information Systems	29
	[1] The Offence and Its Application	29
	[2] The Issue of Illegal Access with or without Use of Technological Measures	31
	[3] Illegal Access and Theory of Information Goods	33
	[B] Illegal System Interference	34
	[1] Overview of the Offence	34
	[2] DDoS Attacks	36
	[3] Other Fields of Application	37
	[C] Illegal Data Interference	38
	[1] Overview of the Offence	38
	[2] New Forms of Malware and Repression	39
	[3] The States as Perpetrators of the Offence	40
	[D] Illegal Interception	41
	[1] Overview of the Offence	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 Offences with Other Offences	46
	[1] Consecutive and Concurrent Sentences	46
	[2] The Concurrent Application of "Computer Related" Offences with Cyber Attacks Offences	47
§2.03	Private Law Aspects of the Regulation of Cyber Attacks	49
	[A] Civil Liability for Cyber Attacks	49
	[B] The Calculation of Damages	51
	[C] The Negligent Protection of an Information System	53
§2.04	Forensic Issues	54
	[A] The Enforcement of Cybercrime Legislation and the Problem of Evidence	54
	[B] Digital Forensics and E-evidence	56
	[1] Electronic Evidence	56
	[2] Principles	58
	[3] Problems and Shortcomings of Digital Evidences	61
	[C] Specific Forensics Categories	63
	[1] Smartphone Forensics	63
	[2] Cloud Forensics	64
§2.05	Personal Data Protection and the IP Address Legal Status	66
	[A] The Double Nature of the IP Address in EU Privacy Law	67
	[1] The IP Address and Personal Data Protection	68
	[2] The IP Address and the Secrecy of Communications	75
	[B] The Processing of the IP Address as Evidence in Criminal Litigation	81

	[1] The IP Address in the Cyber Crime Convention	81
	[2] Processing of IP Address in Cybercrime Cases under the Scope of EU Law	87
§2.06	Investigation and Prosecution of Cybercrime and Jurisdiction	91
	[A] The Issue	91
	[B] The Principles	94
	[1] Territoriality and Jurisdictional Conflicts	94
	[2] Jurisdictional Conflicts	95
	[C] Extraterritorial Jurisdiction	96
	[D] Transborder Access to Evidence under the Cybercrime Convention	97
	[E] Direct Contact to Service Provider	100
	[F] Transborder Access under the Directive 2013/40/EU	100
CHAPTER 3		
Prevention of Cyber Attacks		
<i>Philippe Jougleux & Tatiana-Eleni Synodinou</i>		
		103
§3.01	The Obstacle-Crimes Legislation	104
	[A] Tools Used for Committing Offences	104
	[1] Overview of the Offence of Hacking Tools Distribution	104
	[2] The Three Steps of Malicious Intention	105
	[3] The Black Market of Data	106
	[B] Incitement, Aiding and Abetting and Attempt	107
§3.02	The Role of ISPs in Cybercrime Prevention	108
	[A] ISPs as Gatekeepers of the INTERNET: The Debate about a More Active Role of ISPs in Cybercrime Prevention	108
	[B] The Big Challenge: Balancing ISP Subscribers' Rights with Law Enforcement Objectives	111
	[C] Cybercrime Prevention via Internet Filtering: Precedents and Controversies	114
	[D] The Role of ISPs in Cybercrime Prevention and Its Boundaries: An Interference with Fundamental Rights?	120
	[1] Illegal and Harmful Criminal Content in the EU and Freedom of Expression	120
	[2] The Internet Connection as a Component of the Right of Expression	121
	[a] The Recognition of Internet Access as a Fundamental Value in the Contemporary World	123
	[b] The Guarantee of Internet Access as a Component of the Right of Freedom of Expression	127
	[3] Site Blocking at an ISP Level in the CJEU's Case Law	132

Table of Contents

CHAPTER 4	
Legal Consequences of Cybercrime	
<i>Lilian Mitrou & Tatiana-Eleni Synodinou</i>	
	139
§4.01	The Regime of Security and Data Breach Notification
	139
[A]	Security and Data Breach Notification as a Compliance and Transparency Tool
	139
[B]	The USA Breach Notification Model
	142
[C]	The Current European Framework
	143
[1]	The Electronic Communications Sector: The E-Privacy Directive
	143
[2]	Notification under the Framework Directive
	145
[3]	Notification under the Regulation 611/2013
	146
[D]	The Future: A Comprehensive Notification Regime?
	148
[1]	The Draft General Data Protection Regulation
	148
[2]	The NIS Directive
	150
§4.02	Cybercrime as a Tool for Committing Other Offenses
	151
[A]	Sociology of Hacking: The Enemy from Within
	151
[B]	Cybercrime as a Parallel Economy
	158
Conclusion	
<i>Philippe Jougleux, Lilian Mitrou & Tatiana-Eleni Synodinou</i>	
	163
Appendices	
	169
APPENDIX I	
Directive 2013/40/EU	
	171
APPENDIX II	
Convention on Cybercrime	
	187
Bibliography	
	215
Index	
	231