

Contents

1	Public–Private Collaboration: Cybercrime, Cybersecurity and National Security	1
	Tatiana Tropina	
1.1	Introduction	1
1.2	Cybersecurity, Cybercrime, Cyberwar? Terminology and Misconceptions.	4
1.2.1	Cybersecurity: Different Dimensions and Blurring Borders	5
1.2.2	Areas of Public–Private Collaboration on Cybersecurity.	9
1.3	Regulating Cybersecurity: What Are the Options?.	11
1.3.1	Cybersecurity as a Multi-stakeholder Environment: Transformation	12
1.3.2	Self- and Co-regulation: Theoretical Approaches and Practical Implementation	16
1.3.3	Legislating Cybersecurity?.	19
1.4	Existing Initiatives: From Illegal Content Towards Cyber-Resilience.	20
1.4.1	Fighting Cybercrime: Forms of Cooperation.	21
1.4.2	Cybersecurity: A Call for More Structured Approaches	23
1.5	Problems and a Way Forward	26
1.5.1	Limitations: Mandate of the Governments in Criminal Law and Security.	27
1.5.2	Degree of Governmental Intervention	28
1.5.3	EU NIS Directive: From Voluntary Collaboration to Statutory Regulation?	29
1.5.4	Safeguards.	33

1.5.5	Incentives and Costs	34
1.5.6	Way Forward: Is Statutory Regulation Still an Option?	35
1.6	Conclusion.	35
	References.	37
2	Evolution, Implementation and Practice of Internet Self-regulation, Co-regulation and Public-Private Collaboration	43
	Cormac Callanan	
2.1	The Birth of Self-regulation	44
2.1.1	Introduction	44
2.1.2	Individual	44
2.1.3	Company	45
2.1.4	Industry Sector	45
2.1.5	Guided by Regulation (Sometimes Called Co-regulation)	46
2.1.6	Multi-stakeholder	46
2.1.7	Background	47
2.1.8	Content versus Traffic	48
2.1.9	Usenet News	48
2.1.10	Log Records and Charging.	50
2.1.11	Traditional Telecom Services	50
2.1.12	Open Telecommunications Market	52
2.1.13	Dropping Newsgroups	52
2.1.14	Embryonic Self-regulation	53
2.1.15	Anecdote	55
2.1.16	Conclusion.	55
2.2	Self-regulation Matures	57
2.2.1	Introduction	57
2.2.2	Putting Structure on Self-regulation.	57
2.2.3	UK French Letter	57
2.2.4	UK Child Pornography Laws	60
2.2.5	The Protection of Minors and Human Dignity in Audio-Visual Services	61
2.2.6	US Framework for Global Electronic Commerce	66
2.2.7	Global Information Networks: Realising the Potential Conference, Bonn Germany.	68
2.2.8	Irish Working Group on Illegal and Harmful Use of the Internet	70
2.2.9	Electronic Mail.	73
2.2.10	Newsgroups	74
2.2.11	Web Browsing	74
2.2.12	Web Hosting	75

2.2.13	File Transfer	75
2.2.14	Online Chat	75
2.2.15	Child Pornography	76
2.2.16	Recommendations of the Committee on Illegal and Harmful Use of the Internet	76
2.2.17	Internet Service Provider Associations	77
2.2.18	Bertelsmann Foundation	79
2.2.19	EC Daphne Programme	80
2.2.20	EC Safer Internet Action Plan	82
2.2.21	The INHOPE (Internet Hotline Providers of Europe) Association	85
2.2.22	Legislation and Conventions	86
2.2.23	Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce	87
2.2.24	The Council of Europe Cybercrime Convention	87
2.3	Conclusion.	89
	Annex—Technology Options: Internet Monitoring and Blocking	90
	Appendix I	95
	References.	99