

CONTENTS

Preface	v
About the Author	vii
Abstract	xv
List of Cases Mentioned	xvii
List of Statutes	xix
List of International Instruments	xxi
Chapter I Definitional Issues Relating to Cyberterrorism	1
1.1 Introduction	1
1.1.1 Objective of the Chapter	3
1.2 The Definitions of Important Terminologies	3
1.2.1 Cyber and Cyber Space	4
1.2.2 Terrorism and Cyberterrorism	10
1.3 <i>Modus Operandi</i> of Cyber Attack Terrorism	53
1.3.1 Classification of Cyberterrorism	54
1.3.2 <i>Modus Operandi</i> Adopted by Al-Qaeda	61
1.3.3 Impact of a Cyber Terrorist Attack	62
1.4 The Differences Between Cyberterrorism and Other Related Crimes	69
1.4.1 Cyber Crime and Cyberterrorism	69
1.4.2 Cyber Hooliganism and Cyberterrorism	73

1.4.3	Hactivism and Cyberterrorism	73
1.4.4	Computer-Assisted Crime and Cyberterrorism	74
1.4.5	Information Warfare and Cyberterrorism	75
1.4.6	Separation of Ancillary Cyber Activities from Cyberterrorism in the Definition Perspective	77
1.5	Conclusion	77
Chapter II	The Challenges Faced By International Organisations in Curbing Cyberterrorism	79
2.1	Introduction	79
2.1.1	Objective of the Chapter	80
2.2	Effort Taken by International Organisations	80
2.2.1	The United Nations (UN)	80
2.2.2	The Organization for Security and Cooperation in Europe (OSCE)	88
2.2.3	Interpol	89
2.3	Regional Level Effort and Cooperation	93
2.3.1	The European Union	93
2.3.2	The Council of Europe (CoE)	95
2.3.3	The Group of Eight (G8)	106
2.3.4	Asia-Pacific Economic Cooperation (APEC)	110
2.3.5	North Atlantic Treaty Organization (NATO)	112
2.3.6	International Multilateral Partnership against Cyber Terrorism (IMPACT)	121
2.3.7	The Organisation for Economic Cooperation and Development (OECD)	123
2.3.8	The Association of Southeast Asian Nations (ASEAN)	125
2.4	Bilateral Level of Effort	126
2.5	Harmonisation and Cooperation of International Organisations	129
2.6	Conclusion	132

Chapter III	Application of Legal Provisions in the Case of Cyberterrorism	135
3.1	Introduction	135
3.1.1	Objective of the Chapter	136
3.2	The Elements of Crime for Prosecuting Virtual Crime	137
3.3	Overview of Terrorism and Cyberterrorism Legislations for Responding to Cyberterrorism	139
3.3.1	The US	139
3.3.2	The UK	144
3.3.3	Malaysia	149
3.4	Legal Responses According to Terrorism Statutes	152
3.4.1	Ancillary Cyber Activities from the Perspective of Relevant Countries	153
3.5	Legal Response According to Computer Crime Statutes	168
3.5.1	Unauthorised Access	170
3.5.2	Exceeding Authorised Access	190
3.5.3	Misuse of Devices	194
3.5.4	Unauthorised Acts with Intent to Impair	198
3.5.5	Disclosure of Information	205
3.5.6	Virtual Weaponry Used By Terrorist	210
3.6	Estonian Legal Responses to Cyber Attacks: A Case Study	212
3.6.1	Legal Development in Estonia after the Attack	213
3.6.2	Organisational Development in Estonia: Post Attack	216
3.7	Conclusion	217
Chapter IV	Issues of Enforcement in Cyberterrorism	219
4.1	Introduction	219
4.2	Cyberterrorism Enforcement: An Overview	221
4.3	Current Investigation Process in Cyberterrorism Cases	222
4.3.1	Current Cyber Attack Methods and the Threat they Pose	222
4.3.2	Conducting Investigation and Tracking Cyberterrorism: Current Method	224

4.4 Cyberterrorism Investigation in International Conventions	228
4.4.1 Investigation Process under the Cybercrime Convention	232
4.5 The Investigation Process in Cyberterrorism: An Analysis	236
4.5.1 Gathering Evidence and Prosecuting through Formal and Informal Forensic Investigation	239
4.5.2 Evaluation of Evidence	245
4.6 Current Prosecution Process in Cyberterrorism Cases	246
4.6.1 Transnational Evidence and the Prosecutor: Current Challenges	246
4.6.2 Search Warrant: An Important Tool for the Prosecutor	246
4.6.3 Search Warrants in Cyberterrorism Cases: The US Experience	247
4.6.4 Search Warrants in Cyberterrorism Cases: The UK Experience	262
4.6.5 Search Warrants in Cyberterrorism Cases: The Malaysian Scenario	266
4.6.6 Prosecution in Cyberterrorism Cases: Comparative Analysis between the US and the UK	271
4.7 Extradition	275
4.8 Conclusion	278
Chapter V Issues of Jurisdiction for Cyberterrorism	281
5.1 Introduction	281
5.1.1 Objective of the Chapter	282
5.2 Jurisdiction	282
5.3 The Exercise of Universal Jurisdiction by the International Community and States Against Cyberterrorism	283
5.3.1 The Exercise of Universal Jurisdiction by the International Community	284
5.3.2 The Exercise of Universal Jurisdiction by States	287
5.4 Conflict of Jurisdiction	291
5.5 Conclusion	295

Chapter VI Conclusion and Recommendations	297
6.1 Introduction	297
6.2 Concluding Analysis	297
6.2.1 Issues with Cyberterrorism Definitions	301
6.2.2 The Effective Role of International Organisations in Curbing Cyber Terrorist Activities	304
6.2.3 Application of Legal Provisions in the Case of Cyberterrorism	306
6.2.4 Enforcement	309
6.2.5 Rational Jurisdiction for Cyberterrorism	314
6.3 Recommendations	315
6.3.1 Issues with Definition	315
6.3.2 Challenges Faced by International Organisations Relating to Cyberterrorism	317
6.3.3 Problems in the Application of Law to Cyberterrorism Cases	320
6.3.4 Issues in Enforcement of Cyberterrorism	322
6.3.5 Jurisdiction Issues	327
Index	329