

# TABLE OF CONTENTS

<b>Acknowledgements</b>	<b>vii</b>
<b>Abbreviations and Acronyms</b>	<b>xvii</b>
<b>List of Tables</b>	<b>xix</b>
<b>CHAPTER 1 Introduction</b>	<b>1</b>
1 Cybercrime as a global problem	1
2 Issues of cross-border access	3
2.1 Legal challenges	4
2.2 Cooperation challenges	5
3 Research focus on Indonesia and aims of this Study	8
4 Research question	11
5 Operational definitions used in the study	13
5.1 Cybercrime	13
5.2 Electronic information and electronic evidence	14
5.3 Issues of cross-border access	15
6 Research methodology	16
6.1 Reviewing emerging approaches in resolving issues of cross-border access	16
6.2 Investigating Indonesian practice in resolving issues of cross-border access	17
6.2.1 Reviews of cybercrime cases	17
6.2.2 Eliciting the perceptions of investigators and judges	17
6.2.2.1 Vignette-based questionnaire	18
6.2.2.2 Respondents to the questionnaire	18
7 Research structure	20
<b>CHAPTER 2 Enforcing State Jurisdiction in Cyberspace</b>	<b>25</b>
1 Introduction	25
2 A need to adjust enforcement jurisdiction principles in cyberspace	27
3 State jurisdiction under international law	30
3.1 Types of jurisdiction	30
3.1.1 Prescriptive jurisdiction	30
3.1.2 Enforcement jurisdiction	32
3.1.3 Adjudicative jurisdiction	32
3.2 Fundamental principles of enforcement jurisdiction	32

TABLE OF CONTENTS

3.3	A territorial cybercrime investigation and its extraterritorial effects	36
3.4	Applying the <i>Lotus</i> prohibitive rule in its strict sense	38
4	Territorialising cyberspace to enforce the law	39
4.1	Cyberspace as an artificial State's territory	40
4.2	Limitations of physical control of computer systems	40
4.3	Preserving the territoriality principle and encountering its limitations	41
4.3.1	Data localisation policies	41
4.3.2	Direct cooperation with foreign providers	42
4.3.3	The virtual presence of objects and subjects in a State's territory	42
5	Obtaining e-evidence through nationals of a State	44
6	Encountering the pitfalls of extraterritorial investigation	44
6.1	E-evidence is publicly available	44
6.1.1	The existence of international customary law	45
6.1.2	The virtual presence of e-information in a State's territory	47
6.2	E-evidence is stored in another jurisdiction but accessible territorially	47
6.2.1	Information exposure theory	47
6.2.2	Search-expansion theory	48
6.3	E-evidence is stored in an unknown jurisdiction but accessible territorially	49
6.4	Self-defence, countermeasures, force majeure, distress and necessity	50
7	Resolving territorial and extraterritorial dimensions of the virtual presence nexus	51
8	Reasonableness in exercising the virtual presence nexus	53
8.1	The principle of reasonableness in prescriptive jurisdiction	55
8.2	A principle of reasonableness in enforcing criminal law in cyberspace	56
8.3	The reasonableness principle in practice	60
8.3.1	Comity analysis in the Cloud Act	61
8.3.2	Review the procedure concerning conflicting obligations	61
8.4	Limitations of the principle of reasonableness	63
9	Conclusion	63

<b>CHAPTER 3 Resolving Issues of Cross-border Access Using the Budapest Convention on Cybercrime</b>	<b>67</b>
1 Introduction	67
2 Emerging regional approaches in combating cybercrime	69
2.1 Emerging legal instruments for combating cybercrime	69
2.2 Limitations of mutual legal assistance	72
2.3 Police-to-police cooperation	73
3 The Budapest Convention on Cybercrime	74
3.1 Creating a community of trust in combating cybercrime	74
3.2 Encountering new threats of cybercrime	76
3.2.1 Use of terms	76
3.2.2 Substantive criminal law	78
3.3 Encountering issues of cross-border access	79
3.3.1 Conditions and safeguards	79
3.3.2 Investigative measures and their extraterritorial reach	80
3.3.2.1 Preservation of stored computer data	83
3.3.2.2 Production order	84
3.3.2.3 Search and seizure	86
3.3.2.4 Real-time collection of e-evidence	89
3.3.2.5 Cross-border access under Article 32b	90
3.3.2.6 The use of malware	93
3.4 Mutual legal assistance in obtaining e-evidence	95
3.4.1 The polarisation of the cooperation standard within the Budapest Convention	95
3.4.2 The EU as the backbone of the Budapest Convention	96
3.4.2.1 Historical and organisational relationship between the EU and the Council of Europe	96
3.4.2.2 The role of the Budapest Convention for the EU	98
3.4.3 Incompatibility of data protection regimes in mutual legal assistance	102
3.4.4 Data protection regime between the EU and the US	106
3.5 Improving cooperation mechanisms for cross-border access to e-evidence	108
4 Conclusion	110
<b>CHAPTER 4 American Practice in Resolving Issues of Cross-border Access</b>	<b>113</b>
1 Introduction	113
2 The US adversarial system	114
2.1 Fundamental concepts of the US adversarial system	115

TABLE OF CONTENTS

	2.1.1	Due process of law	115
	2.1.2	Probable cause	116
	2.1.3	Beyond reasonable doubt	116
2.2		Common investigative measures in cybercrime investigation	117
	2.2.1	Subpoena	117
	2.2.2	Search and Seizure	118
	2.2.2.1	The scope of the Fourth Amendment	118
	2.2.2.2	The fundamental elements of the Fourth Amendment	120
3		US multilateral approach in combating cybercrime	121
	3.1	The importance of the Budapest Convention for the US strategy in combating cybercrime	121
	3.2	Compatibility of US legislation with the Budapest Convention	123
4		US blocking instruments	124
	4.1	The Stored Communications Act as blocking instrument	124
	4.2	The Fourth Amendment as blocking instrument	125
	4.2.1	The Verdugo-Urquidez principles	125
	4.2.2	The instrumentality of Verdugo-Urquidez	126
	4.2.3	The Fourth Amendment: sword and shield in cyberspace	127
	4.2.4	Equality before the Constitution under Verdugo-Urquidez	128
	4.2.5	Unequal treatment of cross-border access under Verdugo-Urquidez	128
5		The US's recent bilateral approach in combating cybercrime	132
	5.1	The Cloud Act and the US's approach to improving mutual legal assistance mechanisms	132
	5.2	Direct cooperation with US corporations	132
	5.3	The Cloud Act executive agreement	133
	5.4	Harmonisation of legal systems under the Cloud Act	133
6		US courts' approach in resolving voluminous data	134
7		Resolving issues of cross-border access in US case law	136
	7.1	E-evidence is publicly available	136
	7.2	E-evidence is stored in another jurisdiction but accessible territorially	136
	7.2.1	The importance of <i>Microsoft-Ireland</i>	136
	7.2.2	Determining the reasonableness of extraterritorial search and seizure	138
	7.2.3	Formulating the reasonableness of extraterritorial search and seizure	139

7.3	E-evidence is stored in an unknown jurisdiction yet accessible territorially	139
7.3.1	The importance of <i>Google-cloud</i>	139
7.3.2	Determining the reasonableness of extraterritorial search and seizure	140
7.3.3	Formulating the reasonableness of extraterritorial search and seizure	140
7.4	E-evidence is inaccessible without using malware	141
7.4.1	The importance of the <i>Playpen</i> and <i>Matish</i> cases	141
7.4.2	Determining the reasonableness of extraterritorial search and seizure	142
7.4.3	Formulating the reasonableness of extraterritorial search and seizure	142
8	Conclusion	144
<b>CHAPTER 5 The Indonesian Criminal Justice System</b>		<b>147</b>
1	Introduction	147
2	The Indonesian Inquisitorial System	147
2.1	Compartmentalisation paradigm	148
2.2	The objective of ascertaining the material truth	151
2.3	Constitutional function of the Indonesian inquisitorial system	151
2.4	Main investigation phases	153
2.4.1	Preliminary investigation	154
2.4.2	Formal investigation	157
2.5	Preliminary trial	157
2.5.1	Checks-and-balances issues	158
2.5.2	The pre-trial for pre-investigation	159
2.6	The new KUHAP	160
2.7	Revitalising the checks-and-balances mechanism	160
2.8	The negative system of legal proof	162
2.8.1	Evidence: <i>Alat bukti</i> and <i>barang bukti</i>	162
2.8.2	Admissibility of legal means of evidence	163
3	Investigative measures for cybercrime investigation	165
3.1	A search	165
3.1.1	The scope of a search	165
3.1.2	An urgent search	165
3.1.3	Pre-trial to examine the lawfulness of a search	166
3.2	A seizure	167
3.2.1	Seized objects	167
3.2.2	Types of seizure	168

TABLE OF CONTENTS

3.2.3	Pre-trial for unlawful seizure	169
4	The protection of personal data in cybercrime investigation	171
4.1	Privacy and personal data protection as constitutional rights	171
4.2	Legal implications of personal data protection as a constitutional right	175
5	Conclusion	176
<b>CHAPTER 6 Indonesian Practice in Resolving Issues of Cross-border Access</b>		<b>179</b>
1	Introduction	179
2	Indonesian multilateral approach in combating cybercrime	180
2.1	Budapest Convention on Cybercrime	180
2.2	ASEAN Mutual Legal Assistance Treaty	182
2.3	Police-to-police cooperation	183
3	Electronic Information and Transaction Act (EITA)	184
3.1	Substantive criminal law in the EITA	184
3.2	Criminal procedure law in the EITA	184
3.3	Jurisdiction under the EITA	185
4	Encountering issues of cross-border access	186
4.1	Territorialising the crime	186
4.2	Searching and seizing e-evidence in cyberspace	187
4.2.1	Search and seizure of e-system and the issues of jurisdiction	187
4.2.2	Foreign email accounts as virtual spheres or evidentiary objects	189
4.3	E-information and printouts as evidence	192
4.3.1	Discrepancies in accepting e-information and printouts	193
4.3.2	Maintaining the equal standard of admissibility of evidence	195
4.4	Ordering foreign service providers under the virtual presence nexus	197
4.4.1	Enforcing direct cooperation in criminal matters	197
4.4.2	Enforcing direct cooperation for blocking illegal content	200
4.5	E-evidence is publicly available	202
4.6	E-evidence is stored in another jurisdiction but accessible territorially	203
4.7	E-evidence is stored in an unknown jurisdiction yet accessible territorially	205
4.8	E-evidence is inaccessible without using malware	205

4.8.1	Using malware in investigation	205
4.8.2	Using malware in pre-investigation	207
4.9	Protecting personal data in voluminous search and seizure	209
5	Conclusion	211
<b>CHAPTER 7 Conclusions and Recommendations</b>		<b>215</b>
1	The objective of the study	215
2	Main findings of the study	219
2.1	Sub-research question 1	219
2.2	Sub-research question 2	224
2.3	Sub-research question 3	229
2.4	Sub-research question 4	235
3	Recommendations	245
4	Looking to the Future	258
<b>Appendixes</b>		<b>261</b>
	Appendix-1	261
	Appendix-2	264
<b>References</b>		<b>277</b>