

Inhaltsverzeichnis

<i>Abkürzungen.....</i>	<i>XXI</i>
Kapitel A. Einleitung.....	I
I. Problemstellung.....	1
II. Überblick über den aktuellen Forschungsstand	2
III. Zielsetzung und Gang der Arbeit	4
Kapitel B. Begriff, Phänomenologie und Entwicklung.....	7
I. Computer-, Internet- und Cyberkriminalität	7
1. Definition	7
2. Phänomenologische Betrachtung	11
3. Abgrenzung zu Begriffen.....	13
a) Internetkriminalität	14
b) Cybercrime	15
II. Entwicklung der Computerkriminalität.....	16
1. 1960er Jahre	16
2. 1970er Jahre	18
3. 1980er Jahre	19
4. 1990er Jahre	20
5. 21. Jahrhundert.....	21
III. Statistische Entwicklung der Computerkriminalität	22
1. Statistische Entwicklung der Computerkriminalität in Deutschland.....	23
2. Statistische Entwicklung der Computerkriminalität in Aserbaidshan	24
IV. Phänomene in der Computerkriminalität	25
1. Hacking	25
2. Schadprogramme (Malware).....	27
a) Viren	28
b) Würmer.....	28
c) Trojanisches Pferd	29
d) Ransomware	30
3. Backdoor	30

4. Phishing.....	30
5. Spam.....	31
6. DoS- bzw. DDoS-Angriffe	31

**Kapitel C. Entwicklung der rechtlichen Rahmenbedingungen des
Computerstrafrechts..... 33**

I. Entwicklung der gesetzlichen Grundlagen in Deutschland 33

1. Gesetzgebung zum Datenschutz	33
2. Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)	34
3. Das Informations- und Kommunikationsgesetz (IuKG) vom 22.7.1997	35
4. Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG).....	36
5. 60. Strafrechtsänderungsgesetz (60. StrÄndG).....	36

II. Entwicklung der gesetzlichen Grundlagen in Aserbaidshan 37

1. Überblick.....	37
2. Neues Strafgesetzbuch von Aserbaidshan	38
3. Gesetz zur Änderung des Strafgesetzbuchs vom 29.6. 2012.....	39
4. Weitere Strafrechtsänderungen zu Straftaten in Bezug auf das Internet	40
5. Gesetze im Bereich der Informationstechnologie.....	40

III. Entwicklung der internationalen Rechtsakte 40

1. Cybercrime-Konvention des Europarats.....	41
a) Überblick	41
b) Entstehungsgeschichte.....	41
c) Aufbau	42
d) Ziele.....	43
aa) Harmonisierung der materiell-strafrechtlichen Regelungen.....	43
bb) Erreichung einheitlicher strafprozessualer Rechtsinstrumente.....	43
cc) Internationale Zusammenarbeit.....	44
e) Ratifikation der CyCK.....	44
f) Kritiken.....	45
2. Zusatzprotokolle.....	47
3. Zusatzprotokoll von 2003	47

4. Zusatzprotokoll von 2022	48
5. Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme	49
6. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Ersetzung des RB 2005/222/JI.....	50
a) Verabschiedung	50
b) Ziele	51
c) Aufbau	52
d) Unterschiede zum RB 2005/222/JI.....	52
Kapitel D. Rechtswidriger Zugang.....	55
I. Internationale Vorgaben	55
1. Cybercrime-Konvention des Europarats.....	55
a) Allgemeines	55
b) Objektiver Tatbestand	57
aa) Tatobjekt.....	57
bb) Tathandlung.....	58
cc) Unbefugt.....	58
c) Subjektiver Tatbestand	60
d) Vorbehalte	60
2. Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme	61
3. EU-Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	62
a) Allgemeines	62
b) Objektiver Tatbestand	62
aa) Tatobjekt.....	62
bb) Tathandlung.....	63
cc) Unbefugt.....	64
c) Subjektiver Tatbestand	65
II. Rechtswidriger Zugang im deutschen Strafrecht	65
1. Allgemeines.....	66
2. Objektiver Tatbestand	67
a) Tatobjekt.....	67
aa) Nicht unmittelbare Wahrnehmbarkeit.....	68
bb) Gespeichert oder übermittelt sein	68

cc) Nicht für den Täter bestimmt sein.....	68
dd) Besondere Sicherung gegen unberechtigten Zugang.....	70
b) Tathandlung.....	72
c) Unbefugt.....	74
3. Subjektiver Tatbestand.....	75
4. Strafantrag.....	76
III. Rechtswidriger Zugang im aserbaidischen Strafrecht.....	76
1. Allgemeines.....	78
2. Objektiver Tatbestand.....	79
a) Tatobjekt.....	79
b) Tathandlung.....	80
c) Alternativität der Tatbestände.....	80
aa) Verletzung von Sicherheitsmaßnahmen.....	81
bb) Absicht.....	82
d) Unbefugt.....	83
3. Subjektiver Tatbestand.....	83
a) Strafmündigkeit.....	84
b) Versuch.....	84
4. Qualifikationstatbestände nach Art. 271 Abs. 2 CM.....	85
a) Qualifikationstatbestand nach Art. 271 Abs. 2 Nr. 1 CM.....	85
b) Qualifikationstatbestand nach Art. 271 Abs. 2 Nr. 2 CM.....	85
c) Qualifikationstatbestand nach Art. 271 Abs. 2 Nr. 3 CM.....	86
5. Zusätzlicher Qualifikationstatbestand nach Art. 271 Abs. 3 CM.....	86
6. Strafantrag.....	87
IV. Vergleich des Art. 271 CM mit § 202a StGB im Lichte von europäischen Vorgaben.....	87
1. Geschütztes Rechtsgut.....	87
2. Tatobjekt.....	90
a) Daten und Computersysteme.....	90
b) Sicherheitsmaßnahmen.....	91
3. Tathandlung.....	93
a) Zugang.....	93
b) Überwinden und Verletzen der Sicherheitsmaßnahme.....	93
c) Unbefugt.....	96
4. Subjektiver Tatbestand.....	97

5. Strafmaß	98
6. Strafantrag	99
7. Gebrauch der einschränkenden Tatbestandsmerkmale gem. Art. 2 Satz 2 CyCK	99
V. Bewertung	99
<i>Kapitel E. Rechtswidriges Abfangen</i>	<i>101</i>
I. Internationale Vorgaben	101
1. Cybercrime-Konvention des Europarates	101
a) Allgemeines	102
b) Objektiver Tatbestand	103
aa) Tatobjekt	103
bb) Tathandlung	104
c) Unbefugt	105
d) Subjektiver Tatbestand	105
e) Einschränkende Tatbestände	105
2. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	106
a) Allgemeines	106
b) Objektiver Tatbestand	107
c) Unbefugt	108
d) Subjektiver Tatbestand	109
II. Rechtswidriges Abfangen im deutschen Strafrecht.....	109
1. Allgemeines.....	109
2. Objektiver Tatbestand	111
a) Tatobjekt	111
aa) Nichtöffentliche Datenübermittlung	112
bb) Elektromagnetische Abstrahlung	115
b) Tathandlung	115
aa) Verschaffen	115
bb) Technische Mittel	116
c) Unbefugt	117
3. Subjektiver Tatbestand.....	117
4. Weitere Strafbarkeitsvoraussetzungen	118
III. Rechtswidriges Abfangen im aserbaidischen Strafrecht.....	118
1. Allgemeines.....	120

2. Objektiver Tatbestand	121
a) Tatobjekt	121
aa) Computerdaten	121
bb) Nichtöffentlichkeit von Computerdaten.....	121
b) Tathandlung	124
c) Unbefugt	124
3. Subjektiver Tatbestand.....	124
4. Qualifikationstatbestände nach Art. 272 Abs. 2 CM.....	125
5. Zusätzlicher Qualifikationstatbestand nach Art. 272 Abs. 3 CM.....	125
IV. Vergleich des Art. 272 CM mit § 202b StGB im Lichte von europäischen Vorgaben	125
1. Geschütztes Rechtsgut	126
2. Objektiver Tatbestand	126
a) Elektronische Abstrahlungen.....	129
b) Tathandlung	130
3. Subjektiver Tatbestand.....	130
4. Strafmaß	131
5. Einschränkende Tatbestandsmerkmale gem. Art. 3 Satz 2 CyCK	131
V. Bewertung	131
Kapitel F. Dateneingriff.....	133
I. Internationale Vorgaben	133
1. Cybercrime-Konvention des Europarates	133
a) Allgemeines	133
b) Objektiver Tatbestand	134
aa) Tatobjekt.....	134
bb) Tathandlung.....	135
c) Unbefugt	135
d) Subjektiver Tatbestand	136
e) Vorbehalt gem. Art. 4. Abs. 2 CyCK	136
2. Rahmenbeschluss 222/2005/JI über Angriffe auf Informationssysteme	137
3. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	137
a) Allgemeines	138
b) Objektiver Tatbestand	138

aa) Tatobjekt.....	138
bb) Tathandlung.....	139
c) Subjektiver Tatbestand	140
d) Strafbestimmungen.....	140
II. Dateneingriff im deutschen Strafrecht.....	140
1. Allgemeines.....	140
2. Objektiver Tatbestand	141
a) Tatobjekt.....	141
b) Tathandlung.....	144
aa) Löschen	144
bb) Unterdrücken.....	145
cc) Unbrauchbarmachen	146
dd) Veränderung.....	147
3. Subjektiver Tatbestand.....	148
4. Rechtswidrigkeit	148
III. Dateneingriff im aserbaidshanischen Strafrecht	149
1. Allgemeines.....	152
2. Objektiver Tatbestand	152
a) Tatobjekt.....	152
b) Tathandlung.....	153
aa) Löschen	153
bb) Beschädigen	153
cc) Beeinträchtigen.....	153
dd) Veränderung.....	154
ee) Blockieren	154
c) Erheblicher Schaden.....	154
3. Subjektiver Tatbestand.....	155
4. Qualifikationstatbestände nach Art. 273 Abs. 2 CM.....	155
5. Zusätzlicher Qualifikationstatbestand nach Art. 273 Abs. 4 CM.....	156
IV. Vergleich des Art. 273 CM mit § 303a StGB im Lichte von europäischen Vorgaben	156
1. Allgemeines.....	156
2. Objektiver Tatbestand	157
3. Subjektiver Tatbestand.....	158
4. Sonstige Unterschiede.....	159

V. Bewertung	159
Kapitel G. Systemeingriff.....	161
I. Internationale Vorgaben	161
1. Cybercrime-Konvention des Europarates	161
a) Allgemeines	161
b) Objektiver Tatbestand	162
aa) Tatobjekt.....	162
bb) Tathandlung.....	163
c) Unbefugt	164
d) Subjektiver Tatbestand	165
2. Rahmenbeschluss 222/2005/JI über Angriffe auf Informationssysteme	165
3. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	165
a) Allgemeines	166
b) Objektiver Tatbestand	166
aa) Tatobjekt.....	166
bb) Tathandlung.....	167
c) Unbefugt	167
d) Subjektiver Tatbestand	168
e) Strafbestimmungen	168
II. Systemeingriff im deutschen Strafrecht.....	169
1. Allgemeines.....	170
2. Objektiver Tatbestand	172
a) Tatobjekt.....	172
aa) Datenverarbeitung	172
bb) Erhebliche Störung.....	173
cc) Wesentliche Bedeutung.....	174
b) Tathandlung.....	176
aa) Die Begehung der Datenveränderung nach § 303b Abs. 1 Nr. 1 StGB.....	176
bb) Die Eingabe oder Übermittlung von Daten nach § 303b Abs. 1 Nr. 2 StGB.....	176
cc) Sabotagehandlungen an Datenverarbeitungsanlage oder Datenträger nach § 303b Abs. 1 Nr. 3 StGB	178
3. Subjektiver Tatbestand.....	180

a) Vorsatz.....	180
b) Versuch.....	180
4. Qualifikationstatbestand.....	181
5. Besonders schwere Fälle.....	182
a) § 303b Abs. 4 Nr. 1 StGB.....	182
b) § 303b Abs. 4 Nr. 2 StGB.....	183
c) § 303b Abs. 4 Nr. 3 StGB.....	183
6. Strafbarkeit der Vorbereitungshandlungen, § 303b Abs. 5 StGB	184
III. Der Systemeingriff im aserbajdschanischen Strafrecht	184
1. Allgemeines.....	185
2. Objektiver Tatbestand	186
a) Tatobjekt.....	186
b) Tathandlung.....	186
c) Unbefugt	187
3. Subjektiver Tatbestand.....	187
4. Qualifikationstatbestand gem. Art. 273 Abs. 3 CM	187
5. Zusätzlicher Qualifikationstatbestand gem. Art. 273 Abs. 4 CM.....	188
IV. Vergleich des Art. 273 Abs. 2 CM mit § 303b StGB im Lichte	
von europäischen Vorgaben	188
1. Objektiver Tatbestand	188
a) Datenverarbeitungen und Computersysteme.....	188
b) Wesentliche Bedeutung	189
c) Erhebliche Störung und schwere Behinderung	190
2. Tathandlung.....	191
3. Subjektiver Tatbestand.....	192
4. Qualifikationstatbestände.....	192
5. Besonders schwere Fälle	193
V. Bewertung.....	195

**Kapitel H. Die Strafbarkeit der Vorbereitungshandlungen der
Computerstraftaten** 197

I. Internationale Vorgaben	197
1. Cybercrime-Konvention des Europarats.....	197
a) Allgemeines	198
b) Objektiver Tatbestand	199

aa) Tatobjekt.....	199
bb) Tathandlung.....	200
c) Unbefugt	201
d) Subjektiver Tatbestand	202
e) Tatbestandseinschränkungen.....	202
2. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	202
a) Allgemeines	203
b) Objektiver Tatbestand	203
aa) Tatobjekt.....	203
bb) Tathandlung.....	204
c) Subjektiver Tatbestand	205

II. Strafbarkeit der Vorbereitungshandlungen der

Computerstraftaten im deutschen Strafrecht 205

1. Allgemeines.....	205
a) Kritiken an der Einführung des § 202c StGB	206
b) Bedenken über die Überkriminalisierung der IT-Branche.....	206
c) Strafanzeige	208
d) Beschluss des Bundesverfassungsgerichts vom 18.5.2009	208
2. Objektiver Tatbestand	210
a) Tatobjekt.....	210
aa) Passwörter oder sonstige Sicherungscodes	210
bb) Computerprogramme	211
b) Tathandlung.....	214
3. Subjektiver Tatbestand.....	216
4. Tätige Reue	217

III. Strafbarkeit der Vorbereitungshandlungen der

Computerstraftaten im aserbaidshanischen Strafrecht 218

1. Allgemeines.....	219
2. Objektiver Tatbestand	220
a) Tatobjekt.....	220
aa) Vorrichtungen und Computerprogramme	220
bb) Computerpasswörter, Zugangscodes oder ähnlicher Daten.....	221
b) Tathandlung.....	221
3. Subjektiver Tatbestand.....	224
4. Qualifikation gem. Art. 273-1 Abs. 4 CM.....	225

IV. Vergleich des Art. 273-1 CM mit § 202c StGB im Lichte von europäischen Vorgaben	225
1. Allgemeines.....	225
2. Objektiver Tatbestand	226
3. Subjektiver Tatbestand.....	228
4. Versuch und Strafantrag.....	230
5. Tätige Rue	230
V. Bewertung	230
<i>Kapitel I. Computerurkundenfälschung</i>	<i>231</i>
I. Internationale Vorgaben	231
1. Cybercrime-Konvention des Europarats.....	231
a) Allgemeines	231
b) Objektiver Tatbestand	232
aa) Tatobjekt.....	232
bb) Tathandlung.....	233
c) Subjektiver Tatbestand	233
II. Computerurkundenfälschung im deutschen Strafrecht	234
1. Allgemeines.....	234
2. Objektiver Tatbestand	235
a) Tatobjekt.....	235
b) Funktionelle Parallelität zur körperlichen Urkunde	236
c) Tathandlung.....	238
3. Subjektiver Tatbestand.....	239
4. Schwere Fälle	240
III. Computerurkundenfälschung im aserbaidischen Strafrecht	241
1. Allgemeines.....	242
2. Objektiver Tatbestand	242
a) Tatobjekt.....	242
b) Tathandlung.....	243
3. Subjektiver Tatbestand.....	244
IV. Vergleich des Art. 273-2 CM mit § 269 StGB im Lichte von europäischen Vorgaben	244
1. Objektiver Tatbestand	245

a) Tatobjekt.....	245
b) Tathandlung.....	245
2. Subjektiver Tatbestand.....	246
3. Weitere Unterschiede.....	247
V. Bewertung	248
<i>Kapitel J. Zusammenfassung</i>	<i>249</i>
<i>Kapitel K. Änderungsvorschläge.....</i>	<i>255</i>
I. Rechtswidriger Zugang zu Daten bzw. Computersystemen.....	255
II. Abfangen von Daten.....	256
III. Vorbereitungshandlungen.....	256
IV. Computerurkundenfälschung.....	257
V. Weitere Reformvorschläge.....	257
<i>Literaturverzeichnis</i>	<i>261</i>