

Inhaltsverzeichnis

<i>Vorwort</i>	V
<i>Abkürzungsverzeichnis</i>	XVII

ERSTER TEIL: EINLEITUNG

<i>Einleitung und sachliche Grundlegung</i>	3
A) Problemstellung	3
B) Methoden und Fragestellungen	8
C) Darstellungsweise	10
D) Forschungsstand	10

ZWEITER TEIL: KODIFIZIERUNG DES COMPUTERSTRAFRECHTS

<i>Erstes Kapitel: Technisch-phänomenologische Grundlegung</i>	15
A) Zentrale Entwicklungsetappen der Computertechnik	15
I. Anstieg der Abhängigkeit von der Technik	15
II. Einstellungswandel gegenüber der Technik	23
III. Veränderungen beim Täterkreis	29
B) Angriffsziele	32
I. Computerspionage	32
II. Datenveränderung	35
III. Computersabotage	36
IV. Verwendung des Hacking zur Tatbegehung	39
C) Charakteristika der Computerkriminalität	43
<i>Zweites Kapitel: Legislatorische Grundlegung – das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität</i>	48
A) Vorarbeiten	48
I. Erste Einschätzungsergebnisse des Bundesministeriums der Justiz	49
II. Die Positionierung der Sachverständigenkommission	51

1. Computerspionage.....	54
2. Computersabotage.....	55
3. Zeitdiebstahl.....	57
B) Gesetzgebungsverfahren zum 2. WiKG.....	58
I. Beratungsergebnisse des Rechtsausschusses vom 6. Juni 1984.....	60
1. Phänomenologische Besonderheiten der Computerkriminalität.....	60
2. Entwicklungstendenzen.....	63
3. Überlegungen zu präventiven Ansätzen.....	67
4. Reformansätze für die Implementierung eines Computerstrafrechts.....	68
a) Computerspionage.....	70
b) Computersabotage.....	71
c) Zeitdiebstahl.....	72
5. Ausblick.....	72
6. Zusammenfassung.....	73
II. Diskussionsschwerpunkte der folgenden Beratungen.....	73
1. Computerspionage.....	74
a) Kodifizierung von Begriffsdefinitionen.....	75
b) Das Erfordernis der besonderen Sicherung.....	77
c) Die Höhe des Strafrahmens.....	78
d) Die Ausgestaltung als Antragsdelikt.....	79
e) Zwischenergebnis zur tatbestandlichen Fassung des § 202a.....	79
f) Positionierung zum Hacking.....	79
2. Computersabotage.....	84
a) Erhöhung des Strafrahmens.....	85
b) Zum Erfordernis des Tatbestandsmerkmals „fremd“.....	86
3. Zeitdiebstahl.....	88
III. Beschlussempfehlung des Rechtsausschusses.....	88

C) Zusammenfassung	90
I. Inhalt und Motive für die Einführung des § 202a i.d.F. des 2. WiKG	90
II. Inhalt und Motive für die Einführung des § 303a i.d.F. des 2. WiKG	92
III. Inhalt und Motive für die Einführung des § 303b i.d.F. des 2. WiKG	94
D) Resümee.....	96

DRITTER TEIL:

KODIFIZIERUNG DES INTERNETSTRAFRECHTS

<i>Drittes Kapitel: Technisch-phänomenologische Grundlegung</i>	101
A) Die Entwicklung des Internets	102
I. Wandel vom militärischen zum wissenschaftlichen Netzwerk....	102
II. Von der passiven Kopplung zum interaktiven Datenaustausch	108
III. Übergang vom Wissensspeicher zum Kommunikationsmedium	110
IV. Phase des sog. Internetting	111
V. Zusammenschluss zum „Netz der Netze“	116
VI. Wandel zum Massenmedium.....	119
VII. Zusammenfassung	121
B) Zentrale Risikofaktoren	123
I. Datenübertragungstechnik als struktureller Risikofaktor	123
II. Risikofaktor Software.....	127
III. Anwender als personelle Risikofaktoren.....	130
C) Phänomenologische Besonderheiten der Internetkriminalität.....	132
I. Internetkriminalität	132
II. Gefährdete Interessen	133
1. Vertraulichkeitsverletzungen.....	134
2. Beeinträchtigungen der Integrität und Verfügbarkeit	140

3. Zusammenfassung	145
III. Empirisch-kriminologische Charakteristika	146
IV. Zusammenfassung	153
<i>Viertes Kapitel: Initiativen des Europarates</i>	156
A) Die Empfehlung Nr. R (89) 9 vom 13. September 1989.....	157
I. Die Bewertung der Ausgangssituation	158
II. Allgemeine Ausführungen zur Ausgestaltung der Empfehlung.....	159
III. Materiell-rechtliche Vorgaben der Empfehlung.....	161
1. Unbefugter Zugang.....	162
2. Unberechtigtes Abfangen von Daten.....	163
3. Beeinträchtigung von Computerdaten und -programmen.....	164
4. Eingriffe in Computersysteme	167
5. Ergänzende Ausführungen.....	168
B) Die Convention on Cybercrime vom 23. November 2001.....	168
I. Allgemeine Ausführungen zum Regelungsgegenstand der Konvention.....	172
II. Grundlegende Begriffsbestimmungen.....	173
III. Materiell-rechtliche Vorgaben zu den sog. CIA-Delikten.....	176
1. Rechtswidriger Zugang gem. Art. 2 CCC.....	176
2. Rechtswidriges Abfangen gem. Art. 3 CCC.....	179
3. Eingriff in Daten gem. Art. 4 CCC.....	180
4. Eingriff in ein System gem. Art. 5 CCC.....	182
5. Missbrauch von Vorrichtungen gem. Art. 6 CCC	184
6. Weitergehende Vorgaben	186
IV. Ausblick zum Anpassungsbedarf für das deutsche Strafrecht....	186
V. Die Bedeutung und Tragweite der Konvention	187
<i>Fünftes Kapitel: Initiativen der Europäischen Union</i>	191
A) Die erste strafrechtliche Harmonisierungswelle	191
B) Die zweite Phase der Strafrechtsharmonisierung.....	195

I.	Frühere Aktivitäten der Kommission.....	196
II.	Die Erarbeitung des Kommissionsvorschlags	197
III.	Inhalt des Kommissionsvorschlags vom 19. April 2002	198
	1. Allgemeine Begriffsbestimmungen in Art. 2 des RB	200
	2. Materiell-rechtliche Vorgaben zu den CIA-Delikten.....	202
IV.	Stellungnahmen der Ausschüsse des Europäischen Parlaments	205
	1. Ergänzungsvorschläge der Ausschüsse	206
	2. Begründungen zu den Stellungnahmen	209
V.	Die Fortsetzung des Verfahrens im Rat der Europäischen Union	210
C)	Die inhaltliche Ausgestaltung der Schlussfassung.....	211
	I. Änderungen bei den Begründungserwägungen.....	211
	II. Änderungen zu den Begriffsbestimmungen in Art. 1 des RB ...	212
	III. Anpassungen bei der Computerspionage in Art. 2 des RB.....	213
	IV. Neuerungen zur Computersabotage in Art. 3 des RB.....	214
	V. Gesonderte Kodifizierung der Datenveränderung in Art. 4 des RB	215
	VI. Änderungen bei der Versuchsstrafbarkeit in Art. 5 des RB.....	216
	VII. Vorgaben zum Strafraumen in Art. 6 und Art. 7 des RB.....	216
	VIII. Sonstige Anpassungen.....	219
	IX. Zusammenfassung der grundlegenden Änderungsansätze des Rates.....	219
D)	Die Rechtswirkung des Rahmenbeschlusses 2005/222/JI	220
E)	Zusammenfassende Beurteilung der Kennzeichen der zweiten Phase der Strafrechtsharmonisierung	224
F)	Die dritte Phase der Strafrechtsharmonisierung.....	225
	I. Strukturell bedingte Interessenlage der klagenden Kommission.....	226
	II. Inhalt des EuGH-Urteils in der Rs. C-176/03.....	227
	III. Zusammenfassung zur Rs. C-176/03.....	230
	IV. Reaktionen auf das Urteil	230

1. Mitteilung der Kommission vom 23. November 2005	230
2. Die Bewertung durch das Europäische Parlament.....	231
3. Die Stellungnahme des Bundesrates vom 10. Februar 2006.....	233
4. Reaktion des EuGH im Urteil zur Rs. C-440/05.....	234
V. Bedeutung der EuGH-Rechtsprechung für die dritte Welle der Strafrechtsharmonisierung.....	236
G) Gemeinsamkeiten und Unterschiede zwischen der Convention on Cybercrime und dem Rahmenbeschluss.....	237
I. Mindestvorgaben hinsichtlich der Grundtermini gem. Art. 1 CCC und Art. 1 des RB.....	238
II. Computerspionage gem. Art. 2 CCC und Art. 2 des RB	239
III. Datenveränderung gem. Art. 4 CCC und Art. 4 des RB.....	240
IV. Computersabotage gem. Art. 5 CCC und Art. 3 des RB	240
V. Versuch, Beihilfe und Anstiftung gem. Art. 11 CCC und Art. 5 des RB	240
VI. Sanktionen gem. Art. 13 CCC und Art. 6 und 7 des RB	241
<i>Sechstes Kapitel: Bewertung der bisherigen Strafrechtsharmonisierung</i>	<i>242</i>
A) Institutionelle Weiterentwicklung.....	243
B) Fortentwicklung der verwendeten Rechtsakte	244
C) Notwendigkeit einer europäischen Strafrechtsharmonisierung.....	245
D) Die thematische Begrenzung der Strafrechtsangleichung.....	249
E) Verfahrensbezogene Kritik zum Erlass konkreter Rechtsakte.....	254
F) Kritik an der inhaltlichen Ausgestaltung der erlassenen Rechtsakte.....	257
<i>Siebentes Kapitel: Die Umsetzung der europa- und völkerrechtlichen Vorgaben in nationales Recht</i>	<i>263</i>
A) Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007	263
I. Inhalt des 41. Strafrechtsänderungsgesetzes.....	265
1. Bezugnahme auf die europäischen Begriffsdefinitionen	265
2. Anpassungen im Bereich der Computerspionage.....	266

3. Hauptkritikpunkte in der parlamentarischen Diskussion	270
4. Kodifizierung des § 202b n.F. über das Abfangen von Daten.....	274
5. Geäußerte Kritik zur Neuaufnahme des § 202b.....	276
6. Die Pönalisierung von Vorbereitungshandlungen durch § 202c-E.....	277
7. Die parlamentarische Debatte zu § 202c-E.....	279
a) Kritik zur Reichweite des § 202c Abs. 1 Nr. 2-E.....	280
b) Kritische Äußerungen zur Fallgruppe des sog. Phishing.....	287
c) Stellungnahme des Rechtsausschusses.....	290
d) Änderungsantrag einzelner Abgeordneter und der Fraktion der Linken vom 23. Mai 2007	291
e) Zusammenfassung zur Reichweite des Art. 202c-E.....	292
8. Erste Reaktionen zur Reichweite des § 202c in der Strafrechtspraxis	293
a) Handhabung durch die Staatsanwaltschaft.....	293
b) Nichtannahmebeschluss des Bundesverfassungsgerichts vom 18. Mai 2009.....	293
c) Stellungnahmen in der Literatur.....	296
9. Antragserfordernis	297
10. Vorgaben zur Datenveränderung und Computersabotage ...	298
11. Kritische Stellungnahmen zur Novellierung durch §§ 303a-E und 303b-E.....	302
a) Einwände gegen die Anpassung des § 303a a.F.....	302
b) Kritik an der Ausgestaltung des § 303b-E.....	303
c) Änderungsantrag einzelner Abgeordneter und der Fraktion der Linken zu § 303b-E	305
12. Sonstige Kritikpunkte.....	306
II. Die Beurteilung durch die Kommission	307
1. Grundlegende Kritikpunkte	308
2. Begrüßende Ausführungen im Schlussbericht.....	309

B) Das Vertragsgesetz zur Convention on Cybercrime	310
C) Zusammenfassung zur Umsetzung	312
<i>Achtes Kapitel: Die Richtlinie 2013/40/EU vom 12. August 2013</i>	315
A) Die vierte Harmonisierungswelle nach dem Vertrag von Lissabon.....	315
B) Die Richtlinie 2013/40/EU vom 12. August 2013	318
I. Phänomenologische Veränderungen	318
II. Zentrale Anknüpfungspunkte des Reformvorhabens	322
III. Einleitung des Gesetzgebungsverfahrens durch die Kommission.....	328
IV. Überarbeitung des Kommissionsvorschlags im Rat	329
V. Zentrale Gestaltungsvorschläge.....	332
VI. Die Erarbeitung der Schlussfassung durch das Parlament.....	336
1. Änderungsvorschläge zu den vorangestellten Erwägungen	338
2. Überarbeitung der materiell-rechtlichen Vorgaben	345
VII. Inhalt der Richtlinie – Gemeinsamkeiten und Unterschiede zu den bisherigen Harmonisierungsvorschriften	351
1. Gegenstand und Erwägungen für den Erlass der Richtlinie....	351
2. Begriffsbestimmungen gem. Art. 2 der RL	353
3. Computerspionage gem. Art. 3 der RL.....	354
4. Computersabotage und Datenveränderung gem. Art. 4 und 5 der RL	355
5. Neuaufnahme des rechtswidrigen Abfangens gem. Art. 6 der RL.....	356
6. Aufnahme der Vorfeldstrafbarkeit in Art. 7 der RL	356
7. Vorgaben zu Anstiftung, Beihilfe und Versuch gem. Art. 8 der RL.....	358
8. Anhebung des Strafrahmens gem. Art. 9 der RL.....	358
9. Formelle Vorgaben in Art. 15 bis 19 der RL	360
C) Zusammenfassung	361

<i>Neuntes Kapitel: Umsetzung der Richtlinienvorgaben in innerdeutsches Recht</i>	363
A) Strafbarkeit der Datenhehlerei gem. § 202d StGB.....	363
B) Korruptionsbekämpfungsgesetz.....	367
C) Gesetzentwurf zum „digitalen Hausfriedensbruch“	372
I. Anknüpfungspunkt und Zielstellung des Entwurfs	373
II. Schutzlücken de lege lata	375
III. Schutzlücken bei der Strafverfolgung	380
IV. Stellungnahmen zum Strafrechtsschutz de lege ferenda.....	382
1. Grundtatbestand, § 202e Abs. 1 StGB-E	382
a) Zugang, § 202e Abs. 1 S. 1 Nr. 1 StGB-E	382
b) Gebrauchsrecht, § 202e Abs. 1 S. 1 Nr. 2 StGB-E.....	385
c) Beeinflussen oder Ingangsetzen, § 202e Abs. 1 S. 1 Nr. 3 StGB-E.....	386
2. Erhöhte Strafandrohung.....	387
3. Versuchsstrafbarkeit und prozessuale Einkleidung	390
V. Stellungnahmen zur Schutzrichtung.....	390
VI. Zusammenfassung	395
VII. Alternativen	396

VIERTER TEIL

<i>Zehntes Kapitel: Würdigung</i>	401
A) Technisch-phänomenologische Grundlegung.....	401
B) Legislatorische Grundlegung – Kodifizierung des Computerstrafrechts durch das 2. WiKG.....	404
C) Zusammenhang zwischen der technischen Weiterentwicklung und der Verlagerung gesetzgeberischer Initiativen in den internationalen Raum.....	406
D) Völker- und europarechtliche Angleichungsbemühungen.....	407
I. Convention on Cybercrime des Europarates vom 23. November 2001	408

II. Der Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005.....	410
III. Die Umsetzung in nationales Strafrecht	412
IV. Richtlinie 2013/40/EU vom 12. August 2013 und ihre Umsetzung.....	414
E) Abschließende Würdigung	418

ANHANG

<i>Quellenverzeichnis</i>	423
<i>Literaturverzeichnis</i>	462