

Inhaltsverzeichnis

Vorwort	V
Einleitung	1
I. Thematische Ausgangslage	1
II. Zielbestimmung der Arbeit	4
III. Methodische Überlegungen	7
IV. Gang der Darstellung	8
Kapitel 1: Strafrecht als transnationale Regelungsmaterie	11
§ 1 Materielle Strafrechtsharmonisierung – Begriffsverständnis	12
A. Rechtsquellen des materiellen Strafrechts	12
I. Arten von Rechtsquellen	12
II. Rechtsquellenübersicht und begriffliche Abgrenzungen	13
III. Weitere Akteure bei der Computerkriminalitätsbekämpfung	15
B. Vereinte Nationen	16
I. Grundstruktur der Vereinten Nationen	16
II. Vereinte Nationen und materielles Strafrecht	18
III. Vereinte Nationen und Computerkriminalität	18
C. Europarat	19
I. Grundstruktur des Europarats und EMRK	20
II. Europarat und materielles Strafrecht	20
III. Europarat und Computerkriminalität	23
§ 2 Das materielle Strafrecht der Europäischen Union	25
A. Rechtsgrundsätze des Strafrechts der Europäischen Union	27
I. Grundsatz der begrenzten Einzelermächtigung	28
II. Subsidiaritätsprinzip	28
III. Verhältnismäßigkeitsprinzip	29
IV. Effizienzprinzip (<i>effet utile</i>)	30
V. Unionstreue	31

VI. Strafrechtliches Schonungsgebot	31
B. Europäische Union und materielles Strafrecht	32
I. Materielles Strafrecht der EU „Prä-Lissabon“	33
II. Materielles Strafrecht der EU „Post-Lissabon“	35
1. Prinzipien europäischer Strafrechtsharmonisierung	36
2. Struktur des Art. 83 AEUV	40
a. Art. 83 Abs. 1 AEUV	40
aa. Art. 83 Abs. 1 UAbs. 1 AEUV	41
bb. Art. 83 Abs. 1 UAbs. 2 AEUV	43
cc. Art. 83 Abs. 1 UAbs. 3 AEUV	45
b. Art. 83 Abs. 2 AEUV	45
c. Art. 83 Abs. 3 AEUV	48
C. Europäische Union und Computerkriminalität	48
I. Unionspolitische Programmatik	48
II. Studien	49
III. Mitteilungen	50
IV. Rahmenbeschlüsse	53
V. Richtlinien	53
§ 3 Zusammenfassung	54
Kapitel 2: Computerkriminalität: Ein Rechtsbegriff	57
§ 4 Begriffsbestimmung und Abgrenzung	
zu verwandten Begriffen	59
A. Forschungsstand zum Computerkriminalitätsbegriff	61
B. Abgrenzung zu weiteren Begriffen	66
I. Internetkriminalität	66
II. Cyberkriminalität	67
III. IuK-Kriminalität, Hightechkriminalität und Multimediale Kriminalität	69
IV. Technisch-informatische Definitionsansätze	70
C. Zusammenfassung	71
§ 5 Die einzelnen Bereiche klassischer Begriffsbestimmungen	71
A. Angriffe auf computergestützte Systeme	71
B. Klassische Delikte unter Verwendung von Computern oder anderer moderner Endgeräte	72
C. Inhaltsbezogene Delikte unter Verwendung von Computern oder anderer moderner Endgeräte	73
D. Delikte gegen das Urheberrecht unter Verwendung von Computern oder anderer moderner Endgeräte	73

§ 6	Problematik eines computerstrafrechtlichen Sammelbegriffs	74
A.	Begriffe als Beschreibung eines Kriminalitätsphänomens	75
B.	Verwendung in der polizeilichen und justiziellen Arbeit	75
C.	Tauglichkeit als Grundlage für internationale Harmonisierungen	76
§ 7	Begrenzende Auslegung des Computerkriminalitätsbegriffs	77
A.	Voraussetzungen des Art. 83 Abs. 1 AEUV	78
I.	Besonders schwere Kriminalität	78
II.	Grenzüberschreitende Dimension	79
B.	Reichweite der Harmonisierungskompetenz des Art. 83 Abs. 1 AEUV	80
I.	Einschränkung der Kriminalitätsbereiche	80
II.	Unklarer Wortlaut durch verschiedene Sprachfassungen . .	82
III.	Möglichkeit der Überprüfung konkreter Harmonisierungsmaßnahmen	82
C.	Auslegung des Computerkriminalitätsbegriffs gem. Art. 83 Abs. 1 AEUV	85
I.	EU-Recht vs. nationales Recht: Rangverhältnis und Auslegungsmethodik	85
1.	Vorrang des Unionsrechts	86
a.	Rechtsfolge des Vorrangs	86
b.	Reaktion auf mitgliedstaatlicher Ebene	87
2.	Auslegungsmethodik im EU-Primärrecht	90
a.	Grundlagen des europäischen Auslegungsvorgangs	91
aa.	Grammatische Auslegung	92
bb.	Systematische Auslegung	93
cc.	Historische Auslegung	93
dd.	Teleologische Auslegung	94
ee.	Rechtsvergleichende Auslegung	96
ff.	Bedeutung für den Auslegungsprozess	96
b.	Methodische Erweiterungen	97
aa.	Weitere Methoden der europäischen Verfassungsinterpretation	98
bb.	„Recht &“-Methoden	100
cc.	Dialog im Europäischen Verfassungsgerichtsverbund	101
II.	Exkurs: Das Bundesverfassungsgericht und die Auslegung strafrechtlicher EU-Kompetenznormen	104
1.	Vereinbarkeit des Lissabon-Vertrags mit deutschem Verfassungsrecht	105

2. Strafrechtsspezifische Elemente des Lissabon-Urteils	105
III. Stellungnahme	107
D. Schranken des EU-Primärrechts im Harmonisierungsprozess	110
I. Subsidiaritätsprinzip	110
II. Verhältnismäßigkeitsprinzip	111
III. Strafrechtlicher Schonungsgrundsatz	112
IV. Stellungnahme	112
§ 8 Computerkriminalität als europäischer Rechtsbegriff	114
A. Grundbedingungen der primärrechtskonformen Begriffsbestimmung	116
B. Klassifizierung anhand von Begehungsmöglichkeiten	117
C. Klassifizierung anhand von Angriffsobjekten	119
D. Entwicklung eines netzwerkspezifischen Computerkriminalitätsbegriffs	120
I. Grundannahmen	120
II. Netzwerkspezifische Computerkriminalität	122
III. Konsequenzen eines netzwerkspezifischen Computerkriminalitätsverständnisses	124
E. Zwischenergebnis und Zusammenfassung	126
Kapitel 3: Harmonisierungen im EU-Computerstrafrecht	129
§ 9 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln	130
A. Exkurs: Rechtsnatur der Rahmenbeschlüsse nach Art. 34 Abs. 2 S. 2 lit. b) EUV a.F. i.V.m. Art. 31 Abs. 1 lit. e) EUV a.F.	130
B. Inhalt und Reichweite des Rahmenbeschlusses 2001/413/JI	132
I. Aufbau und Erwägungsgründe	133
II. Maßgeblicher Inhalt	133
III. Umsetzung in deutsches Strafrecht	134
C. Kritische Auseinandersetzung	134
D. Subsumtion unter den Begriff der Computerkriminalität des Art. 83 AEUV	135
I. Computerstrafrechtlicher Netzwerkaspekt	135
II. Vorbereitungshandlungen als Bestandteil eines Kriminalitätsbereichs	137
E. Zusammenfassung und Bewertung	138

§ 10 Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie	138
A. Richtlinie 2011/93/EU als Weiterentwicklung des Rahmenbeschlusses 2004/68/JI	139
I. Computerbezogene Regelungen	140
II. Umsetzungserfordernisse und Abweichungsmöglichkeiten	141
B. Subsumtion unter den netzspezifischen Computerkriminalitätsbegriff	141
C. Zusammenfassung und Bewertung	146
§ 11 Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	146
A. Aufbau und Erwägungsgründe	148
B. Materiell-rechtlicher Regelungsbereich der Richtlinie	150
I. Rechtswidriger Zugang zu Informationssystemen	150
II. Rechtswidriger Systemeingriff	151
III. Rechtswidriger Eingriff in Daten	151
IV. Rechtswidriges Absfangen von Daten	152
V. Tatwerkzeuge	152
VI. Anstiftung, Beihilfe und Versuch	153
C. Umsetzungsstand in Deutschland	154
D. Subsumtion unter den netzwerkspezifischen Computerkriminalitätsbegriff	155
E. Unterschiede zur Cybercrime Convention	156
I. Cybercrime Convention im Überblick	157
1. Aufbau der Konvention	157
2. Umsetzungsstand und aktueller Diskurs	159
II. Vergleich: „core cybercrime approach“ vs. „comprehensive approach“	160
§ 12 Vorfeldstrafbarkeiten im Computerstrafrecht	162
A. Vorbereitungshandlungen im Strafnormgefüge	162
B. Systematische Kritik an der computerstrafrechtlichen Vorfeldstrafbarkeit	167
C. Verfassungsrecht und computerstrafrechtliche Vorfeldtatbestände	169
D. Untersuchung der (Teil-)Nichtigkeit von Richtlinie 2013/40/EU	173
I. Kompetenzmäßigkeit	177
1. Rechtsvergleichende Aspekte zur Abgrenzung zwischen Polizeirecht und Strafrecht	181
a. Deutsches Recht	183

b. Französisches Recht	188
c. Spanisches Recht	189
d. Stellungnahme	190
II. Materielle Grenzen und mitgliedstaatliche Abweichungsmöglichkeiten	194
1. Identitätsklausel des Art. 4 Abs. 2 S. 1 EUV	195
2. Auslösung des Notbremsemechanismus des Art. 83 Abs. 3 AEUV	200
3. Zwischenergebnis	208
III. Ergebnis zur (Teil-)Nichtigkeit von Richtlinie 2013/40/EU	209
E. Zusammenfassung und Bewertung	210
 Kapitel 4: Perspektiven des EU-Computerstrafrechts	213
§ 13 Informationssysteme als kritische EU-Infrastrukturen	215
A. IuK-Technologien als kritische Infrastrukturen	215
B. Vernetzung in der Europäischen Union	217
C. Vertiefte Integration für eine effektive Strafverfolgung und Bestrafung	218
§ 14 Harmonisierungsmodelle	219
A. Ausbau der Zusammenarbeit	220
B. Ausbau der materiellen Integration	222
I. Europäisches Strafgesetzbuch	222
II. Strafgericht der Europäischen Union	224
III. Internationaler Cybergerichtshof	225
IV. Zwischenergebnis	227
C. Kompetenzausweitung einer Europäischen Staatsanwaltschaft	228
I. Einführung: Die Europäische Staatsanwaltschaft	228
1. Aufgabenbereich	229
2. Institutioneller Aufbau	230
3. Befugnisse	230
4. Aktueller Stand des Verfahrens	231
II. Computerstrafrecht als geeignete Rechtsmaterie für eine Erweiterung	232
1. Bekämpfung transnationaler Kriminalitäts- erscheinungen	233
2. Schutz europäischer Rechtsgüter	234
III. Umfang der Strafverfolgungsbefugnisse	235
§ 15 Ergebnis zu den computerstrafrechtlichen Perspektiven in der EU	239

<i>Inhaltsverzeichnis</i>	XIII
Fazit	241
Literaturverzeichnis	245
Sachregister	267