

## Inhaltsverzeichnis

<b>A. Einleitung</b> .....	17
I. Einführung in die Thematik .....	17
II. Gegenstand der Arbeit .....	19
III. Gang der Untersuchung .....	19
IV. Methodik und Verortung der Arbeit .....	21
<b>B. Das Phänomen der Darknet-Kriminalität</b> .....	23
I. Das Phänomen der Cyberkriminalität .....	23
1. Die Evolution des Begriffs der Cyberkriminalität .....	23
2. Cyberkriminalität im engeren und weiteren Sinne .....	25
3. Dynamische Erscheinungsformen der Cyberkriminalität .....	26
4. Relevante Erscheinungsformen im Jahr 2023 .....	28
II. Die Grundlagen des Darknets .....	31
1. Der Begriff des Darknets .....	31
2. Das Tor-Projekt .....	33
3. Funktionsweise und Nutzung des Tor-Netzwerkes .....	34
a) Die Einwahl ins Tor-Netzwerk .....	35
b) Die Nutzungsmöglichkeiten des Tor-Netzwerkes .....	36
c) Die helle Seite des Tor-Netzwerkes .....	38
III. Der Begriff der Darknet-Kriminalität .....	40
1. Begriffsbestimmung der Darknet-Kriminalität .....	40
2. Differenzierung zwischen Darknet-Kriminalität im engeren, weiteren und weitesten Sinne .....	41
3. Darknet-Kriminalität als Teil der Plattformkriminalität .....	42
IV. Die Erscheinungsformen der Darknet-Kriminalität .....	43
1. Die Grundlagen der Underground Economy .....	43
a) Die Ursprünge der Underground Economy .....	44
b) Die Vertragsabwicklung der Underground Economy .....	45
c) Die Rolle von Kryptowährungen .....	47
d) Die Waren der Underground Economy .....	48

2. Crime as a Service .....	50
3. Der Austausch von Kinderpornographie .....	52
4. Anschlusstaten als Darknet-Kriminalität im weitesten Sinne .....	54
5. Ausschluss der Phänomenbereiche der Hasskriminalität, Cybermobbing und Fake News .....	54
V. Abstrakte rechtliche Einordnung .....	55
VI. Zwischenergebnis .....	56
<b>C. Herausforderungen des staatlichen Umgangs mit Darknet-Kriminalität .....</b>	<b>58</b>
I. Die rechtspolitischen Herausforderungen .....	58
1. Der Rolle der Rechtspolitik .....	58
2. Das Spannungsverhältnis von Freiheit und Sicherheit .....	59
3. Darknet-Kriminalität im Lichte dieses Spannungsfeldes .....	61
a) Effektive Strafverfolgung von Darknet-Kriminalität .....	61
b) Das legitime Bedürfnis nach Anonymität .....	62
c) Weitere klassische Freiheitsrechte des digitalen Raums .....	64
d) Bindung an verfassungsrechtliche Schranken .....	66
e) Chilling effects und weitere Kollateralschäden .....	68
4. Zusammenfassung rechtspolitische Herausforderungen .....	69
II. Die strafprozessualen Herausforderungen .....	70
1. Akteure der Verfolgung von Darknet-Kriminalität .....	70
a) Die deutsche Polizei im Auftrag der Staatsanwaltschaften .....	70
b) Das BKA .....	71
c) Schwerpunktstaatsanwaltschaften für Cyberkriminalität .....	72
d) Das BSI .....	73
e) ZITiS .....	74
2. Geringe Bedeutung von Cyber-Ermittlungsmaßnahmen .....	75
a) Maßnahmen zur Erhebung von Telekommunikationsdaten .....	75
b) Das Scheitern klassischer Cyber-Ermittlungsmaßnahmen bei Ermittlungen im Darknet .....	79
c) Finanzermittlungen .....	80
d) Weitere klassische Ermittlungsmaßnahmen .....	81
3. Erfolgreiche Ermittlungspraxis im Darknet .....	82
a) Zugriff auf öffentlich zugängliche Informationen .....	82
b) Verdeckte personale Ermittlungen .....	85
c) Die staatliche Tatprovokation .....	86

d) Zulässigkeit von Honeypots und Schein-Plattformen? .....	90
e) Computergenerierte Keuschheitsproben .....	91
f) Übernahme von digitalen Identitäten .....	93
g) Ermittlungen an der Schnittstelle zur Realwelt .....	95
h) Durchsuchung und Sicherstellung von digitalen Daten .....	97
i) IT-forensische Auswertung von Daten .....	98
j) Digitale forensische Linguistik .....	99
4. Zusammenfassung strafprozessuale Herausforderungen .....	100
III. Die internationalen Herausforderungen .....	101
1. Die Akteure der europäischen Zusammenarbeit .....	102
2. Die Akteure der internationalen Zusammenarbeit .....	103
3. Rechtshilfe und internationaler Informationsaustausch .....	105
4. Die Bedeutung der Cybercrime-Konvention .....	107
5. Gemeinsame Ermittlungsgruppen .....	109
6. Verwertung von ausländischen Erkenntnissen .....	110
7. Zusammenfassung internationaler Herausforderungen .....	112
IV. Die materiell-rechtlichen Herausforderungen .....	112
1. Der Begriff der Lücke im materiellen Recht .....	113
2. Die Strafwürdigkeit des Betriebs krimineller Plattformen .....	116
3. Erfassung des konkreten Unrechtsgehalts .....	118
a) Handel mit Betäubungsmitteln und anderen Substanzen .....	118
b) Handel mit Waffen, Kriegswaffen und Sprengstoffen .....	120
c) Der Austausch von kinderpornographischen Inhalten .....	121
d) Crime as a Service-Dienstleistungen .....	121
e) Die Beihilfe nach § 27 StGB .....	122
aa) Grundlagen der Beihilfestrafbarkeit .....	122
bb) Die Herausforderungen beim Nachweis der Beihilfe .....	123
cc) Möglichkeiten zur Feststellung einer Haupttat .....	125
dd) Möglichkeiten zur Feststellung eines Vorsatzes .....	126
ee) Das Problem der „vollautomatisierten Plattformen“ .....	128
ff) Das Problem der „neutralen Beihilfe“ .....	130
f) Die Anwendung von Auffangtatbeständen .....	132
aa) Bildung krimineller Vereinigungen (§ 129 StGB) .....	132
bb) Öffentliche Aufforderung zu Straftaten (§ 111 StGB) .....	133
cc) Geldwäsche (§ 261 StGB) .....	134
4. Erfassung des abstrakten Unrechtsgehalts .....	134

a) Geringe praktische Relevanz rein abstrakter Fälle .....	134
b) Anknüpfungspunkte ohne konkrete Nutzertaten .....	135
c) Keine wesentlichen Schutzlücken .....	136
5. Analyse der bisherigen Rechtsprechung .....	136
a) Methodik der Analyse .....	137
b) Deutschland im Deep Web .....	137
c) Cyberbunker .....	139
d) Wall Street Market .....	140
e) Dark Market .....	141
f) Chemical Revolution .....	142
g) Fraudsters .....	143
h) Darknet-Foren „d.cc“ und „g.me“ .....	143
i) Elysium .....	144
j) Boystown .....	145
k) Verfahrensübersicht .....	146
l) Analyse der Ergebnisse .....	148
6. Zusammenfassung materiell-rechtliche Herausforderungen .....	148
V. Zwischenergebnis .....	149
<b>D. Der materiell-rechtliche Ansatz des Gesetzgebers in Gestalt des § 127 StGB</b> ...	150
I. Chronologie des Gesetzesvorhabens .....	150
1. Beschlüsse der Justizministerkonferenz .....	150
2. Koalitionsvertrag der 19. Legislaturperiode .....	151
3. Vorschlag des Landes Nordrhein-Westfalen im Bundesrat .....	152
4. Vorschlag des BMI im Rahmen des IT-Sicherheitsgesetz .....	154
5. Referentenentwurf des BMJ .....	155
6. Gesetzesentwurf der Bundesregierung .....	157
7. Anhörung und Empfehlungen des Rechtsausschusses .....	159
8. Gesetzesbeschluss und Verkündung .....	161
II. Erläuterung der wesentlichen Inhalte .....	162
1. Erläuterungen des objektiven Tatbestands .....	162
a) Das Merkmal des Betreibens .....	162
aa) Das Betreiben als Tathandlung des § 127 StGB .....	162
bb) Der Betreiber als Täter des § 127 StGB .....	163
cc) Unterlassen, Tatdauer und Beendigung .....	164
b) Handelsplattform im Internet .....	166

aa) Der Bestandteil der Plattform .....	166
bb) Der Bestandteil des Handels .....	167
cc) Der Bestandteil des Internets .....	167
c) Kriminelle Zweckausrichtung der Plattform .....	168
d) Rechtswidrige Tat i. S. v. § 127 Abs. 1 StGB .....	169
e) Ermöglichung oder Förderung .....	170
2. Erläuterung des subjektiven Tatbestands .....	171
3. Rechtsfolgen und Subsidiaritätsklausel .....	171
4. Die Qualifikation des § 127 Abs. 3 und 4 StGB .....	172
a) Die Gewerbsmäßigkeit nach § 127 Abs. 3 Alt. 1 StGB .....	172
b) Die bandenmäßige Begehung nach § 127 Abs. 3 Alt. 2 StGB .....	173
c) Die Verbrechensqualifikation des § 127 Abs. 4 StGB .....	173
5. Weitere Regelungen des Änderungsgesetzes .....	174
a) Änderungen § 5 Nr. 5b StGB .....	174
b) Anpassungen in der StPO und Zitiergebot .....	175
III. Kritische Würdigung der geschaffenen Rechtslage .....	175
1. Maßstäbe einer kritischen Würdigung .....	175
2. Kriminalpolitische Betrachtung des § 127 StGB .....	176
a) Kriminalpolitische Erforderlichkeit des § 127 StGB .....	177
aa) Schließung von Lücken im materiellen Recht .....	177
bb) Unzureichende Wertungsmöglichkeiten .....	177
cc) Verhinderung von Gefahren und Prävention .....	179
dd) Die Erfüllung strafprozessualer Bedürfnisse .....	181
ee) Zweckmäßigkeit des materiell-rechtlichen Ansatzes .....	184
ff) § 127 StGB im Lichte kriminalpolitischer Tendenzen .....	187
gg) Zwischenergebnis .....	190
b) Die weiteren Mängel und Defizite des § 127 StGB .....	190
aa) Orientierungspunkte der Zweckausrichtung .....	190
bb) Keine Beschränkungen der Vorfeldstrafbarkeit .....	191
cc) Umfassender sachlicher Anwendungsbereich .....	193
dd) Teilweise ungeeignete Abgrenzungsmerkmale .....	195
ee) Umkehr des Regel- und Ausnahmeverhältnisses .....	197
ff) Leerlaufen der Subsidiaritätsregel .....	198
gg) Hebel für strafprozessuale Ermittlungsbefugnisse .....	199
hh) Extensiver Straftatenkatalog .....	200
ii) § 127 StGB als politisches Strafrecht .....	201
jj) Fehlende Rechtssicherheit durch unklare Merkmale .....	203

kk) Misslungene Regelung zum Strafanwendungsrecht .....	204
ll) Widerspruch zur Beihilfedogmatik .....	205
mm) Zwischenergebnis .....	205
c) Kriminalpolitische Angemessenheit des § 127 StGB .....	206
3. Verfassungsrechtliche Betrachtung des § 127 StGB .....	206
a) Maßstab der Verfassungswidrigkeit von Strafgesetzen .....	207
b) Vereinbarkeit mit dem Bestimmtheitsgrundsatz .....	208
c) Vereinbarkeit mit dem Schuldgrundsatz .....	210
d) Vereinbarkeit mit dem Verhältnismäßigkeitsgrundsatz .....	211
aa) Legitimes Ziel des § 127 StGB .....	211
bb) Geeignetheit des § 127 StGB .....	212
cc) Verfassungsrechtliche Erforderlichkeit des § 127 StGB .....	213
dd) Verfassungsrechtliche Angemessenheit des § 127 StGB .....	215
4. Europarechtliche Betrachtung des § 127 StGB .....	219
a) Das europarechtliche Haftungsregime für Plattformen .....	219
b) Überwachungspflicht durch die Hintertür? .....	221
c) Stellungnahme zur Vereinbarkeit mit EC-RL/TMG .....	224
5. Abschließende Würdigung des § 127 StGB .....	226
IV. Mögliche Konsequenzen für § 127 StGB .....	226
1. Aufhebung des § 127 StGB? .....	227
2. Begrenzung des Anwendungsbereichs des § 127 StGB .....	228
3. Verobjektivierung des Merkmals der Zweckausrichtung .....	231
4. Gesteigerte Vorsatzanforderungen .....	232
5. Überarbeitung des Straftatenkatalogs .....	233
6. Reduzierung des Strafmaßes .....	235
7. Änderung der Regelungsbezeichnung .....	235
8. Sondertatbestand für kinderpornographische Inhalte? .....	235
9. Anpassungen der begleitenden prozessualen Regelungen? .....	236
10. Fazit und zusammenfassender Vorschlag .....	237
E. Alternative Lösungsansätze .....	239
I. Die Bedeutung alternativer Lösungsansätze .....	239
II. Alternative strafprozessrechtliche Lösungsansätze .....	240
1. Vorratsdatenspeicherung und ihre Alternativen .....	240
a) Das Ringen um die Vorratsdatenspeicherung .....	240
b) Das Quick-Freeze Verfahren .....	244

c) Die Login-Falle .....	245
d) Summarische Bewertung .....	246
2. Auflockerung von Schranken oder erweiterte Befugnisse .....	247
a) Ermächtigung zu „milieubedingten“ Straftaten .....	247
b) Grundlage für Honeypots und Schein-Plattformen .....	248
c) Ermächtigung zur Beschlagnahme von Accounts .....	249
d) Grundlage für virtuelle Verdeckte Ermittler .....	250
e) Summarische Bewertung .....	252
3. Mögliche Inpflichtnahme von privaten Dritten .....	252
a) Inpflichtnahme der Darknet-Anbieter .....	253
b) Intensivierung der Kooperation mit Postdienstleistern .....	254
c) Blacklisting von inkriminierten Transaktionen .....	254
d) Summarische Bewertung .....	256
4. Die stärkere Nutzung moderner Informationstechnologie .....	257
a) Die automatisierte Datenerfassung- und Datenverarbeitung .....	257
b) Einsatz von KI in der Strafverfolgung .....	260
c) Monitoring Systeme am Beispiel des Dark Web Monitors .....	263
d) Summarische Bewertung .....	265
III. Alternative finanziell-organisatorische Lösungsansätze .....	268
1. Ausbau personeller Ressourcen .....	268
2. Angemessene Ausbildung und technische Ausstattung .....	270
3. Einführung von spezialisierten Strafkammern .....	271
4. Effektive Nutzung der bestehenden Ressourcen .....	272
5. Prävention und Öffentlichkeitsarbeit .....	273
6. Systematische Löschung von inkriminierten Inhalten .....	273
7. Summarische Bewertung .....	275
IV. Alternative internationale Lösungsansätze .....	275
1. Neue Grundlagen für Rechtshilfe und Datenaustausch .....	276
a) Die Einführung einer E-Evidence-VO .....	276
b) Zweites Zusatzprotokoll zur Cybercrime-Konvention .....	279
c) UN-Cybercrime-Konvention .....	281
2. Weiterentwicklung von Europol .....	282
3. Standards zum Umgang mit elektronischen Beweismitteln .....	283
4. Weitere internationale Harmonisierung des Rechts .....	284
5. Summarische Bewertung .....	285
V. Alternative Ansätze als Teile einer Gesamtstrategie .....	286

<b>F. Zusammenfassung, Kernthesen und Fazit .....</b>	288
I. Zusammenfassung .....	288
II. Kernthesen .....	293
III. Fazit .....	296
<b>Literaturverzeichnis .....</b>	298
<b>Sachwortverzeichnis .....</b>	328