

Internetrecht und Digitale Gesellschaft

Band 61

Der materiell-rechtliche Ansatz des § 127 StGB

**Ein angemessener Umgang mit
den Herausforderungen bei der Verfolgung
von Darknet-Kriminalität?**

Von

Torben Lang



Duncker & Humblot · Berlin

TORBEN LANG

Der materiell-rechtliche Ansatz des § 127 StGB

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 61

Der materiell-rechtliche Ansatz des § 127 StGB

Ein angemessener Umgang mit
den Herausforderungen bei der Verfolgung
von Darknet-Kriminalität?

Von

Torben Lang



Duncker & Humblot · Berlin

Der Fachbereich Rechtswissenschaft
der Johann Wolfgang Goethe-Universität Frankfurt am Main hat diese Arbeit
im Wintersemester 2023/2024 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

D 30

Alle Rechte vorbehalten

© 2024 Duncker & Humblot GmbH, Berlin
Satz: TextFormA(r)t, Daniela Weiland, Göttingen
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 2363-5479

ISBN 978-3-428-19239-7 (Print)

ISBN 978-3-428-59239-5 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2023/2024 vom Fachbereich Rechtswissenschaft der Johann Wolfgang Goethe-Universität Frankfurt am Main als Dissertation angenommen.

Ein besonderer Dank gilt zunächst meinem Doktorvater, Herrn Professor Dr. Matthias Jahn, der mir bereits im Rahmen meiner Themenfindung wichtige Anregungen gab, stets für ein konstruktives Gespräch zur Verfügung stand und mir gleichwohl den erforderlichen wissenschaftlichen Freiraum gewährte. Ein großer Dank gebührt zudem Herrn Professor Dr. Christoph Burchard für die zügige Erstellung des Zweitgutachtens sowie Frau Professorin Dr. Beatrice Brunhöber für die Leitung der Prüfungskommission.

Großen Dank schulde ich außerdem Herrn Tarek Köhler, Frau Dr. Carolin Sauer-
mann (geb. Puscher), Frau Christina Diegel und Frau Hannah-Louise Thonke, die durch ihr zügiges Korrekturlesen und ihre wertvollen fachlichen Kommentare einen großen Anteil zu dem Erfolg dieser Arbeit beigetragen haben. Der größte Dank in dieser Hinsicht gilt jedoch meiner Mutter, Frau Gabriele Lang, die mit Abstand meine unermüdlichste Korrekturleserin gewesen ist.

Von Herzen danken möchte ich auch meiner ganzen Familie sowie meinen Freunden, die mich in dieser anspruchsvollen Phase meines Lebens stets unterstützt haben. In dieser Hinsicht gilt mein größter Dank allerdings vor allem meiner Freundin, Frau Svenja Uhlemann, die mich durch all meine kleineren und größeren Krisen in dieser Zeit begleitet hat und allzeit ein offenes Ohr für meine Sorgen und Nöten hatte.

Frankfurt am Main, Mai 2024

Torben Lang

Inhaltsverzeichnis

A. Einleitung	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. Das Phänomen der Darknet-Kriminalität	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.	Anschlusstaaten 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
C.	Herausforderungen des staatlichen Umgangs mit Darknet-Kriminalität	58
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
D.	Der materiell-rechtliche Ansatz des Gesetzgebers in Gestalt des § 127 StGB ...	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

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

Hinweise zum Auswertungsstand, Zitierung von Internetquellen, Abkürzungen und geschlechterneutraler Sprache

Die in der Arbeit verwendeten Quellen wurden ausgewertet bis zum Stichtag 31. Oktober 2023. Zu diesem Zeitpunkt wurden auch die in der Arbeit zitierten Internetquellen zuletzt abgerufen. Reine Internetquellen sind unmittelbar in den Fußnoten verlinkt. Internetquellen mit erkennbarem Autor wurden mit entsprechender Verlinkung in das Literaturverzeichnis aufgenommen.

Für die Drucklegung wurden nachträglich die nach Einreichung der Arbeit erschienenen Arbeiten von Bächer und Haas sowie die Veröffentlichung der BGH-Entscheidung im sog. Cyberbunker-Verfahren berücksichtigt.

Abkürzungen richten sich – so weit nicht ausdrücklich erläutert – nach Kirchner.¹

Der Verfasser hat sich um geschlechtsneutrale Sprache bemüht. Falls auf eine Doppelnennung oder geschlechtsneutrale Bezeichnungen zugunsten einer besseren Lesbarkeit verzichtet wurden, beziehen sich die verwendeten Personenbezeichnungen stets gleichermaßen auf Personen aller Geschlechter.

¹ *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 8. Aufl. 2015.

Abbildungs- und Übersichtsverzeichnis

Abbildung 1: Erfasste und aufgeklärte CCieS-Fälle des BKA	28
Abbildung 2: Funktionsweise des Tor-Netzwerkes laut BSI	35
Abbildung 3: Hidden Wiki, eigener Screenshot vom 09.12.2021	37
Abbildung 4: BlackMart, eigener Screenshot vom 18.03.2022	45
Abbildung 5: BitPharma, eigener Screenshot vom 18.03.2022	49
Abbildung 6: Dark Web Hackers, eigener Screenshot vom 18.03.2022	51
Verfahrensübersicht der Rechtsprechung zur Darknet-Kriminalität	146

A. Einleitung

I. Einführung in die Thematik

In den letzten Jahrzehnten hat die Digitalisierung unsere Gesellschaft grundlegend verändert.¹ Ein damit einhergehendes Phänomen ist das Aufkommen großer Internetplattformen. Neben den sog. Sozialen Medien, die vornehmlich der Kommunikation, dem Teilen von Inhalten und der Pflege sozialer Beziehungen dienen,² erfreuen sich insbesondere digitale Handelsplattformen, wie *Amazon* und *eBay*, im asiatischen Raum aber etwa auch *Alibaba* und *jd.com* aufgrund ihres reichhaltigen Angebots an Waren und Dienstleistungen großer Beliebtheit.³ Der Vorteil dieser Plattformen für die Kunden ist, dass sie zeitlich flexibel auf ein weitreichendes Angebot an Waren und Dienstleistungen zugreifen können.⁴ Der Vorteil für Händler ist, dass sie keine eigenen Marktstrukturen benötigen und einen direkten Zugang zu einer Vielzahl an potenziellen Abnehmern erhalten.⁵ Im Rahmen dieses sog. E-Commerce⁶ wurde allein in Deutschland im Jahr 2022 ein Umsatz von 90,4 Milliarden Euro erzielt.⁷

Parallel zur fortschreitenden Digitalisierung der Gesellschaft findet bereits seit einiger Zeit auch in verschiedenen Kriminalitätsbereichen eine Digitalisierung statt. Dabei hat sich auch ein Phänomenbereich der sog. Cyberkriminalität entwickelt, bei dem die Strukturen des E-Commerce genutzt werden, um insbesondere im sog. Darknet im großen Stil inkriminierte Waren und Dienstleistungen zu handeln oder andere inkriminierte Inhalte auszutauschen. Aus diesem niedrigschwelligen Zugang zu inkriminierten Waren, Dienstleistungen und Inhalten, resultieren teilweise erhebliche Gefahren für unsere Gesellschaft und die von der Rechtsordnung geschützten Güter. Daher haben sich Strafverfolgungsbehörden in den letzten Jahren vermehrt um die Verfolgung dieser sog. Darknet-Kriminalität bemüht, wobei im Fokus der Ermittlungen regelmäßig die Betreiber derartiger Plattformen standen. Das Betrei-

¹ *Hilgendorf/Kusche/Valerius*, Computer- und Internetstrafrecht, 3. Aufl. 2022, § 5 Rn. 5; *Bär*, in: *Wabnitz/Janovsky* (Hrsg.), *Handbuch Wirtschafts- und Steuerrecht*, 5. Aufl. 2020, Kap. 15 Rn. 1.

² *Taddicken/Schmidt*, in: *Taddicken/Schmidt* (Hrsg.), *Handbuch Soziale Medien*, 2020, S. 3; vgl. auch die Legaldefinition in § 1 S. 1 NetzDG.

³ *Heinemann*, *Der neue Online-Handel*, 13. Aufl. 2022, S. 56 ff.; *Deges*, *Grundlagen des E-Commerce*, 2020, S. 1 ff.

⁴ *Deges*, *Grundlagen des E-Commerce*, 2020, S. 32 f.

⁵ *Deges*, *Grundlagen des E-Commerce*, 2020, S. 30 ff.

⁶ Abkürzung des englischen Ausdrucks Electronic-Commerce = elektronischer Handel.

⁷ Vgl. Statista, *E-Commerce-Umsatz mit Waren in Deutschland in den Jahren 2000 bis 2022*, vom 05.05.2023; weitere Zahlen bei *Heinemann*, *Der neue Online-Handel*, 13. Aufl. 2022, S. 57.

ben einer Plattform, über die inkriminierte Waren und Dienstleistungen gehandelt oder ausgetauscht werden, war durch das deutsche Strafrecht lange Zeit nicht eigenständig unter Strafe gestellt. Vielmehr wurden die Ermittlungsverfahren wegen etwaiger Verstöße gegen das BtMG, das WaffG oder anderen Strafnormen, die nicht gezielt im Zusammenhang mit Cyber- und Darknet-Kriminalität stehen, geführt.

Am 24. Juni 2021 wurde im Deutschen Bundestag in den letzten Atemzügen der ablaufenden 19. Legislaturperiode noch eine Vereinbarung aus dem Koalitionsvertrag des Jahres 2018 umgesetzt und die Einführung einer eigenständigen Strafbarkeit des Betriebens sog. krimineller Handelsplattformen gemäß § 127 StGB n.F.⁸ beschlossen.⁹ Zentrale Begründung für die Einführung dieser neuen Vorschrift war dabei, dass durch das neue Gesetz eine bestehende Strafbarkeitslücke geschlossen werden sollte.¹⁰

Die weit überwiegende Meinung innerhalb der Rechtslehre lehnte die Einführung des § 127 StGB nachdrücklich ab.¹¹ Insbesondere wurde dabei das Bestehen einer Lücke im materiellen Recht vehement bestritten, da das geltende Recht aus Sicht der Rechtslehre bereits vor Einführung des § 127 StGB ausreichend materiellrechtliche Anknüpfungspunkte für eine Verfolgung und sachgerechte Erfassung der Darknet-Kriminalität bot.¹² Für eine Verabschiedung des Gesetzes sprachen

⁸ Bis zur Einführung des § 127 StGB n.F. war in § 127 StGB a.F. die Strafbarkeit der Bildung bewaffneter Gruppen geregelt (nunmehr § 128 StGB n.F.). Sofern in der nachfolgenden Arbeit § 127 StGB genannt wird, ist damit § 127 StGB n.F. gemeint.

⁹ Gesetzesentwurf vom 31.03.2021; Strafbarkeit des Betriebens krimineller Handelsplattformen im Internet und des Bereitstellens entsprechender Server-Infrastrukturen (BT-Drs. 19/28175); Koalitionsvertrag zwischen CDU, CSU und SPD zur 19. Legislaturperiode, 2018, S. 128.

¹⁰ BT-Drs. 19/28175, S. 10 ff.; Gesetzesentwurf des Landes Nordrhein-Westfalen im Bundesrat vom 18.01.2019; Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen (BR-Drs. 33/19), S. 3; BMI, RefE IT-Sicherheitsgesetz 2.0 vom 27.03.2019, S. 78; sowie Koalitionsvertrag zwischen CDU, CSU und SPD zur 19. Legislaturperiode, 2018, S. 128.

¹¹ So etwa: *Jahn*, Stellungnahme vom 05.05.2021 zu BT-Drs. 19/28175, S. 1 ff.; *Zöller*, Stellungnahme vom 29.04.2021 zu BT-Drs. 19/28175, S. 1 ff.; *Rückert*, Stellungnahme vom 03.05.2021 zu BT-Drs. 19/28175, S. 1 ff.; *Brodowski*, Stellungnahme vom 30.04.2021 zu BT-Drs. 19/28175, S. 1 ff.; *Zöller*, KriPoZ 2021, 79 ff.; *Kusche*, JZ 2021, 27 ff.; *Gerhold*, ZRP 2021, 44 ff.; *Eisele*, in: Engelhart/Kudlich/Vogel (Hrsg.), FS Sieber, 2021, S. 757, 765; Kriminalpolitischer Kreis, Stellungnahme vom März 2020 zu § 126a StGB, S. 1 ff.; *Ceffinato*, ZRP 2019, 161 ff.; *Greco*, ZIS 2019, 435 ff.; *Kubicziel/Mennemann*, jurisPR-StrafR 8/2019, Anm. 1; *Laudon*, StRR 2019, 10; *Bachmann/Arslan*, NZWiSt 2019, 241 ff.; *Zöller*, KriPoZ 2019, 274 ff.; *Kubicziel*, Augsburgsburger Papier zur Kriminalpolitik 1/2019, 7 f.; *Bäcker/Golla*, Strafrecht in der Finsternis, Verfassungsblog vom 21.03.2019; *Gercke*, ZUM 2019, 798, 799; *Bartl/Moßbrucker/Rückert*, Angriff auf die Anonymität im Internet, 2019, S. 1 ff.

¹² *Jahn*, Stellungnahme vom 05.05.2021 zu BT-Drs. 19/28175, S. 5 ff.; *Rückert*, Stellungnahme vom 03.05.2021 zu BT-Drs. 19/28175, S. 4 ff.; *Zöller*, KriPoZ 2021, 79, 83; *Zöller*, Stellungnahme vom 29.04.2021 zu BT-Drs. 19/28175, 2 ff.; vgl. auch die Untersuchungen von: *Weber*, Die Strafbarkeit von Plattformbetreibern im Darknet, 2022, S. 78 ff., 298; *Wüst*, Die Underground Economy des Darknets, 2022, S. 67 ff.

sich hingegen vor allem Vertreter der Strafverfolgungsbehörden aus.¹³ Diese argumentierten, dass sie bei der Verfolgung von Darknet-Kriminalität mit zahlreichen Herausforderungen konfrontiert seien und die Erweiterung des materiellen Rechts durch § 127 StGB ein notwendiger Schritt zur effektiven Verfolgung von Darknet-Kriminalität sei.¹⁴

II. Gegenstand der Arbeit

Die vorliegende Arbeit setzt gedanklich an diesem Widerspruch an und untersucht die Frage, ob es sich bei dem vom Gesetzgeber gewählten Ansatz der Ergänzung des materiellen Rechts durch die Vorschrift des § 127 StGB (sog. materiell-rechtlicher Ansatz) um einen angemessenen Umgang mit den Herausforderungen, insbesondere bei der Verfolgung von Darknet-Kriminalität, handelt. Dafür bedarf es zunächst einer grundlegenden Erläuterung des Phänomens der Darknet-Kriminalität sowie einer Analyse der bestehenden Herausforderungen des staatlichen Umgangs mit Darknet-Kriminalität, insbesondere bei deren strafrechtlicher Verfolgung. Erst im Anschluss kann die Angemessenheit des § 127 StGB vollumfänglich bewertet und in Kontrast gestellt werden zu etwaigen alternativen Lösungsansätzen. Das Ergebnis der Untersuchung stellt abschließend eine rechtspolitische Handlungsempfehlung in Form von Kernthesen dar.

III. Gang der Untersuchung

Entsprechend des dargestellten Untersuchungsgegenstandes beginnt die vorliegende Arbeit in einem ersten Schritt mit einer allgemeinen Erläuterung des Phänomens der Darknet-Kriminalität (Kapitel B: *Das Phänomen der Darknet-Kriminalität*). Dabei bedarf es zunächst einer kurzen Einführung in das Phänomen der Cyberkriminalität, da es sich bei der Darknet-Kriminalität um einen speziellen Phänomenbereich der Cyberkriminalität handelt und sich in der Praxis viele Überschneidungen und Zusammenhänge ergeben. Im Anschluss daran wird in die begrifflichen, historischen und technischen Grundlagen sowie die unterschiedlichen Nutzungsarten des Darknets eingeführt. Basierend darauf wird erläutert, wie der Begriff der Darknet-Kriminalität im Sinne der vorliegenden Arbeit zu verstehen ist und welche Erscheinungsformen dessen kohärentem Leitbild zugeordnet werden können. Den Abschluss des Kapitels bildet eine abstrakte rechtliche Einordnung der Darknet-Kriminalität.

¹³ So etwa: *Wullrich*, Stellungnahme vom 30.04.2021 zu BT-Drs. 19/28175, S. 1 ff.; *Piechaczek* (Deutscher Richterbund), Stellungnahme vom Januar 2021 zu BT-Drs. 19/28175, S. 1 ff.; *Goger*, Stellungnahme vom 29.04.2021 zu BT-Drs. 19/28175, S. 1 ff.

¹⁴ *Goger*, Stellungnahme vom 29.04.2021 zu BT-Drs. 19/28175, S. 1 f.; *Wullrich*, Stellungnahme vom 30.04.2021 zu BT-Drs. 19/28175, S. 2.