

Inhaltsverzeichnis

Abbildungsverzeichnis	19
§ 1 Einleitung	21
§ 2 Technische Grundlagen	24
A. Terminologie	24
I. Internet	25
1. Clearnet	25
2. Darknet	26
II. World Wide Web	26
1. Surface Web	27
2. Deep Web	28
3. Dark Web	28
III. Darknet-Technologien in der Praxis	29
1. „Helle Seiten“ und verfassungsrechtlicher Schutz	30
2. Missbrauch zur Begehung von Straftaten	31
3. Forderung eines „Darknet-Verbots“	32
B. Die Anonymisierungstechnologie Tor	32
I. Prinzip des Onion Routing	33
1. Tor-Knoten zur Weiterleitung des Datenverkehrs	34
2. Zufällige Routenwahl durch das Tor-Netzwerk	35
II. TLS-Verschlüsselung der Datenpakete	36
1. Entry-nodes	36
2. Middle-nodes	37
3. Exit-nodes	37
III. Möglichkeiten der Deanononymisierung	38
C. Onion Services und der Tor-Browser	40
I. Onion Services	40
II. Tor-Browser	41
1. Download und Installation	41
2. Surfen im Surface und Deep Web	42
3. Surfen im Tor-basierten Dark Web	44
D. Zusammenfassung	46

§ 3 Straftaten im Tor-Netzwerk	47
A. Rechtstatsächliche Untersuchung	47
I. Strafrechtlich relevante Plattformen	48
1. Handelsplattformen	48
a) Aufbau und Struktur	48
b) „Post-Silk-Road-Ära“	50
c) Postversand der Waren	51
d) Bezahlung mit Kryptowährungen	54
e) Escrow- und Depositsysteme	54
f) Auswirkungen der COVID-19-Pandemie	56
2. Diskussionsforen	57
3. Pädokriminelle Tauschbörsen	59
II. Beteiligte Akteur*innen	61
1. Plattform-Betreiber*innen	61
2. Plattform-Nutzer*innen	63
B. Anwendbarkeit des deutschen Strafrechts auf darknetspezifische Sachverhalte	65
I. Feststellung von Handlungs- und Erfolgsort bei Verwendung der Tor-Software	65
1. Besonderheiten bei abstrakten Gefährdungsdelikten	65
2. Jüngere Rechtsprechung und Abkehr vom Töben-Urteil	66
3. Diskussionen und unterschiedliche Ansichten in der Literatur	67
II. Keine „darknetspezifischen“ Probleme des deutschen Strafanwendungsrechts	68
C. Phänomenologie relevanter Straftatbestände	69
I. Deliktsbereich „Cyberenabled Crime“	70
1. Verstöße gegen die §§ 29 ff. BtMG; § 95 AMG	70
2. Verstöße gegen das Waffengesetz, §§ 51, 52 WaffG	71
3. Handel mit gefälschten Waren und sonstigen Produkten, §§ 146 ff. StGB	73
4. Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte, § 184 b StGB	74
a) Verlagerung der pädokriminellen Szene in das Tor-Netzwerk	75
b) Austausch sogenannter „Grooming Manuals“, § 176e StGB	75
II. Deliktsbereich „Cybercrime as a Service“	77
1. Verbreitung von Schadsoftware, §§ 202c ff. StGB	77

2. Hehlerei mit ausgespähten Daten, § 202d StGB	78
3. Geldwäschdienstleistungen, § 261 StGB	79
4. Betrieb und Steuerung von Botnetzen, §§ 202a f. StGB	80
5. „Doxing“ von personenbezogenen Daten, § 42 BDSG	82
6. Anstiftung zu Kapitaldelikten i.S.d. §§ 212, 211 StGB	82
III. Zwischenergebnis	83
D. Zusammenfassung	84
§ 4 Strafbarkeit der Plattform-Administrator*innen	86
A. Einführung einer eigenen Strafbarkeit für den Plattform-Betrieb	86
I. BR-Drs. 33/19 vom 18.01.2019	87
II. Referentenentwurf IT-Sicherheitsgesetz 2.0	88
1. RefE IT-SiG 2.0 in der Fassung vom 27.03.2019	89
2. RefE IT-SiG 2.0 in der Fassung vom 07.05.2020	90
III. Referentenentwurf des BMJV vom 27.11.2020	90
IV. Regierungsentwurf vom 10.02.2021	91
V. BT-Drs. 19/28175 vom 31.03.2021	91
B. Verhältnis zu den Haftungsprivilegierungen der §§ 8–10 TMG	93
I. Systematische Verortung der §§ 8–10 TMG	94
1. Integrationsmodell	94
2. „Vorfilterlösung“	95
3. Stellungnahme	96
II. Sachlicher und persönlicher Anwendungsbereich	97
1. Sachlicher Anwendungsbereich der §§ 8–10 TMG	97
a) „Informations- und Kommunikationsdienste“	97
b) Ausschlussstatbestand des § 3 Nr. 24 TKG	98
c) Ausschlussstatbestand des § 3 Nr. 25 TKG	98
d) Ausschlussstatbestand des § 2 Abs. 1 RStV	99
2. Persönlicher Anwendungsbereich der §§ 8–10 TMG	99
III. Einzelne telemedienrechtliche Privilegierungstatbestände	100
1. Durchleitung von Informationen i.S.d. § 8 TMG	100
2. Zwischenspeicherung von Informationen i.S.d. § 9 TMG	101
3. Speicherung von Informationen i.S.d. § 10 TMG	101
IV. Wegfall der telemedienrechtlichen Haftungsprivilegierung	102
1. Aktive Rolle bei der Erbringung des Dienstes	102
2. „Zu-Eigen-Machen“ fremder Informationen	104
V. Zwischenergebnis zu B.	105

C. Strafrechtliche Haftung nach spezialgesetzlichen Vorschriften	105
I. Alleintäterschaftliche Strafbarkeit, § 25 Abs. 1 StGB	106
1. Strafvorschriften der §§ 29 ff. BtMG	106
a) § 29 Abs. 1 S. 1 Nr. 1 BtMG	107
b) § 29 Abs. 1 S. 1 Nr. 10 BtMG	108
2. Strafvorschrift des §§ 95 Abs. 1 AMG	109
3. Strafvorschriften der §§ 51, 52 WaffG	109
4. Strafvorschrift des § 184b StGB	111
a) § 184b Abs. 1 Nr. 1 Alt. 1 StGB	111
b) § 184b Abs. 1 Nr. 1 Alt. 2 StGB	112
c) § 184b Abs. 1 Nr. 2 StGB	113
5. Strafvorschrift des § 129 Abs. 1 StGB	114
a) Vereinigungsbegriff des § 129 StGB	114
aa) Personelles Element	114
bb) Zeitliches Element	115
cc) Organisatorisches Element	116
dd) Voluntatives Element	117
b) Tathandlungen nach § 129 Abs. 1 StGB	118
II. Mittäterschaftliche Strafbarkeit, § 25 Abs. 2 StGB	118
1. Gemeinsamer Tatentschluss	119
2. Mittäterschaftlicher Tatbeitrag	120
III. Teilnahmestrafbarkeit, §§ 26, 27 StGB	121
1. Anstiftung, § 26 StGB	121
2. Beihilfe, § 27 StGB	122
a) Teilnahmefähige Haupttat	122
b) „Hilfeleisten“ i.S.v. § 27 StGB	123
c) Förderung von Straftaten Dritter	123
d) Gehilfenvorsatz	124
IV. Zwischenergebnis zu C.	125
D. Rechtliche Würdigung des neuen § 127 StGB	126
I. Keine Erforderlichkeit zur Schließung von Strafbarkeitslücken	126
II. Folgen für die bisherige allein- und mittäterschaftliche Haftung	127
1. Tateinheitliche Idealkonkurrenz zu mitverwirklichten Straftatbeständen	127
2. Zurücktreten des § 127 StGB im Wege der formellen Subsidiarität	127

III. Strafschärfende Vertatbestandlichung von Beihilfehandlungen	128
1. Wegfall der limitierten Akzessorietät	128
2. Keine obligatorische Strafmilderung	129
3. Vorverlagerung der strafrechtlichen Haftung	129
IV. Strafanwendungsrechtliche Besonderheiten	129
V. Stellungnahme	130
E. Zusammenfassung	131
§ 5 Strafrechtliche Ermittlungen im Tor-Netzwerk	133
A. „Klassische“ Internetermittlungen	133
I. Fehlschlagen aufgrund des Onion Routings	134
1. Keine Auskunftserteilung über IP-Adressen	134
a) Surfen im Tor-basierten Dark Web	135
b) Surfen auf Webseiten im Clearnet	136
2. Unbekannte Serverstandorte	137
II. Rückgriff auf alternative Ermittlungsansätze	137
B. Verdeckte Ermittlungsmaßnahmen	138
I. „Online-Streife“ auf Plattformen und Foren	138
II. Nutzung von selbst erstellten „Fake-Accounts“	139
1. Strafprozessuale Ermächtigungsgrundlage	139
a) Verfassungsrechtliche Rahmenbedingungen	140
b) Ermittlungsgeneralklausel aus §§ 161, 163 StPO	141
2. Langfristige Kommunikationsbeziehungen	142
a) Verdeckte Ermittlungen i.S.v. § 110a StPO	144
b) Erforderlichkeit alternativer Ermittlungsansätze	145
III. Übernahme bereits bestehender Online-Profile	146
1. Vorteile der verdeckten Identitätsübernahme	146
2. Zugriff auf bereits bestehende Online-Accounts	147
a) Freiwillige Herausgabe der Login-Informationen	147
b) Beschlagnahme zu Beweis Zwecken, § 94 Abs. 1 StPO	148
aa) Begriff des „Gegenstands“ i.S.d. § 94 Abs. 1 StPO	148
bb) Potentielle Beweisbedeutung der Online-Accounts	149
c) Beschlagnahme zur Sicherung der Einziehung, § 111b StGB	149
aa) Einziehungsfähige Gegenstände i.S.d. § 74 Abs. 1 StGB	149

bb) Anordnungsvoraussetzungen des § 111b Abs. 1 StPO	150
d) Vollzug durch Abänderung der Login-Informationen	150
e) Keine Verpflichtung zur aktiven Preisgabe der Zugangsdaten	151
f) Anderweitige Ermittlung der benötigten Login-Informationen	151
aa) Im Rahmen der Online-Durchsuchung i.S.v. § 100b StPO	152
bb) Passive Duldung des Zugriffs auf die Online-Accounts	152
g) Einziehung der Online-Accounts, § 74 Abs. 1 StGB	153
h) Zwischenergebnis	153
3. Übernahme der Online-Profile für verdeckte Ermittlungen	154
a) Eingriff in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG	154
b) Ermittlungsgeneralklausel aus §§ 161, 163 StPO	156
c) Kein bloß geringfügiger Grundrechtseingriff	157
4. Einwilligung in die Weiterführung der Online-Profile	157
5. Nutzung der Online-Accounts gegenüber Dritten	158
a) Unzulässigkeit von täuschungsbedingten Selbstbelastungen	158
b) Sonstige verfassungsrechtliche Rahmenbedingungen	160
c) Initiierung neuer Kommunikationsbeziehungen	162
d) Eingriff in laufende Gesprächskontakte	162
aa) Inkrimierte Kommunikationsverhältnisse	163
bb) Schutzwürdige Kommunikationsverhältnisse	163
cc) Kein Rückgriff auf § 110a StPO Abs. 1 StPO	164
6. Reformvorschlag aus dem RefE IT-Sicherheitsgesetz 2.0	165
a) Entwurfsregelung des § 163g StPO-E	165
b) Rechtliche Würdigung des § 163g StPO-E	166
c) Streichung der Vorschrift des § 163g StPO-E	167
7. Zwischenergebnis zu III.	168
C. Testkäufe von inkriminierten Waren	168
I. Zulässigkeit von staatlichen Tatprovokationen	169
1. Entwicklungen in der jüngeren Rechtsprechung	169
2. Auftritt von Ermittler*innen als Käufer*innen	170
3. Auftritt von Ermittler*innen als Verkäufer*innen	172
II. Daktyloskopische und serologische Untersuchungen	172

III. Auskunftsverlangen gegenüber Postunternehmen	173
1. Zugriff auf Kund*innen- und Sendungsdaten	174
a) „Tracking“ von Paketen mit illegalen Inhalten	174
b) Observation von Postfilialen und Packstationen	174
2. Rechtsgrundlage für die Beauskunftung über Postdaten	175
b) Gewahrsamerfordernis des § 99 S. 1 StPO a.F.	176
c) Ermittlungsrichterlicher Beschluss des BGH	176
d) Keine retrograde Beauskunftung über Postdaten	177
3. Ausweitung des § 99 StPO durch das StPO- Fortentwicklungsg	177
a) Rechtslage seit Inkrafttreten der Norm am 01.07.2021	178
b) Ergänzung der Vorschrift um § 99 Abs. 2 StPO	178
aa) Kritik an der Neufassung aus der Strafrechtspraxis	179
bb) Stellungnahme und rechtliche Würdigung	180
D. Technische Ermittlungsmaßnahmen	181
I. Einsatz computergenerierter Missbrauchsabbildungen	181
1. Forderung sogenannter „Keuschheitsproben“	182
2. Einführung der §§ 184b Abs. 6 StGB, 110d StPO	183
3. Technische Möglichkeiten der Umsetzung	183
a) Erstellung von Drahtgittermodellen	183
b) Computergenerierter Chatbot „Sweetie“	184
c) Einsatz von Deep-Learning-Verfahren	186
d) Methoden des maschinellen Lernens	187
e) Erkennbarkeit aus Sicht der Multimedia-Forensik	188
4. Zwischenergebnis	189
II. Geolokalisierung von Dateien über EXIF-Metadaten	189
1. Upload von Bild- und Videodateien im Tor-Netzwerk	190
2. Gespeicherte EXIF-Metadaten und GPS-Koordinaten	190
3. Rechtsgrundlage für das Aufrufen der Dateieigenschaften	191
4. Ausschaltung oder Löschung der EXIF-Metadaten	192
III. Nachladen von externen Dateieinbettungen	192
1. Vorgehensweise der Ermittler*innen beim „IP-Tracking“	193
2. „IP-Tracking“ von Tatverdächtigen aus dem Tor- Netzwerk	194
3. Rechtsgrundlage für das „IP-Tracking“	195
IV. Quellen-Telekommunikationsüberwachung	196
1. TLS-Verschlüsselung beim Onion Routing	197
2. Aufspielen von Überwachungsprogrammen	197

3. Weitergehende ermittlungsrelevante Hinweise	198
V. Online-Durchsuchung	198
1. Ausleiten von ermittlungsrelevanten Informationen	199
2. Beschlagnahme und Entschlüsselung von Datenträgern	199
VI. Forensisches Hacking zur Serverlokalisierung	200
1. Auffinden und Ausnutzen von Sicherheitslücken	200
2. Erforderlichkeit einer Ermächtigungsgrundlage	201
a) Kein „staatliches Hacking“ i.S.d. §§ 100a, b StPO	201
b) Erhebung von Verkehrsdaten i.S.d. § 100g StPO	202
3. Lokalisierung von Webservern anhand ihrer IP-Adressen	202
4. Erforderlichkeit weiterer Ermittlungsmaßnahmen	203
5. Einholung von Bestandsdatenauskünften i.S.d. § 100j StPO	204
6. Praxisbeispiel der pädokriminellen Tauschbörse „Elysium“	204
VII. Beschlagnahme von Speichermedien und Datenbeständen	205
1. Entschlüsselung von beweisrelevanten Datenträgern	205
2. Praxisbeispiel des Diskussionsforums „DiDW“	206
3. Durchsicht beweisrelevanter Daten, § 110 StPO	207
4. Nutzung von externen Hosting-Dienstleistungen	207
a) Räumlich getrennte Speichermedien innerhalb Deutschlands	208
aa) Durchsuchung bei den Hosting-Dienstleister*innen	209
bb) Kein Zugriff auf „Bulletproof-Hosting-Services“	209
b) Räumlich getrennte Speichermedien außerhalb Deutschlands	210
c) Erforderlichkeit der Einholung von Rechtshilfersuchen	210
aa) Zugriff auf im EU-Inland gespeicherte Daten	211
(1) Richtlinie 2014/41/EU vom 03.04.2014 über die EEA	211
(2) Vorschlag der EU-Kommission zur E-Evidence-VO	212
bb) Zugriff auf Daten im Geltungsbereich der CCC	213
(1) Geltungsbereich der Cybercrime-Konvention	213
(2) Rechtshilfersuchen i.S.d. Art. 31 Abs. 1 CCC	214
cc) Sonstige bi- oder multilaterale Übereinkünfte	214

d) Unbekannte Serverstandorte	215
aa) Zulässigkeit des Zugriffs auf nicht-lokalisierbare Daten	216
bb) Keine vorherige Einholung von Rechtshilfeersuchen	216
5. Beschlagnahme und Abschaltung von lokalisierbaren Servern	217
6. Beschlagnahme der dazugehörigen Onion-Domains	217
VIII. Einsatz von behördlichen Honeypot-Servern	219
1. Praxisbeispiel der Handelsplattform „Hansa Market“	219
2. Weiternutzung zur Begehung von Straftaten	220
3. Zulässigkeit der Übernahme von kriminellen Plattformen	220
a) Verwirklichung verschiedener Straftatbestände	221
b) Keine gesetzliche Befugnisnorm in Deutschland	222
4. Möglichkeit des polizeilichen Datenaustauschs	223
IX. Abgreifen von Zugangsdaten mittels Phishing	223
1. Zulässigkeit des Betriebens von Phishing-Webseiten	224
a) Ermächtigungsgrundlage des § 100b StPO	224
b) Ermächtigungsgrundlage des § 100h StPO	225
c) Kein Rückgriff auf die §§ 161, 163 StPO	225
2. Kein Abgreifen von Zugangsdaten mittels Phishing	226
X. Nutzung von Open Source Intelligence (OSINT)	226
1. Manuelle Suche nach relevanten Informationen	227
2. Automatisierte Datenerhebung und -auswertung	227
a) Kooperationsprojekt „Dark Web Monitor“	228
b) Praxisbeispiel der Handelsplattform „Silk Road“	229
3. Rechtsgrundlage für OSINT-Ermittlungen	230
a) Grundrechtsrelevanz von OSINT-Ermittlungen	231
b) Ermächtigungsgrundlage des § 98a StPO	231
c) Rückgriff auf die §§ 161, 163 StPO	232
aa) Manuelle OSINT-Ermittlungen	232
bb) Automatisierte OSINT-Ermittlungen	233
(1) Vorliegen eines Anfangsverdachts	233
(2) „Monitoring“ mit anonymisierten Daten	234
(3) Datenschutzrechtliche Bestimmungen	235
(4) Qualitatives Element	236
(a) Bloß geringfügige Persönlichkeitsrelevanz	236

(b) Praxisbeispiel des Crawlings von Verkaufsangeboten	236
(c) Erstellung von Persönlichkeits- und Bewegungsprofilen	237
(5) Quantitatives Element	238
(6) Algorithmisches Element	238
(7) Zeitliches Element	239
cc) Zusammenfassung	240
4. Zwischenergebnis zu X.	240
XI. Auswertung der Bitcoin-Blockchain	241
1. Bitcoin als meist genutztes Zahlungsmittel im Tor-Netzwerk	242
a) Öffentlich einsehbare Transaktionshistorie im Bitcoin-System	243
aa) Erstellung von Schlüsselpaaren aus <i>public</i> und <i>private keys</i>	243
bb) Manuelle Einsicht und Auswertung von Transaktionsvorgängen	244
cc) Beispiel des Bitcoin-Spendenkontos von „DiDW 3.0“	245
b) Softwaregestützte Auswertung der Bitcoin-Blockchain	246
c) „Know your customer“-Prinzip, §§ 2 Abs. 1, 10 ff. GwG	247
2. Gegenmaßnahmen zur Verschleierung von Transaktionsvorgängen	248
E. Zusammenfassung	248
§ 6 Gesamtergebnis der Untersuchung	253
A. Ergebnisse auf rechtstatsächlicher Ebene	254
B. Ergebnisse auf telemedienrechtlicher Ebene	255
C. Ergebnisse auf materiell-strafrechtlicher Ebene	255
D. Ergebnisse auf strafprozessualer Ebene	257
Literaturverzeichnis	263