Studienarbeit im Rahmen eines Schwerpunktseminars
im Sommersemester 2018 an der
Ernst-Moritz-Arndt Universität Greifswald

„Das Darknet – Schutzraum für politisch verfolgte oder Tummelplatz für Kriminelle?“

Zur Verfügung gestellt für
Dr. Brauer Rechtsanwälte
www.die-anwalts-kanzlei.de/darknet-anwalt/

Dr. Brauer
Rechtsanwälte

Inhaltsverzeichnis

A. Einleitung

Mit zunehmender Häufigkeit kommt seit geraumer Zeit in der Öffentlichkeit das sogenannte Darknet zur Sprache: Ein Ort innerhalb des Internets, der den dort agierenden Personen ohne jegliche Regeln oder Kontrolle sämtliche Freiheiten einräumen soll, die innerhalb der regulierten Bereiche des Internets so nicht vorstellbar sind. Was genau sich jedoch hinter diesem Begriff verbirgt, ist für viele jedoch weiterhin unklar. Die Bezeichnung Darknet zeichnet dabei zunächst einmal ein düsteres Bild. Häufig werden im Zusammenhang mit dem Darknet Abbildungen von dunklen Gestalten gebraucht, deren Gesichter hinter einem Kapuzenpullover versteckt sind.

Dieser Eindruck wird dadurch verstärkt, dass in den Medien häufig berichtet wird, wie das Darknet von Kriminellen als Umschlagplatz für Drogen, Waffen oder andere illegale Güter genutzt wird. Das Darknet sieht sich daher auch von staatlichen Stellen demselben Vorwurf ausgesetzt, der auch in der Vergangenheit gegenüber zahlreichen anderen Verschlüsselungssystemen erhoben worden ist:

Die Schaffung von abhörsicheren Kommunikationsmöglichkeiten behindert die staatliche Verfolgung von Terrorismus und Kriminalität.[1] Immer wieder werden daher Forderungen nach der Schaffung staatlicher Zugriffsmöglichkeiten auf verschlüsselte Kommunikationsmöglichkeiten gestellt. Die Möglichkeit zur anonymen Kommunikation bietet gleichzeitig jedoch auch vielen Menschen Schutz, die aus verschiedenen Gründen unter Verfolgung und Zensur zu leiden haben.

Dies wirft letztendlich folgende Frage auf: Überwiegen die durch die Möglichkeit zur anonymisierten Kommunikation geschaffenen positiven gesellschaftlichen Wirkungen die neu entstehende Infrastruktur für Kriminalität? Im Verlauf dieser Arbeit soll daher zur Beantwortung dieser Frage nach einer allgemeinen Darstellung des Darknets zunächst die Bedeutung des Darknets für die unterschiedlichen Arten der Kriminalität dargestellt werden, um nach einer anschließenden Darstellung der positiven Aspekte eine Gesamtwürdigung vornehmen zu können.

B. Das Darknet – Begriff und Funktionsweise

Das Internet lässt sich lose in drei unterschiedliche Bereiche unterteilen. Das sogenannte Clearweb[2] umfasst den frei zugänglichen Teil des Internets. Hierunter fallen sämtliche Webseiten oder Dokumente, welche von den gängigen Suchmaschinen indexiert oder in Webverzeichnissen aufgelistet sind.

Die Inhalte des Internets, welche nicht von Suchmaschinen indexiert werden, bei denen eine Indexierung bewusst vermieden wird oder deren Erreichbarkeit durch Zugangssperren oder Passwörter eingeschränkt wird, werden in ihrer Gesamtheit als

1 Siehe hierzu: *Schulze,* Media and Communication 2017, 54.

2 Auch Surface Web oder Visible Web genannt.

Deep Web[3] bezeichnet. Dieses Deep Web macht nach Schätzungen bis zu 96 Prozent aller Internetseiten aus.[4] Hierzu gehören beispielsweise Datenbanken, E-Mail-Konten oder veraltete Webseiten oder Hyperlinks. Einen Unterbereich des Deep Web stellt das sogenannte Darknet dar. Hierbei handelt es sich um Inhalte, auf welche nur mit Hilfe spezieller Anonymisierungssoftware zugegriffen werden kann.

Das bekannteste und für die Praxis bedeutendste Anonymisierungsmittel ist der sogenannte TOR-Browser, wobei TOR für „The Onion Routing" steht, es etablieren sich jedoch auch zunehmend Alternativen zu TOR, exemplarisch seien hier Freenet[5] und Invisible Internet Project (I2P) genannt.

Aufgrund der aktuell bestehenden herausragenden Bedeutung des TOR-Netzwerkes soll in dieser Arbeit nur dieses System in seinen Grundzügen exemplarisch für die Funktionsweise des Darknets dargestellt werden. Im englischen Sprachgebrauch wird in Bezugnahme auf den TOR-Dienst auch die Bezeichnung *Onionland* für das Darknet gebraucht[6], in deutschen Foren wird diesbezüglich auch von der *Zwiebel* gesprochen.

Zunächst benötigt der Nutzer einen TOR-Client. Dieser wählt aus einer Liste von TOR-Servern eine zufällige Route über drei TOR-Knotenpunkte zum gewünschten Inhalt aus. Die Datenpakete des Nutzers werden nun zusammen mit seiner IP-Adresse verschlüsselt und an den Eintrittsknoten (Entry Node) verschickt, welcher die Daten über einen Zwischenknoten (Relay) zum Austrittsknoten (Exit Node) weiterleitet.

Hierbei sind jedem Server nur die anderen Server bekannt, mit denen er in einem unmittelbaren Kontakt steht. Der Zwischenknoten kennt somit beispielsweise den Eintritts- und den Austrittsknoten, nicht jedoch Absender oder finalen Empfänger der Daten. Der Client wiederholt dieses Vorgehen in regelmäßigen Abständen, so dass die zur Verbindung genutzten Server alle 10 Minuten gewechselt werden. Diese schichtartige Verschlüsselungsweise zeigt auch, weshalb die Zwiebel als Symbol und Namensgeber dieses Systems gewählt worden ist.

Da somit nicht die IP-Adresse des eigentlich auf die Webseite zugreifenden Nutzers, sondern stattdessen die eines TOR-Servers protokolliert wird, können Nutzer so grundsätzlich anonym auf Inhalte im Internet zugreifen, da zur Identifizierung des Nutzers die Verbindungsdaten sämtlicher genutzten TOR-Server einer verwendeten Route erforderlich wären, diese ihre entsprechenden Daten jedoch regelmäßig löschen und auch häufig im Ausland betrieben werden, was die faktischen Möglichkeiten zur Nachvollziehung von Nutzern massiv einschränkt.[7]

---

3 Auch Hidden Web oder Invisible Web genannt.

4 *Hostettler,* S. 17 f.

5 Nicht zu verwechseln mit dem gleichnamigen Telekommunikationsunternehmen, vgl. auch https://freenetproject.org (Zuletzt abgerufen am 20.03.2018).

6 *Hostettler,* S. 18.

7 Kindhäuser/Neumann/Paeffgen/*Kretschmer,* StGB § 145d Rn. 25; *Kochheim,* Rn. 1325.

Zugriffe auf das Darknet erfolgen aktuell weitestgehend über stationäre Rechner, aber auch für mobile Geräte wie Tablets oder Mobiltelefone werden zunehmend Möglichkeiten zur Nutzung des TOR-Netzwerkes entwickelt. So existieren aktuell bereits mehrere entsprechende Applikationen sowohl für iOS- als auch für Android-betriebene Mobiltelefone.

Die Struktur einer Zieladresse einer Webseite im TOR-Netzwerk unterscheidet sich häufig ebenfalls vom Clearweb, so setzen sich die meisten nur über einen TOR-Browser erreichbaren Adressen aus einer keinen eigenen Sinn ergebenden Reihenfolge von Zahlen und Buchstaben mit dem Abschluss .onion zusammen.[8]

Die Anzahl der nur ein solches TOR-System zu erreichenden Seiten bewegt sich dabei in den letzten Jahren im Wesentlichen zwischen 50.000 und 60.000 Webseiten.[9] Das Anzeigen einer Webseite über den TOR-Browser dauert im Verhältnis zu der Nutzung eines regulären Browsers deutlich länger.

Dies hat verschiedene Gründe. Neben dem Umstand, dass ein Verbindungsaufbau über mehrere Zwischenserver zusätzliche Zeit benötigt, kann der Verbindungsaufbau auch dadurch verlangsamt werden, dass das TOR-System versucht, die jeweiligen Routen über Server in verschiedenen Staaten aufzubauen.

Hinzu kommt, dass die Relaisserver in einer dezentralisierten Struktur von Freiwilligen betrieben werden, was zu einem Kapazitätsgefälle bei den verschiedenen Servern führt.

Zu beachten ist, dass es sich beim Begriff des Darknets keineswegs um einen klar definierten technischen Begriff handelt. So existiert neben dem bereits dargestellten weiten Begriffsverständnis auch eine Auffassung, die die Begrifflichkeit des Darknets auf geschlossene Peer-to-Peer-Netzwerke bezieht, in welchen die Kommunikation über verschlüsselte Direktverbindungen erfolgt.[10]

Im weiteren Rahmen dieser Arbeit wird jedoch das weite Begriffsverständnis des Darknets zu Grunde gelegt.

C. Das Darknet als Tätigkeitsfeld für Kriminalität

Die Nutzung eines TOR-Netzwerkes stellt aufgrund der dargestellten Möglichkeiten zum anonymen Auftreten im Internet ein attraktives Betätigungsfeld für Straftäter dar. Vor diesem Hintergrund ist es wenig überraschend, dass mehrere Studien zu dem Ergebnis gekommen sind, dass rund die Hälfte der nur über einen TOR-Browser auf-

8 Die Adresse des Darknet-Suchdienstes Torch lautet beispielsweise: http://xmh57jrzrnw6insl.onion/ (Zuletzt abgerufen am 27.03.2018).
9 Vgl.: https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2016-01-01&end=2018-02-15 (Zuletzt abgerufen am 20.03.2018).
10 *Kochheim,* Rn. 401.

rufbaren Seiten illegale Inhalte aufweisen.[11] Im Folgenden sollen die unterschiedlichen Arten von Kriminalität, welche über das Darknet erfolgen, sowie die dazu genutzten Strukturen dargestellt werden. Der Begriff der Kriminalität orientiert sich hierbei an den strafrechtlichen Gesetzten der Bundesrepublik Deutschland, bestimmte Kommunikationsweisen oder Inhalte, die beispielsweise von autoritär geführten Staaten als illegal betrachtet werden, sowie politischer Aktionismus, der auch in der Bundesrepublik die Grenzen der Strafbarkeit überschreiten kann, sind aus dieser Darstellung bewusst ausgeklammert.

I. Grundstrukturen

Als Infrastruktur für Kriminalität im Darknet dienen häufig im TOR-Netzwerk betriebene virtuelle Schwarzmärkte. Diese Märkte nehmen unterschiedliche Gestalt an, während manche Märkte insbesondere die größeren Strukturen des legalen Onlinehandels übernehmen und als dritte Person zwischen Käufern und Verkäufern vermittelnd auftreten, handelt es sich bei anderen Märkten um Kleinanzeigenportale oder Foren, über welche die Beteiligten den Kontakt zueinander aufbauen. Insbesondere die größeren Märkte erwirtschaften durch dieses System auch eigene Gewinne, da sie für die von ihnen angebotenen Dienste Gebühren verlangen. Die erschwerte Rückverfolgbarkeit der Nutzer im Darknets bietet hierbei Möglichkeiten für illegale Transaktionen, welche so bisher nur für den klassischen Onlinehandel im Clearweb bestanden. So verfügte beispielsweise der Darknet-Marktplatz Silk Road über ein Treuhanderkontosystem sowie ein Bewertungssystem, mit dem getätigte Transaktionen bewertet werden können und dass den Händler die Möglichkeit eines Reputationsaufbaues bietet.[12] Diese Strukturen ermöglichen auch technisch verhältnismäßig unerfahrenen Käufern einen einfachen Zugang zum Erwerb unterschiedlicher krimineller Leistungen oder Waren. Viele Märkte verfügen auch über ein System zur Streitschlichtung, um aus den Transaktionen resultierende Streitigkeiten zwischen den Parteien beizulegen. Manche Händler bieten auch die Möglichkeit zur Rücksendung der Ware und Rückerstattung des Kaufpreises an.[13] Solche Leistungen, wie sie sonst nur bei legalem Warenhandel üblich sind, stellen einen wesentlichen Unterschied zu den analogen Märkten für illegale Waren dar. Neben diesen Märkten bieten manche Händler auch eigene Geschäftsseiten im Darknet an, welche in der Regel auf bestimmte Dienstleistungen oder Produkte spezialisiert sind.[14] Die Kommunikation zwischen den Parteien wird regelmäßig über die eigenen Nachrichtensysteme der Märkte abgewickelt, wobei eine zusätzliche Ende-zu-Ende-Verschlüsselung der Nachrichten durch die Nutzer möglich ist.

11 *Intelliagg*, Shining a light on the dark web, siehe S. 9 der PDF-Datei (48% illegale Inhalte nach US. und britischem Recht betrachtet); *Moore/Rid,* Cryptopolitik and the Darknet, siehe S. 16 der PDF-Datei (ca. 56% illegale Inhalte nach allgemeinen Maßstäben betrachtet); ähnlich auch: *Owen/Savage,* The Tor Dark Net, siehe S. 12 der PDF-Datei (Ohne genaue Klassifizierung der Legalität der Inhalte).

12 *Christin,* Traveling the Silk Road, S. 12 ff. der PDF.

13 *Paoli/Aldridge/Ryan/Warnes,* Behind the curtain, S. 84 der PDF.

14 *Paoli/Aldridge/Ryan/Warnes,* Behind the Curtain, S. 33 der PDF.

Als Währung haben sich auf diesen Märkten unterschiedliche Kryptowährungen, von denen Bitcoin die bekannteste und wohl meistgenutzte darstellt[15], durchgesetzt. Hierbei handelt es sich um digitale Parallelwährungen, welche über das Internet durch Peer-to-Peer-Anwendungen ausgetauscht werden und ohne eine zentrale Abwicklungsstelle auskommen. Die Transaktionen sind dabei grundsätzlich allesamt öffentlich einsehbar[16], eine Identifikation der Transaktionspartner scheitert in der Regel jedoch an dem Umstand, dass Nutzer nur pseudonymisiert erfasst werden.

Als denkbare Alternative zu Kryptowährungen besteht die Möglichkeit zur Zusendung von Banknoten per Post, auch als cash-per-post bezeichnet.[17] Dieses System schafft jedoch für den Händler Gefahren durch die Zustellung des Geldes und dürfte auch für den Käufer in Ermangelung eines Treuhändersystems weniger attraktiv als die Nutzung von Kryptowährungen sein.

Für die Versendung im Darknet erworbener illegaler Waren stehen mehrere unterschiedliche Varianten zur Verfügung. Hierzu können beispielsweise leerstehende Häuser oder Wohnungen genutzt werden, die als Lieferadresse angegeben werden und an denen der Käufer die bestellen Waren von einem Paketboten entgegennehmen kann oder bei denen ein Ablageort mit dem Zusteller vereinbart wird. Weiterhin können bei leerstehenden Häusern oder Mehrfamilienhäusern auch ungenutzte oder zusätzlich angebrachte Briefkästen vom Empfänger genutzt werden.

Ebenfalls nutzbar ist das Packstationssystem der Deutschen Post. Da eine Überprüfung der Identität des Absenders nicht erfolgt, und der Empfänger unter Verwendung einer falschen Identität, welche er beispielsweise im Darknet erworben oder anderweitig erlangt hat, auf die Sendung zugreifen kann, stellt dieses Vorgehen einen effektiven Weg zur Zustellung von im Darknet erworbenen Waren dar.[18] Weiterhin ist denkbar, eine Direktzustellung per Post an den Empfänger über Mittelsmänner durchzuführen. Zur Vermeidung der durch die Nutzung des Postsystems entstehenden Risiken kann auch das sogenannte *dead drop*-Modell genutzt werden. Hierbei wird die Zustellung über einen als Dienstleister hinzugezogenen Dritten durchgeführt, welcher die Warensendung an einem bestimmten Ort deponiert und diesen dann dem Empfänger mitteilt.[19] Da detaillierte Anweisung und Anleitungen zu den jeweiligen Methoden in Foren im Clearweb häufig untersagt werden, sind die entsprechenden Erläuterungen häufig ebenfalls im Darknet aufzufinden.[20]

---

15 Weitere Kryptowährungen sind beispielsweise: Namecoin, Peercoin, Dash oder Ripple.
16 Beispielsweise über: https://blockchain.info (Zuletzt abgerufen am 20.03.2018).
17 *Fünfsinn/Ungefuk/Krause,* Krim 2017, 441.
18 *Goebel/Berke,* Wirtschaftswoche vom 22. Dezember 2015.
19 *Aldridge/Askew,* Delivery Dilemmas, S. 8 der PDF.
20 *Paoli/Aldridge/Ryan/Warnes,* Behind the Curtain, S. 43 der PDF.

II. Drogenhandel

Während die zunehmende Verbreitung von Mobiltelefonen und Pagern zur Folge hatte, dass im Rahmen des Betäubungsmittelhandels vormals offene Märkte in geschlossene umgewandelt wurden, in denen die Händler nur noch an Kunden veräußerten, welche ihnen persönlich bekannt waren oder die ihnen über für sie vertrauenswürdige Kanäle vermittelt worden waren, bietet das Darknet Händlern nunmehr die Möglichkeit, einen offenen, aber gleichzeitig anonymisierten Markt zu betreiben.[21]

Der Handel findet hierbei sowohl über größere Märkte als auch über die Webseiten auf bestimmter Ware spezialisierter Einzelhändler statt.[22] Ein nicht zu unterschätzender Vorteil dieser neuen Märkte liegt für die Händler auch darin, dass diese nicht wie die klassischen Märkte lokal begrenzt sind, beispielsweise durch den Bewegungsradius des Händlers oder abgesteckte Geschäftsgebiete konkurrierender Veräußerer.

Hinzu kommt, dass sowohl Händler als auch Käufer nicht der Gefahr ausgesetzt sind, dass es im Rahmen einer Transaktion zu körperlicher Gewalt kommt.

Der Anteil der Darknet-Märkte am Gesamtmarkt für illegalen Drogenhandel ist noch verhältnismäßig gering. Zwar stellen Umsätze aus dem illegalen Drogenhandel schätzungsweise 90% des über das Darknet erwirtschafteten Umsatzes dar, für die Jahre 2011 bis 2015 wurde der Umsatz von in Europa ansässigen Händler jedoch nur auf 80 Millionen Euro geschätzt, der mit dem Verkauf illegaler Drogen in derselben Regien erwirtschaftete Gesamtumsatz wird dagegen nur für das Jahr 2013 auf 24 Milliarden Euro geschätzt.[23]

Das Darknet als Distributionsnetzwerk macht somit aktuell nur einen verschwindend geringen Anteil des Gesamtmarktes aus. Dies mag neben dem Umstand, dass die entsprechenden Märkte noch relativ jung sind, auch damit zusammenhängen, dass die zur Nutzung notwendigen technischen Grundlagen noch keine allzu starke Verbreitung in der Gesellschaft gefunden haben.

Hinzu kommt, dass die klassischen Märkte auch weiterhin gewisse Vorzüge gegenüber dem Erwerb von Betäubungsmitteln im Darknet bieten.

Einen wesentlichen Faktor dürfte es hierbei darstellen, dass Transaktionen, welche über das Darknet abgewickelt werden, regelmäßig zum Käufer zurückführende Spuren hinterlassen dürften.

---

21 *Aldridge/Décary-Hétu,* Hidden wholesale: The drug diffusing capacity of online cryptomarkets, S. 8 der PDF.

22 Siehe dazu die Abbildungen Nr. 1 und Nr. 2.

23 Europäischer Drogenbericht 2017, S. 22 der PDF; *Soska/Christin*, Measuring the Longitudinal Evolution of the Online Anonymus Marketplace Ecosystem, S. 15 der PDF veranschlagen einen Umsatz von 150 bis 180 Millionen Dollar für den weltweiten Drogenhandel über das Darknet.

Zwar ist der Handel im Darknet wesentlich auf ein anonymes Auftreten ausgerichtet, in der Vergangenheit haben die Strafverfolgungsbehörden jedoch bei ihrem Vorgehen gegen Darknet-Märkte wiederholt größere Mengen an Nutzerdaten erlangen können, welche in der Folge zur strafrechtlichen Verfolgung der Kunden eingesetzt worden sind.[24]

Neben dem Umstand, dass solche später verwertbaren Spuren bei einem analogen Erwerb deutlich leichter zu vermeiden sind, wird sich ein analoger Erwerb häufig auch aus einfacher in seiner Ausführung gestalten, da beispielsweise kein Erwerb von Kryptowährungen oder eine kompliziertere Geschäftsabwicklung notwendig sind.

Je nach Art der Betäubungsmittel dürfte auch das jeweilige Konsumverhalten Auswirkungen auf die Attraktivität des Darknets als Erwerbsort haben, da aufgrund der Zustellung ein gewisser zeitlicher Rahmen zwischen dem Erwerb und dem Erhalt der Ware einzukalkulieren ist.

Eine besonders relevante Bezugsquelle dürfte das Darknet daher besonders für solche Konsumenten darstellen, die über keine oder nur unzulängliche Kontakte zu analogen Händlern verfügen.

Weiterhin ist davon auszugehen, dass besonders im Bereich des Handels mit Betäubungsmitteln das Darknet nicht nur von Endverbrauchern genutzt wird, sondern dass auch analoge Händler hierrüber Waren zur Weiterveräußerung beziehen, wobei um Ausmaß dieser Erscheinung nur Vermutungen angestellt werden können, welche sich beispielsweise an der Höhe von getätigten Einkäufen orientieren.

Eine wesentliche Rolle dürfte das Darknet für den internationalen Drogenhandel spielen. Welche Auswirkungen dieses Phänomen auf die Betäubungsmittelmärkte im Allgemeinen hat dürfte wesentlich von der jeweiligen Produktart abhängen.

Während für Drogen, welche aus Ländern mit einem niedrigen technologischen Entwicklungsstand stammen, beispielsweise afghanisches Heroin, auch weiterhin klassische Versorgungswege die Regel darstellen dürften, kann das Darknet für andere Betäubungsmittel eine wichtige Verbindung zwischen Ländern, in denen diese preiswert hergestellt oder legal erworben werden können, und den letztendlichen Endverbrauchern darstellen.[25]

24 Siehe exemplarisch hierzu nur: *Gibbs/Beckett,* The Guardian vom 20.07.2017.

25 *Aldridge/Décary-Hétu,* Hidden Wholesale, S. 13 der PDF.

III. Waffenhandel

Zu den im Darknet angebotenen Waren gehören auch unterschiedliche, ansonsten nicht frei verkäufliche Waffen. Hierbei werden sowohl Waffen, welche legal über den Besitz eines Waffenscheins erworben werden können, als auch solche, welche unter den Anwendungsbereich des Kriegswaffenkontrollgesetzes[26] fallen, gehandelt. Mediale Aufmerksamkeit erlangte dieser Umstand nachdem bekannt wurde, dass der Attentäter von München aus dem Jahre 2016, David Ali Sonboly., seine Tatwaffe im Darknet erworben hatte.[27]

Das Angebot an unterschiedlichen Waffen im Darknet ist dabei sehr weitreichend. Bezüglich Handfeuerwaffen umfasst es sämtliche gängigen Handfeuerwaffen[28], wobei auch vollautomatische Waffen angeboten werden. Bei diesen Waffen handelt es sich sowohl um Schusswaffen, die gezielt als solche gebaut worden sind, denkbar ist hierbei beispielsweise die Veräußerung von Waffen als alten Armeebeständen, als auch um solche, die einem entsprechenden Umbau unterzogen worden sind. So ist es beispielsweise möglich, Schreckschuss-, Deko oder Startschusspistolen zu vollfunktionalen Schusswaffen umzubauen.[29] Weiterhin werden aber auch Waffenteile wie Verschlussstücke oder Gewehrläufe, Zubehör wie Zielfernrohre, Anleitungen zum Waffenbau, Munition oder Sprengkörper wie Handgranaten angeboten. Denkbar ist aber auch ein Handel mit Giftstoffen, so wird beispielsweise auch der Verkauf des radioaktiven und hochgradig tödlichen Isotops Polonium 210 im Darknet angeboten.[30]

Die Bedeutung des Darknets für den illegalen Waffenhandel liegt weniger in der Anzahl der dort getätigten Transaktionen, Schätzungen bemessen der Wert der dort monatlich getätigten Umsätze auf 80.000 US-Dollar im Monat[31], was nur einen Bruchteil des gesamten Marktes ausmachen dürfte. Die zentrale Problematik liegt vielmehr darin, dass einerseits das Darknet den Zugang zu Waffen deutlich erleichtert. Während beispielsweise der analoge Markt für Betäubungsmittel grundsätzlich ohne größeren Aufwand für jedermann zugänglich ist, gilt dies nicht für den Handel mit Waffen. Das Darknet beseitigt diese Barriere und ermöglicht damit beispielswiese Terroristen, regulären Straftätern oder Amokläufern einen erleichterten Zugang zu ihren Tatmitteln. Andererseits ist auch zu beachten, dass das Darknet den Handel mit Waffen weiter internationalisiert und somit weitere Barrieren zwischen Händlern und Käufern beseitigt. Dies erleichtert es beispielsweise, Waffen aus Staaten wie den USA, in denen diese verhältnismäßig leicht legal erworben werden können, in Staaten mit restriktiveren

26 Gesetz über die Kontrolle von Kriegswaffen, BGBl. I 1961, 444.
27 Hierzu exemplarisch für viele: *Federl,* Der Tagesspiegel vom 25.07.2016.
28 Siehe hierzu exemplarisch Abbildung Nr. 4.
29 *Candea/Dahlkamp/Schmitt/Ulrich/Wiedmann-Schmidt,* Spiegel Online vom 24.03.2016.
30 *Williams,* Daily Star vom 24.07.2016.
31 *Paoli/Aldridge/Ryan/Warnes,* Behind the Curtain, S. 66 der PDF.

Waffengesetzen und damit deutlich gesteigerten Schwarzmarktpreisen zu veräußern.[32] Zu beachten ist hierbei jedoch, dass die Intensität der Zollkontrollen bei einem Versand außerhalb eines Binnenmarktes diese Effekte in einem gewissen Rahmen beschränken kann.

IV. Geldwäsche

Das Darknet kann auch zu Zwecken der Geldwäsche genutzt werden, indem dort Gegenstände aus rechtswidrigen Taten gegen Kryptowährungen eingetauscht werden.[33] Zwar speichert bei Kryptowährungen die sogenannte Blockchain sämtliche getätigten Transaktionen öffentlich einsehbar seit Erschaffung des jeweiligen Systems, da jedoch für jede Transaktion ein neuer Identifikationsschlüssel generiert werden kann und auch die Anonymisierung von erlangten Währungseinheiten durch sogenannte Mixing-Dienste, welche auf die Unterbrechung der über die Blockchain nachvollziehbaren Transaktionskette ausgerichtet sind, möglich ist, ist eine gezielte Verschleierung von Transaktionswegen möglich. So erlangte Bitcoins können über andere Dienstleistungsseiten in reales Geld umgewandelt werden.[34] Ob Kryptowährungen selbst unter den Begriff des vermögenswerten Gegenstands im Sinne des § 261 StGB fallen, ist allerdings noch nicht abschließend geklärt.[35]

V. Datenhehlerei

Das Darknet kann ebenfalls genutzt werden, um mit illegal erlangten Daten, wie beispielsweise die von Kreditkarten- oder Email-Benutzerkonten, zu handeln. In diesem Zusammenhang wurde durch das sogenannte Vorratsdatenspeicherungsgesetz[36] der Straftatbestand der Datenhehlerei nach § 202d StGB eingeführt. Diese Norm soll vor einer Vertiefung einer Verletzung des formellen Datengeheimnisses, welche durch eine entsprechende Vortat erfolgt ist, schützen.[37]

Hierzu wird bestraft, wer sich oder einem anderen nicht öffentlich zugängliche Daten, welche durch eine andere rechtswidrige Tat erlangt worden sind, verschafft und dabei in der Absicht handelt sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Für die Begriffsbestimmung der allgemein zugänglichen Daten wird ausweislich der Gesetzesbegründung auf den § 10 Abs. 5 S. 2 BDSG abgestellt.[38] Dieser Bezug schafft jedoch im Zusammenhang mit der Existenz des Darknets tatbestandliche Schwierigkeiten für die Norm.

---

32 Vgl. hierzu *Paoli/Aldridge/Ryan/Warnes,* Behind the Curtain, S. 77 ff. der PDF.
33 Satzger/Schluckebier/Widmaier/*Jahn*, StGB § 261 Rn. 19.
34 *Ciancaglini/Balduzzi/McArdle/Rösler,* Das Deep Web erkunden, S. 22 der PDF.
35 *Boehm/Pech,* MMR 2014, 75 (77).
36 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BGBl. I 2015, 2218.
37 Münchener Kommentar zur Strafgesetzbuch/*Graf,* StGB § 202d Rn. 2a.
38 BT-Drs. 18/5088, S. 45.

Nach § 10 Abs. 5 S. 2 BSDG sind nämlich solche Daten öffentlich zugänglich, welche von jedermann ohne vorherigen Anmeldung, Zulassung oder Entrichtung eines Entgeltes genutzt werden können.

Es ist nun zu erwarten sein, dass ein nicht unwesentlicher Anteil der Transaktionen, die dem Anwendungsbereich des § 202d StGB unterfallen, über das Darknet abgewickelt wird. Da das Darknet jedoch grundsätzlich von jedermann ohne gesonderte Fachkunde genutzt werden kann, wird vertreten, dass demnach dort angebotene Daten auch öffentlich zugänglich wären, der Anwendungsbereich der Norm würde sich dann auf Fälle beschränken, in denen der Erwerb der Daten nur bestimmten Personen offen steht.[39]

Dies würde auch zur Folge haben, dass Strafverfolgungsbehörden im Einzelfall gegebenenfalls mit der Problematik konfrontiert werden würden, dass sie den Nachweis erbringen müssten, dass die von einem Täter erlangten Daten nicht im Darknet verfügbar seien.[40] Eine so drastische Einschränkung des Anwendungsbereiches des § 202d StGB dürfte die Existenz des Darknets tatsächlich jedoch nicht zur Folge haben. Der § 10 Abs. 5 S. 2 BSDG bezieht sich nämlich auf Daten, welche über die Nutzung eines automatisierten Abrufverfahrens abrufbar sind.[41]

Dass erlangte Datensätze jedoch zur freien Verfügung im Darknet veröffentlich werden dürfte jedoch eine Ausnahme darstellen. Naheliegender ist, dass im Falle einer Veräußerung der Daten der Händler diese direkt oder über die Nutzung eines Treuhänders an den Käufer weiterleitet. Da jedoch eine Sendung von Daten an einen weiteren Nutzer keinen Fall eines automatisierten Abrufverfahrens im Sinne des § 10 BDSG darstellt[42], können auch solche Transaktionen dem Straftatbestand des § 202d StGB unterfallen.

VI. Verbotene pornographische Inhalte

Eine zentrale Bedeutung hat das Darknet für die Verbreitung von verbotenen pornographischen Inhalten, hierbei im Besonderen für pädopornographische Schriften und Bilder im Sinne des § 184b StGB.[43] So bemessen einzelne Studien den Anteil der Zugriffe auf Seiten mit pädopornographischen Inhalten auf 80% der Gesamtzugriffe im Darknet.[44]

Da durch die Funktionsweise des TOR-Systems die bisherigen Ansätze zur Bekämpfung solcher Inhalte wie Netzsperren, wie sie beispielsweise das gescheiterte Zugangs-

39 *Gercke,* ZUM 2016, 825 (827); *Stam,* StV 2017, 488 (489 f.).
40 *Gercke,* ZUM 2016, 825 (827 f.).
41 Beck'scher Onlinekommentar Datenschutzrecht/Wolff/Brink/*von Lewinski,* BDSG § 10 Rn. 45 ff.
42 Vgl. Beck'scher Onlinekommentar Datenschutzrecht/Wolff/Brink/*von Lewinski,* BDSG § 10 Rn. 6.
43 Eine Auflistung von Webseiten mit entsprechenden Inhalten findet sich beispielsweise unter folgender Adresse: http://wikilink77h7lrbi.onion/dir/adult.html (Zuletzt abgerufen am 27.03.2018), eine Überprüfung der Funktionsweise der dort angegeben Weblinks wurde vom Verfasser jedoch nicht durchgeführt.
44 *Owen/Savage,* The Tor Dark Net, S. 12 der PDF.

erschwerungsgesetz[45] zum Inhalt hatte, keinerlei Effekt erzielen können, ist es wenig verwunderlich, dass ein wesentlicher Teil der pädopornographischen Inhalte im Internet in neuster Zeit über das Darknet zu erreichen ist.[46]

Dem Darknet kommen bei der diesbezüglichen Kriminalität zwei unterschiedliche Funktionen zu. Einerseits wird es zur Verbreitung von Inhalten genutzt, sowohl zum gegenseitigen Austausch von Nutzern als auch zur gezielten Veräußerung. Das Darknet wird von den Nutzern solcher Inhalte jedoch auch genutzt, um sich über die unterschiedlichen Methoden auszutauschen, die einem sicheren Zugriff auf pädopornographische Inhalte und der Vermeidung von Strafverfolgung dienen.[47] Ein denkbares Mittel gegen die Verbreitung solcher Inhalte könnte eine Sperrung der entsprechenden Seiten durch die Betreiber des TOR-Netzwerkes darstellen, diese lehnen Sperrungen von Inhalten jedoch im Allgemeinen ab, da sie andernfalls eine Zunahme von Zensuranfragen befürchten.[48]

Für die Verbreitung pädepornographischer Inhalte dürfte das Darknet in Zukunft auch noch weiter an Bedeutung gewinnen. Gewisse Vorgänge werden mit hoher Wahrscheinlichkeit auch in Zukunft über das Clearweb abgewickelt werden.

Dies gilt beispielsweise einerseits für Liveübertragungen von Missbrauch, bei denen der Nutzer die konkreten Missbrauchshandlungen dirigieren kann, da die geringe Übertragungsgeschwindigkeit des Darknets hierfür ungeeignet sein dürfte, als auch für die Erlangung von Bildmaterial aus Regionen wie Afrika oder Südostasien, da dort entsprechende Technologien noch keine ausreichende Verbreitung gefunden haben und auch eine Bezahlung in Kryptowährungen für die Veräußerer wenig attraktiv erscheint oder komplexe Verschlüsselungssysteme aufgrund der dortigen technischen Infrastruktur für die Täter kein Erfordernis darstellen.[49]

Dennoch stellt die Möglichkeit eines anonymen Austausches von Daten, welche unter den Anwendungsbereich des § 184b StGB fallen, ein schwerwiegendes Problem dar, da in Ermangelung einer physischen Zustellung zum Empfänger die Chancen einer Identifizierung durch die Strafverfolgungsbehörden nur verschwindend gering sind.

Die Existenz des Darknets wirkt somit dem Normzweck des § 184b StGB, welcher durch eine Bekämpfung der Märkte die Herstellung von neuem Material verhindern und potentielle Opfer dadurch schützen möchte[50], entgegen.

---

45 Gesetz zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen, BGBl. I 2010, 78.
46 Sieber/Satzger/von Heintschel-Heinegg/*Sieber,* § 24 Rn. 53.
47 *Europol,* IOCTA 2017, S. 39 der PDF.
48 *Owen/Savage,* The Tor Dark Net, S. 14 der PDF.
49 Vgl. *Europol,* IOCTA 2017, S. 50 der PDF.
50 Münchener Kommentar zum StGB/*Hörnle,* StGB 184b Rn. 1.

VII. Fälschungsgüter

Das Darknet wird ebenfalls zum Vertrieb von Fälschungsgütern genutzt, welche zwischen 1,5% und 2,5% der angebotenen Waren im Darknet ausmachen.[51] So werden auf den dortigen Märkten beispielsweise Ausweisdokumente wie Reisepässe, Führerscheine oder Personalausweise angeboten.[52] Das Qualitäts- und Preisniveau schwankt zwischen den unterschiedlichen Anbietern, ob die angebotenen Dokumente jedoch auch über eine tatsächliche Gültigkeit verfügen, ist ohne einen Erwerb dieser Produkte nicht zu ermitteln.[53] Auch Scans von Ausweisdokumenten können für geringfügige Preise erworben werden. Diese können beispielsweise genutzt werden, um eine falsche Identität im Internet zu erstellen. Neben Ausweisdokumenten wird auf den Darknet-Märkten auch mit Falschgeld gehandelt, wobei die Qualität der angebotenen Banknoten stark variieren kann.[54] Neben der Ware selbst werden regelmäßig Anleitungen und Vorschläge zur Inumlaufbringung der gefälschten Banknoten bereitgestellt.

Neben Ausweisdokumenten und Falschgeld, welche den Großteil der angebotenen Fälschungsgüter ausmachen, kann auch eine Vielzahl anderer gefälschter Waren wie beispielsweise Schmuck, Kleidung, pharmazeutische Erzeugnisse oder elektronische Geräte über das Darknet erworben werden.[55] Der Preis solcher Waren ist dabei im Schnitt um ein Drittel niedriger als der der Originalwaren.[56]

VIII. Illegale Dienstleistungen

Neben dem Handel mit illegalen Waren werden über das Darknet auch unterschiedliche illegale Dienstleistungen angeboten. Dieses Phänomen wird auch als Crime-as-a-Service-Modell bezeichnet.[57]

Einen wichtigen Bereich stellen hierbei die angebotenen technischen Dienstleistungen dar. Hierunter fällt zum Beispiel die Bereitstellung von Webseiten, über die Straftäter kommunizieren und illegale Transaktionen oder Handlungen planen oder durchführen können. Zu den angebotenen Dienstleistungen gehört weiterhin auch die Vermietung von Botnetzen. Hierbei handelt es sich um Netzwerke von Rechnern, welche mit einer Schadsoftware infiziert worden sind und ohne Kenntnisnahme der Nutzer fremdgesteuert werden können. Diese Netzwerke können zur Verbreitung von Malware, Ransomware und Spammails oder anderen kriminellen Aktivitäten genutzt werden.[58]

---

51 *Europol,* IOCTA 2017, S. 50 der PDF.
52 Siehe hierzu exemplarisch Abbildung Nr. 3.
53 *Ciancaglini/Balduzzi/McArdle/Rösler,* Das Deep Web erkunden, S. 26 der PDF.
54 Zum Handel mit Falschgeld siehe exemplarisch Abbildung Nr. 6.
55 Zum Handel mit verschreibungspflichtigen Pharmazeutika siehe exemplarisch Abbildung Nr. 5.
56 *Europol,* Intellectual Property Crime on the Dark Net, S. 3 der PDF.
57 *Meywirth,* Krim 2016, 355 (356).
58 *Meywirth,* Krim 2016, 355 (357).

Zusätzlich können solche Botnetze auch für DDoS-Attacken auf Webseiten genutzt werden. Hierbei wird eine Zieladresse so stark mit Anfragen beschickt, dass der angefragte Dienst überhaupt nicht mehr oder nicht mehr effektiv genutzt werden kann. Solche Angriffe können reinen Vandalismus darstellen, sie können aber auch genutzt werden, um Erpressungen, beispielsweise von Onlinehändlern, durchzuführen oder eine Ablenkungen für einen Hauptangriff, welcher beispielsweise auf einen Datendiebstahl ausgerichtet ist, zu schaffen. Solch Angriffe können, wie auch verschiedene Hacking-Dienstleistungen, auch direkt erworben werden, wobei insbesondere DDoS-Attacken verhältnismäßig günstig zu erstehen sind.[59]

Weiterhin werden auch verschiedene Finanzdienstleistungen sowie logistische Dienste bei der Zustellung von illegal erworbenen Waren wie die Ablage der Waren an bestimmten Dropping-Punkten oder die Bereitstellung von Packstationen angeboten.[60]

Zu den angebotenen kriminellen Dienstleistungen gehören vereinzelt auch Durchführung von Tötungsdelikten, einfachen Gewaltverbrechen, die Zufügung von dauerhaften körperlichen Schäden oder sogar Vergewaltigungen.[61] Auch hierbei sollen Dritte als Treuhänder genutzt werden, um ein vertragstreues Verhalten der Parteien zu sichern. Ob es sich hierbei um ernstzunehmende Angebote handelt, lässt sich jedoch kaum verifizieren, da die entsprechenden Seiten aus Gründen der Diskretion regelmäßig nicht über sie angeblich erfolgreich vermittelte Taten berichten möchten.[62] Wiederholt haben sich solche Angebote jedenfalls als Unwahrheiten oder sogar sogenannte *Honeypots*, also eine gezielt eingerichtete Falle für Kriminelle, herausgestellt.[63] Weiterhin existieren auch Seiten, auf welchen auf den Tod einer Person zu einem bestimmten Zeitpunkt gewettet werden kann. Hier könnte ein potentieller Attentäter auf den Tod einer Person einer Person zu einem bestimmten Zeitpunkt wetten und diesen daraufhin selbst herbeiführen.[64]

IX. Darknet und Terrorismus

Die dargestellten Strukturen des Darknets werden nicht nur von Straftätern aus dem Bereich der herkömmlichen Kriminalität genutzt, sondern sind auch von terroristischen Organisationen für die Erreichung ihrer Zwecke entdeckt worden.

Das Darknet kann hierbei sowohl zur Erlangung von Waffen oder anderen Tatmitteln, zur Koordination von Operationen, zur Rekrutierung neuer Mitglieder, zur Verbreitung von Propagandamaterial als auch zur Finanzierung entsprechender Organisationen genutzt werden.

59 Vgl. *Makrushin,* Was kostet eine DDos-Attacke.
60 *Meywirth,* Krim 2016, 355 (358).
61 Siehe hierzu exemplarisch Abbildung Nr. 7.
62 *Ciancaglini/Balduzzi/McArdle/Rösler,* Das Deep Web erkunden, S. 32 der PDF.
63 Hierzu exemplarisch nur: *Murdock,* International Business Times vom 13.05.2016.
64 *Chertoff/Simon*, The Impact of the Dark Web, S. 10 der PDF.

So wurde beispielsweise bekannt, dass al-Qaida-Führungskader das Darknet zur Kommunikation genutzt haben.[65]

Im Rahmen der Terrorismusfinanzierung ist zu beachten, dass Kryptowährungen kaum dazu geeignet sind alltägliche Ausgaben wie die Bezahlung einer Miete zu tätigen.

Da eine Umwandlung von Kryptowährungen in reguläre Währungseinheiten zwar möglich ist, jedoch auch ein gewisses Identifizierungsrisiko in sich birgt, dürfte sich der finanzielle Anwendungsbereich des Darknets auf den Erwerb von illegalen Gütern wie Waffen oder gefälschte Ausweisdokumente sowie die Veräußerung inkriminierter Wertgegenstände, wie beispielsweise Raubkunst, beschränken.[66]

Auch im Rahmen der Verbreitung von Propagandamaterial schränkt die Nutzung des Darknets den Empfängerkreis ein, hier wird daher auch auf andere verschlüsselte Kommunikationsmittel wie beispielsweise die Applikation *Telegram* zurückgegriffen.[67] Eine weitere Funktion kann dem Darknet auch bei der Entstehung von Terrorzellen zukommen.

Seit etwa dem Jahre 2004 hat sich die Radikalisierung von potentiellen Terroristen durch wechselseitige Kommunikation zu einem nicht unerheblichen Teil in das Internet verlagert.[68]

Da terrorismusnahe Netzwerke jedoch im Clearweb einer starken Überwachung von staatlichen Institutionen ausgesetzt sind, propagandistische Inhalte sowie entsprechende Accounts in Social-Media-Netzwerken häufig gelöscht werden und in der Vergangenheit beispielsweise auch schon Angriffe des Internetkollektives Anonymous auf Webseiten, welche in einem Zusammenhang mit dem islamischen Staat stehen sollten, bekannt wurden, gewinnt das Darknet als Rückzugsort für Terroristen an Interesse.[69]

D. Bekämpfung und Verfolgung von Kriminalität im Darknet

Die Schattenwirtschaft des Darknets stellt die Strafverfolgungsbehörden für eine Vielzahl neuer Herausforderungen, da eine klassische Überwachung oder Entschlüsselung des TOR-Netzwerkes technisch aktuell nicht im Rahmen ihrer Möglichkeiten liegt.

Im Folgenden sollen die unterschiedlichen Möglichkeiten zur Bekämpfung der im Darknet erfolgenden Kriminalität dargestellt werden.

65 *Rosner/London/Mendelboim,* Backdoor Plots: The Darknet as a Field for Terrosism.
66 *Teichmann,* Krim 2018, 30.
67 *Weimann,* Terrorist Migration to the Dark Web, S. 2 der PDF.
68 *Bock/Harrendorf,* ZSTW 2014, 337 (341).
69 *Mey,* Darknet S. 58 f.

I. Klassische Ermittlungsmethoden

Auch wenn die anonymisierte Kommunikation die diesbezüglichen Möglichkeiten einschränkt, können traditionelle Ermittlungsmethoden einen wertvollen Beitrag zur Bekämpfung von Kriminalität im Darknet beitragen. So können beispielsweise verdeckte Ermittler oder nicht offen ermittelnde Polizeibeamte eingesetzt werden. Ermittler können dabei als einfache Akteure auf den Märkten auftreten, denkbar ist jedoch auch, dass erlangte digitale Identitäten von langjährigen Szenemitgliedern übernommen werden, um so einen besseren Zugang zu Informationen zu erlangen.[70] Zu der Übernahme einer digitalen Identität ist jedoch erforderlich, dass die Strafverfolgungsbehörden die jeweiligen Zugangsdaten unmittelbar oder durch die Kooperation des eigentlichen Inhabers erlangen, da dieser über die Mittel der StPO nicht zu einer Herausgabe seiner Passwörter gezwungen werden kann.[71] Problematisch dürften sich weiterhin auch Netzwerke darstellen, die von ihren Mitgliedern strafbare Handlungen als Aufnahmeritual oder auf regelmäßiger Basis als Aktivitätsnachweis zur Fernhaltung passiver Mitglieder verlangen.[72] Denkbar ist aber auch, dass den Strafverfolgungsbehörden Hinweise zugespielt werden, so führte beispielsweise ein Hinweis einer niederländischen Sicherheitsfirma bezüglich eines im Clearweb gelegenen Entwicklungsservers der Seite Hansa zu deren Schließung.[73]

Diesen Ermittlungsmethoden sind jedoch auch gewisse Grenzen gesetzt. Einerseits ist zu beachten, dass eine Infiltrierung der Märkte dadurch erschwert wird, dass es sich bei den Märkten im Darknet nicht im klassische kriminelle Organisationen mit einer hierarchischen Struktur handelt, sondern dass diese vielmehr von einer Reihe international verstreuter Einzelpersonen betrieben werden, deren interne Kommunikation pseudonymisiert abläuft und die höchstwahrscheinlich ebenfalls keine Kenntnis darüber besitzen, wer ihre Komplizen tatsächlich sind. Vor dem Hintergrund, dass somit selbst die Enttarnung einzelner Betreiber eines Marktes diesen nicht zwangsläufig lahmlegen muss, können die hohen Kosten von personalen Maßnahmen gegebenenfalls unverhältnismäßig sein.[74]

II. Abfangen und Rückverfolgung von Postsendungen

Wichtige Mittel zur Identifizierung von Verkäufern und Empfängern illegaler Waren aus dem Darknet stellen der Zugriff von Strafverfolgungsbehörden auf Postzusendungen sowie hinzugehörige Auskunftsverlangen dar, da solche Sendungen ein verbindendes Element zwischen den Märkten des Darknets und den dort agierenden Protagonisten herstellen können. Unproblematisch ist hierbei die Beschlagnahme von Postsendun-

70 *Fünfsinn/Ungefuk/Krause,* Krim 2017, 440 (444).
71 *Krause,* NJW 2018, 678 (680).
72 Exemplarisch hierzu: BGH, BeckRS 2012, 06061.
73 *Greenberg,* Wired vom 08.03.2018.
74 Vgl. auch *Kruithof/Aldridge/Décary-Hétu/u.A.,* Internet-facilitated drugs trade, S. 127 der PDF.

gen, welche sich im Gewahrsam des Postdienstleisters befinden, hierfür stellt der § 99 StPO eine Rechtsgrundlage dar. Als weniger intensive Eingriffsform wird bei Vorliegen der Voraussetzungen einer Beschlagnahme auch allgemein eine Befugnis zur Verlangung von Auskünften über solche Postsendungen anerkannt.[75] Ein solches Auskunftsverlangen setzt jedoch nach der aktuell in Rechtsprechung und Literatur vorherrschenden Auffassung voraus, dass die entsprechende Sendung noch nicht an den Empfänger zugestellt worden ist.[76] Besonders zu beachten ist hierbei, dass der Bundesgerichtshof in einem jüngeren Beschluss einen Rückgriff auf allgemeine Vorschriften zur Beschlagnahme für solche retrograden Auskünfte auf der Grundlage eines systematischen Vorranges des § 99 StPO ausgeschlossen hat.[77] Dieser Umstand engt die Möglichkeiten der Strafverfolgungsbehörden zu einer Identifizierung von Straftätern somit nicht unwesentlich ein. Dies ist jedoch insoweit problematisch, als dass der § 99 StPO nach der Intention des Gesetzgebers keinesfalls eine exklusive Wirkung gegenüber retrograden Auskunftsverlangen entfalten sollte.[78] Da somit nach der ursprünglichen gesetzgeberisch intendierten Systematik ein Zugriff auf solche Informationen über den § 94 StPO möglich sein sollte, wäre diesbezüglich eine Klarstellung durch den Gesetzgeber zu begrüßen.[79] Insbesondere bei der zunehmend an Bedeutung gewinnenden Bekämpfung von Kriminalität im Darknet würde dies die Arbeit der Strafverfolgungsbehörden erleichtern.

Hinzu kommt, dass auch der häufig grenzüberschreitende Charakter der Sendungen rechtliche Komplikationen bei der Rückverfolgung von Sendungen hervorrufen kann. Auch nutzen die Händler eine Vielzahl von Methoden zur Verschleierung ihrer Sendungen. Besonders Betäubungsmittel werden häufig in so kleinen Mengen erworben, dass diese problemlos in unauffälligen regulären Briefumschlägen versendet werden können.[80]

III. Überwachung und Erkennung von Akteuren im Darknet

Ein mögliches Mittel zur Identifizierung von Straftätern in Darknet stellt die manuelle oder automatisierte Überwachung und Auswertung von Märkten dar. Denkbar ist beispielsweise, bei der Überwachung der Märkte nach Anhaltspunkten für eine Identifizierung zu suchen, welche von Nutzern unbeabsichtigt hinterlassen worden. So warnt beispielswiese der TOR-Browser seine Nutzer, dass eine Maximierung des TOR-Browsers eine zur Nutzeridentifizierung nutzbare Bestimmung der Bildschirmgröße ermöglich

75 Münchener Kommentar zur StPO/*Günther,* StPO § 99 Rn. 42 mit weiteren Nennungen.
76 BGH, NJW 2017, 680; Systematischer Kommentar zur StPO/*Wohlers/Greco,* StPO § 99 Rn. 19 mit weiteren Nennungen.
77 BGH, NJW 2017, 680 (681).
78 *Krause,* NZWiSt 2017, 60 (61 f.); *Weisser,* wistra 2016, 387 (390).
79 *Krause,* NZWiSt 2017, 60 (62); *Weisser,* wistra 2016, 387 (391).
80 *Martin,* Lost on the Silk Road, S. 8 der PDF.

kann.[81] Auch können beispielsweise hochgeladene Bilddateien Metadaten enthalten, welche Rückschlüsse auf den Ersteller der Dateien zulassen können. Die Märkte haben jedoch begonnen Vorkehrungen gegen solche Ermittlungsmöglichkeiten zu treffen, so können beispielweise Metadaten automatisch im Rahmen des Uploads einer Datei von der jeweiligen Seite entfernt werden. Weiterhin ist vereinzelt die Auswertung von Massendaten um hierdurch Verbindungen zwischen genutzten Pseudonymen und IP-Adressen herstellen zu können, wobei eine Nutzung solcher Methoden bisher noch nicht dokumentiert ist.[82] Weiterhin ist zu beachten, dass die Relaisserver des TOR-Netzwerkes in einer dezentralisierten Struktur von Freiwilligen bereitgestellt werden. Es ist somit für staatliche Institutionen möglich, selbst solche Relaisserver zu betreiben, um hierdurch auf die über die Server weitergereichten Informationen zugreifen zu können. Dass dieses Vorgehen bereits seit mehreren Jahren eine gängige Praxis darstellt, lässt eine Auswertung geheimer Dokumente des Bundesnachrichtendienstes deutlich werden.[83]

Denkbar ist auch, Angriffe auf die Geräte der Nutzer durchzuführen. Hierzu können beispielsweise Mittel der Quellen-Telekommunikationsüberwachung wie sogenannte Trojaner genutzt werden, um die Kommunikation der Nutzer auszulesen. So konnten beispielsweise niederländische Behörden nach der heimlichen Übernahme des Marktes Hansa einzelne Käufer dazu bewegen, eine Datei mit einem vermeintlichem Sicherungscode zur Rückerlangung von überwiesenen Kryptowährungseinheiten auch im Falle einer Marktschließung herunterzuladen, wobei die Datei tatsächlich zur Identifizierung der IP-Adresse der Händler diente.[84] Solche Methoden setzen jedoch einerseits einen Kontakt zu der jeweiligen Zielperson voraus und verlangen weiterhin, dass diese auch unachtsam genug ist, die für den Angriff notwendigen Dateien selbst herunterzuladen.

Ein weiterer Weg zur Identifizierung von Straftätern kann über die Rückverfolgung von getätigten Kryptowährungstransaktionen führen. Europol hat in diesem Zusammenhang die Bedeutung von Kryptowährungen zur Identifizierung von Straftätern erkannt[85], die technischen Möglichkeiten zur Verschleierung von Transaktionshistorien dürften jedoch auch hier einer Verfolgung von Straftätern häufig Schwierigkeiten bereiten.[86] Auch kann eine gezielte Auswertung von verschiedenen Nutzerprofilen einer Zielperson auf unterschiedlichen Plattformen einen Anhaltspunkt für eine weiterführende Personenrecherche bieten. Zur Identifizierung von Internetnutzern kann grundsätzlich auch das sogenannte Browser-Fingerprinting eingesetzt werden.

---

81 Siehe dazu auch die Abbildung Nr. 1.

82 *Kruithof/Aldridge/Décary-Hétu/u.A.,* Internet-facilitated drugs trade, S. 130 der PDF.

83 *Moßbrucker,* APUZ vom 10.11.2017.

84 *Greenberg,* Wired vom 08.03.2018.

85 *Europol,* IOCTA 2016, S. 44 der PDF.

86 Siehe hierzu auch: Kapitel C IV dieser Arbeit.

Die Entwickler des TOR-Projektes sind sich dieser Gefahr jedoch bewusst und entwickeln ihre Technologie konstant fort, um den verschiedenen Möglichkeiten zum Fingerprinting entgegenzutreten.[87]

Diese Methoden zur Identifizierung von Straftätern im Darknet sehen sich jedoch mit unterschiedlichen Komplikationen konfrontiert. Zunächst ist zu beachten, dass die Beschlagnahme eines für einen Darknetmarkt genutzten Servers nicht zwangsläufig eine Identifizierung der Personen zur Folge haben muss, die auf diesem Markt in illegale Transaktionen involviert waren, da einerseits die hierzu erforderlichen Daten regelmäßig verschlüsselt sind, anderseits bereits häufig ein Zugang zu diesen verschlüsselten Daten bereits an einer Verschlüsselung des Servers selbst scheitert.[88]

Soweit eine Entschlüsselung dieser Daten möglich ist, werden Zuordnungen durch die Nutzung von TOR-Browsern weiter erschwert. Weiterhin kommt erschwerend hinzu, dass das Darknet einer sehr starken Fluktuation ausgesetzt ist. So kommt es regelmäßig vor, dass Foren oder Märkte ihre URLs nur für wenige Tage oder Wochen beibehalten. Eine erfolgreiche Anklage von Straftätern setzt daher eine besonders akribische Dokumentation ihres Handelns im Darknet voraus.[89] Auch zu beachten ist, dass Ermittlungen im Darknet dadurch verkompliziert werden, dass diese vollumfänglich auf die Auswertung von Daten angewiesen sind. Daten können jedoch gegenüber physischen Beweismitteln verhältnismäßig leicht abgeändert, entfernt und manipuliert werden, so dass die Strafverfolgungsbehörden auf eine schnelle Erlangung der für sie relevanten Daten angewiesen sind.[90]

IV. Störung der Onlinemärkte

Den Strafverfolgungsbehörden stehen verschiedene Möglichkeiten offen, um die Funktionsweise von illegalen Onlinemärkten einzuschränken. Da für den Handel mit illegalen Gütern über das Darknet das Vertrauen der einzelnen Parteien in das jeweilig genutzte System von essentieller Bedeutung ist, kann ein gezielt herbeigeführter Vertrauensverlust einen solchen Markt wesentlich schädigen. Dies kann beispielsweise erreicht werden, indem die Erreichbarkeit von Märkten temporär unterbrochen wird, beispielsweise durch DDoS-Attacken, oder gezielt das Aufkommen von Vorkassebetrug gesteigert wird. Der Effektivität solcher Maßnahmen wird jedoch verstärkt durch die Nutzung von Treuhändersystemen und der Dezentralisierung der Märkte begegnet, auch konnten solche Methoden in der Vergangenheit wohl auch nur die Lebensdauer einzelner Märkte beeinflussen.[91]

Ein solcher Vertrauensverlust kann andererseits auch durch wiederholte Schließungen

87 *Perry/Clark/Murdoch/Koppen,* The Design and Implementation of the TOR Browser, Kapitel 4.6.
88 *Kruithof/Aldridge/Décary-Hétu/u.A.,* Internet-facilitated drugs trade, S. 129 der PDF.
89 *Ciancaglini/Balduzzi/McArdle/Rösler,* Das Deep Web erkunden, S. 38 der PDF.
90 *Koops/Goodwin,* Cyberspace, the cloud, and cross-border criminal investigation, S. 18 der PDF.
91 *Kruithof/Aldridge/Décary-Hétu/u.A.,* Internet-facilitated drugs trade, S. 28 f. der PDF.

von Märkten durch die Strafverfolgungsbehörden und die anschließende Auswertung der erlangten Daten zur Identifizierung und Verfolgung der Käufer erreicht werden. So war es beispielsweise Europol in Kooperation mit der US-Amerikanischen DEA sowie niederländischen Polizeibehörden im Jahre 2017 gelungen, im Rahmen der Operation Bayonet, die großen Darknetmärkte Hansa und AlphaBay zu schließen und eine große Zahl an Nutzerdaten zu erlangen.[92] Während ähnliche Aktionen in der Vergangenheit bisher jeweils nur einzelne Märkte betrafen, stellte diese Operation insoweit eine Besonderheit dar, als dass das Ausweichen der Nutzer auf andere Märkte antizipiert und gezielt von den Behörden zur Informationsgewinnung genutzt worden war. So wurde zunächst AlphaBay abgeschaltet, um so die dort aktiven Händler und Kunden zu Hansa zu locken. In der Folge ließen die Strafverfolgungsbehörden Transaktionen dieser Seite, welche sie auch bereits infiltriert hatten, für mehrere Tage weiterlaufen, um so Beweismaterial gegen die Beteiligten zu erlangen.

Im Rahmen dieser Operation wurde eine Reihe von Funktionen von Hansa manipuliert, so dass beispielsweise verschickte Nachrichten vor ihrer Verschlüsselung oder die Metadaten von Bilddateien vor ihrer Entfernung durch das System heimlich gespeichert werden konnten.[93] Auch wenn solche Erfolge die Attraktivität des Darknets als Umschlagort für illegale Waren temporär beeinträchtigen dürften, spricht der Umstand, dass auch in der Vergangenheit größere Erfolge wie die erste Schließung der Plattform Silk Road im Jahre 2013 oder die multinational geführte Operation Onymous im Jahre 2014 keine dauerhafte Unterbindung dieses Phänomens erreichen konnten.[94]

Der Wert solcher Operationen darf dennoch nicht unterschätzt werden, da für Betreiber solcher Märkte so ein Anreiz dafür geschaffen wird, dass sie, sobald sie eine Größe erreicht haben, bei der sie ein interessantes Ziel für entsprechende Maßnahmen darstellen, ihren Markt schließen und die im Treuhändersystem eingelagerten monetären Werte einbehalten, was wiederum einen Vertrauensverlust für den Handel im Darknet zur Folge hat.[95] Für die Nutzer entsteht somit ein Spannungsfeld, da ein Markt einerseits eine gewisse Größe und Bestandsdauer benötigt um Vertrauen aufzubauen, andererseits aber ab einem gewissen Wachstum die Wahrscheinlichkeit eines sogenannten Exit-Scams steigt. Aufgrund der hohen Bedeutung von gegenseitigem Vertrauen für die Funktionsweise solcher Märkte können diese auch mit sogenannte Sybil-Attacken, also eine größer angelegte Erstellung von falschen Identitäten in einem Netzwerk, effektiv angegriffen werden.[96]

92 *Greenberg,* Wired vom 20.07.2017.
93 *Greenberg,* Wired vom 08.03.2018.
94 *Greenberg,* Wired vom 20.07.2017.
95 *Kruithof/Aldridge/Décary-Hétu/u.A.,* Internet-facilitated drugs trade, S. 65 f. der PDF.
96 *Décary-Hétu/Laferrière,* Discrediting Vendors in Online Criminal Markets, S. 20 zum Handel mit Kreditkartendaten.

E. Die positiven Aspekte des Darknets

Neben den dargestellten Möglichkeiten, das Darknet für schädliche Zwecke zu nutzen, bietet das Darknet auch zahlreiche Anwendungsmöglichkeiten, die allgemein als positiv aufgefasst werden können. Hierbei ist zu beachten, dass die konkrete Nutzung dieser Mittel dabei nicht bewertet werden soll. Gerade politischer Aktivismus und sogenanntes Whistleblowing, also das Öffentlichmachen von wichtigen geheimen oder geschützten Informationen, werden nicht nur in autoritär geführten Staaten kriminalisiert, sondern können auch im westlichen Kulturkreis die Grenze zur Strafbarkeit überschreiten. Soweit im Folgenden Beispiele angebracht werden, dienen diese nur der Veranschaulichung und sollen keine Wertung enthalten. Diese sollen im Folgenden in ihren Grundzügen dargestellt werden.

I. Private Nutzung durch Einzelpersonen

Für den privaten Internetnutzer bietet die durch die Nutzung des Darknets entstehende Möglichkeit zur anonymen Nutzung des Internets eine Reihe unterschiedlicher Anreize. So können auf diesem Weg beispielsweise Zensurmaßnahmen wie die Sperrung des sozialen Netzwerkes Facebook, welches seit dem Jahre 2014 eine gesonderte Adresse, welche nur durch Nutzung eines TOR-Browsers erreichbar ist, unterhält[97], in der Volksrepublik China umgangen werden. Nachdem die im Jahre 2013 begonnene globale Überwachungs- und Spionageaffäre das Ausmaß der verdachtsunabhängigen Telekommunikationsausspähung durch die Geheimdienste der USA und des Vereinigten Königreiches offenlegte, sind auch im westlichen Kulturkreis Anreize zu einer Verlagerung von Telekommunikation in Netzwerke mit einer erschwerten Zugreifbarkeit entstanden. Weiterhin kann das Darknet auch einen Rückzugsort für Menschen darstellen, die aus Gründen wie der religiösen oder ethnischen Zugehörigkeit oder ihrer sexuellen Orientierung einer Verfolgung oder Diskriminierung ausgesetzt sind. Das Darknet erweitert somit die bereits über das Clearweb bestehenden Möglichkeiten für Minderheiten, sich durch anonymisierte Kommunikation zu emanzipieren.[98] Über das Darknet kann auch ein ungestörter Zugang zu sogenannten Schattenbibliotheken wie Sci-Hub gewährleistet werden, die in, juristisch freilich nicht unbedenklicher Art und Weise, einen freien Zugang zu sonst nur kostenpflichtig nutzbarer wissenschaftlicher Literatur gewähren.[99] Weiterhin kann das Darknet auch für hochsensible Kommunikation oder Datenaustausch genutzt werden, bei der verhindert werden soll, dass eine dritte Partei wie beispielsweise ein E-Mail-Provider eine Zugriffsmöglichkeit auf den Informationsaustausch erhält, aber auch die automatisierte Auswertung eines digitalen Fußabdruckes, beispielsweise zum Zwecke von personalisierter Werbung, kann durch eine Nutzung des Darknets vermieden werden.

---

97 https://facebookcorewwwi.onion/ (Zuletzt abgerufen am 20.03.2018).

98 Vgl. *Bock/Harrendorf,* ZSTW 2014, 337 (342).

99 *Mey,* Darknet S. 72 f.

II. Journalismus im Darknet

Eine wesentliche Bedeutung hat das Darknet für Journalisten in Staaten, in denen Medieninhalte stark zensiert werden. So wird das Darknet beispielsweise verstärkt von Journalisten in der Volksrepublik China und dem Iran genutzt. Vermehrt haben auch Zeitungen und Verlage aus dem westlichen Kulturkreis wie die New York Times begonnen, Seiten im Darknet einzurichten, welche die eigenen journalistischen Inhalte dort zugänglich machen und die von Informanten und sogenannte Whistleblowern genutzt werden können, um ohne die Gefahr einer Rückverfolgbarkeit geheime Informationen zu übermitteln.[100] Bei einem Upload wird dem Nutzer hierbei häufig auch ein Passwort zugeteilt, durch das er eine eventuelle Antwort der Redaktion oder weitere Fragen entgegennehmen kann. Auch reine Enthüllungsportale wie WikiLeaks haben regelmäßig auch eine Präsenz im Darknet. Neben den klassischen Journalisten bietet das Darknet auch bedeutenden Schutz für Blogger, welche über bestimmte Missstände berichten. So wurden in der Vergangenheit beispielsweise wiederholte mexikanische Blogger auf brutale Weise hingerichtet, nachdem sie über die lokalen Drogenkartelle berichtet hatten.[101]

Bei all dem ist jedoch zu beachten, dass das Darknet aufgrund seiner verhältnismäßig langsamen Datenübertragungsgeschwindigkeit wenig dazu geeignet ist, Inhalte direkt einem größeren Publikum zugänglich zu machen. Das Darknet dürfte daher häufig eher ein Kommunikationsmittel darstellen, welches von Journalisten genutzt werden kann, um Inhalte an Personen zu vermitteln, die diese über andere Mittel einem breiteren Spektrum zugänglich machen können.[102]

III. Aktivismus und Whistleblowing im Darknet

Das Darknet hat sich als ein bewährtes Mittel für politische Aktivisten entwickelt, denen bei der Nutzung konventioneller Kommunikationsmethoden eine Verfolgung droht. So ist beispielsweise die Opposition in Syrien, nachdem dort seit den Jahren 2010 und 2011 der Zugang zum Internet verstärkt eingeschränkt worden ist, auf das Darknet ausgewichen.[103]

Auch in der Bundesrepublik sind politische Aktivisten im Darknet tätig. So waren beispielsweise die von Aktivisten aus dem linksextremen Spektrum genutzten deutschen Ableger von Indymedia, de.Indymedia.org[104] und sowie Linksunten.indymedia.org, welche im August 2017 verboten wurde, im Darknet zu finden.[105]

---

100 *Schlag/Wenz*, Deutschlandfunk vom 12.02.2018.
101 *Epakto,* Mexican Drug Cartels New Target: Blogger.
102 *Moßbrucker,* APUZ vom 10.11.2017
103 *Schlag/Wenz,* Deutschlandfunk vom 12.02.2018.
104 Die hierzu gehörige Darknetadresse lautet: http://4sy6ebszykvcv2n6.onion/ (Zuletzt abgerufen am 27.03.2018).
105 *Mey,* Heise Online vom 16.11.2017;

Aber auch rechtsextreme Kreise haben im Darknet Kommunikationsnetze eingerichtet, so betreib beispielsweise die US-Amerikanische rechtsextreme Nachrichtenseite The Daily Stormer ein geschlossenes Diskussionsforum im Darknet.[106]

Eine besondere Bedeutung hat das Darknet auch für sogenannte Whistleblower, welche durch dieses Netzwerk über illegales Handeln von Behörden oder Unternehmen, Korruptionsfälle, Insiderhandel oder andere Problematiken informieren können, ohne dabei eine direkte Rückverfolgung der Informationen zu der eigenen Person zu ermöglichen.

So wurde eine nicht unerhebliche Anzahl der großen Enthüllungen in den letzten Jahren durch Skandalaufdecker veranlasst.

Die der Weltöffentlichkeit bekannt gewordenen drastischen Folgen, die ihr Handeln beispielsweise für Informanten wie Bradley Manning oder Edward Snowden nach sich gezogen hat, dürfte eine abschreckende Wirkung für weitere Whistleblower haben.

Durch eine Verringerung der Entdeckungsgefahr können somit wieder stärkere Anreize für die Aufdeckung von Missständen geschaffen werden.

IV. Staatliche Nutzung des Darknets

Das Darknet wird auch von staatlichen Institutionen genutzt. Vor diesem Hintergrund ist es wenig überraschend, dass staatliche Stellen, im diesem Fall im Besonderen US-Amerikanische Militärbehörden, beispielswiese auch bei der Entwicklung des TOR-Netzwerkes involviert waren und im Jahre 2011 60% die Finanzierung des Projektes aus Zuwendungen des US-Regierung erfolgte.[107]

Das Darknet kann dabei zur Informationsgewinnung oder zur verdeckten Operation oder Kommunikation genutzt werden. So können beispielsweise Ermittler verdächtige Webseiten observieren, ohne dass die Zielpersonen durch die Kenntnisnahme von Zugriffen durch für sie auffällige IP-Adressen gewarnt werden können.

Denkbar ist auch, dass Strafverfolgungsbehörden dort Annahmestellen für anonyme Hinweise einrichten können. Diese Nutzung des Darknets ist natürlich nicht auf abwehrende Maßnahmen beschränkt.

So wird beispielsweise der Volksrepublik China vorgeworfen, durch Industriespionage, welche auch über das Darknet erfolgt, die eigene Wirtschaft zu starken.[108]

106 http://bbs.dstormer6em3i4km.onion/ (Zuletzt abgerufen am 27.03.2018).
107 *O'Neill,* How Tor is building a new Dark Net; TOR Annual Report 2012, S. 8 der PDF.
108 *Witsch,* Wirtschaftswoche vom 26.05.2016.

F. Zusammenfassende Betrachtung

Das Darknet ist mehr als nur ein harmloses Medium zur anonymisierten Kommunikation, sondern schafft eine mannigfaltige Anzahl von neuen Vorgehensmöglichkeiten für Straftäter.

Gleichzeitig ist eine pauschale Verurteilung, welche ein bestimmtes Medium zur Ursache eines Problems stigmatisiert, so wie dies beispielsweise in der Vergangenheit schon im Rahmen der sogenannten Killerspieldebatte passiert ist[109], ebenfalls unangebracht und wenig zielführend.

So wie beispielsweise die Käufer eines Marktes für Betäubungsmittel im Falle dass dieser geschlossen wird auf den nächsten Markt ausweichen, so würde ein Wegfall des Darknets wohl nur in den wenigstens Fällen die Folge nach sich ziehen, dass die dort stattfindende Kriminalität in der analogen oder restlichen digitalen Welt, beispielsweise innerhalb von Peer-to-Peer-Netzwerken, ebenfalls unterbleibt. Trotzdem sind stetige Maßnahmen der Strafverfolgungsbehörden notwendig, um die kriminellen Aktivitäten wenigstens einzudämmen und nicht das Gefühl eines vollkommen rechtsfreien Raumes im Internet entstehen zu lassen.

Da sich solche Maßnahmen jedoch häufig als kosten- und aufwandsintensiv darstellen, ist eine Fokussierung der Maßnahmen auf besonders problematische Kriminalitätsbereiche notwendig. Hierbei ist auch zu berücksichtigen, dass sich die gesellschaftlichen Auswirkungen der Deliktsbegehung über das Darknet je nach Deliktsart durchaus unterscheiden können.

Während beispielsweise der Handel und Austausch von pädopornographischen Material oder Waffen durch das Darknet ein deutlich gesteigertes Bedrohungspotential erlangen, können im Rahmen des Handels mit Betäubungsmitteln auch positive Effekte denkbar sein. So besteht beispielsweise die Möglichkeit, dass die Händler aufgrund eines Interesses an positiven Kundenbewertungen und dem Druck durch Mitbewerber Drogen von höherer Qualität veräußern und auf das Strecken ihrer Ware mit schädlichen Substanzen verzichten.

Auch kommt es im Zusammenhang mit analogen Drogenmärkten regelmäßig zu Gewaltdelikten, teilweise geschieht dies aufgrund von Meinungsstreitigkeiten zwischen den Parteien, aber auch Konflikte zwischen den Händler, beispielsweise bei der Übernahme von Märkten, können gewalttätige Auseinandersetzungen zur Folge haben, welche im Rahmen eines digitalisierten Handels kaum denkbar sind.

Weiterhin ist in Betracht zu ziehen, dass die Anwendung von modernen technischen Ermittlungsinstrumenten häufig nicht unerhebliche Eingriffe in die Privatsphäre und die Freiheitsrechte der gesamten Gesellschaft erfordert.

---

109 Hierzu exemplarisch nur: *Brühl,* Süddeutsche Zeitung vom 23.07.2016.

Auch ist der tatsächliche Nutzen solcher schweren Eingriffe häufig fraglich, so kam beispielweise ein Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahre 2011 zu dem Ergebnis, dass Vorratsdatenspeicherung zu keiner messbaren Steigerung der Aufklärungsquote führt.[110]

Auch können die Maßnahmen zur Schwächung von Verschlüsselungen die Sicherheitsinteressen von Bürgern beeinträchtigen, ohne dass diese einem direkten Eingriff durch staatliche Institutionen ausgesetzt sind.

So können beispielsweise staatliche Hintertüren in technischen Geräten oder Softwareprogrammen auch von Hackern oder fremden Geheimdiensten als mögliche Schwachpunkte innerhalb eines Sicherheitssystemes erkannt und ausgenutzt werden.

Gleichzeitig ist jedoch davon auszugehen, dass der tatsächliche Nutzung solcher Maßnahmen sich innerhalb eines überschaubaren Rahmens halten dürfte, da Kriminelle und Terroristen nach Bekanntwerden solcher Hintertüren verstärkt zu Anwendungen greifen werden, die aufgrund ihrer Natur keiner staatlichen Kontrolle unterliegen, beispielweise Open-Source-Software.

Hinzu kommt, dass die Frage danach, was genau als kriminelles Handeln einzuordnen ist, auch wesentlich von staatlichen und gesellschaftlichen Wertungen und Entscheidungen abhängt. Eine Schwächung von Verschlüsselungsmöglichkeiten, welche in Deutschland zur Bekämpfung des Waffenhandels im Darknet genutzt wird, kann von einem autoritär geführten Staat gegen Menschenrechtsorganisationen, Dissidenten und Journalisten zur Anwendung gebracht werden.

Da gerade Computerprogramme einer sehr leichten und schnellen Verbreitung zugänglich sind, lässt sich nur schwer beschränken, wer solche Software nutzen kann. So hatte beispielsweise der marokkanische Staat den regierungskritischen Blogs *Mamfakinch* mit Hilfe von italienischer Überwachungssoftware bekämpft.[111]

Weiterhin ist zu beachten, dass auch in demokratisch organisierten Staaten die Gefahr eines Missbrauches von Überwachungssoftware möglich ist.

Da in Menschenrechtsverletzungen, Kriegsverbrechen oder Korruption verwickelte staatliche Institutionen ein bedeutendes Interesse an der Geheimhaltung ihrer problembehafteten Aktivitäten haben, besteht auch für sie tatsächlicher Bedarf für Mittel, die zur Entanonymisierung von Whistleblowern oder Journalisten eingesetzt werden können. So wurden beispielsweise in Mexiko Journalisten mit Spionagesoftware attackiert, welche einer israelischen Firma zugeschrieben worden ist, die laut eigenen Aussagen ihre Technologie nur an Regierungen zur Kriminalitätsbekämpfung veräußert.[112]

---

110 *Kilchling,* Schutzlücken durch Wegfall der Vorratsdatenspeicherung? S. 239 ff. der PDF.

111 *Moßbrucker,* APUZ vom 10.11.2017.

112 *Angulo,* Reuters vom 20.06.2017.

Auch der durch unabhängige Medien und staatliche Institutionen geschaffenen Wahrnehmung des Darknets kommt eine wichtige Bedeutung zu.

Sobald das Darknet in der kollektiven Wahrnehmung zentral als Rückzugsort für Straftäter stigmatisiert ist, kann dies legitime Nutzer abschrecken und die Entfaltung einer demokratisierenden Wirkung des Darknets, wie sie zuvor bereits oft dem Clearweb zugeschrieben worden ist[113], wesentlich behindern.

Hinzu kommt, dass während das Bedrohungspotenzial durch über das Darknet erfolgende Kriminalität über Statistiken und medial weitläufig zur Kenntnis genommene Beispielsfälle wie den Amoklauf von München aus dem Jahre 2016 leicht verdeutlicht werden kann, das demokratische Potenzial des Darknets sich jedoch dagegen schwer in Zahlen und direkt wahrnehmbaren Effekten darstellen lässt. Für die Emanzipierung gesellschaftlich marginalisierter Gruppen oder die Schaffung neuer gesellschaftlicher Impulse durch alternative Kommunikationswege werden in Statistiken zu fassende Zahlen schließlich kaum zu bemessen sein. Das Darknet hat somit mit der klassischen Problematik zu kämpfen, dass die Wohltaten der Freiheit häufig erst im Moment ihres Wegfalles bewusst wahrgenommen werden, eine Bedrohungssituation hingegen eine deutlich direktere Wahrnehmung hervorruft.

Das Darknet verkörpert letztendlich in einem besonderen Maße den Umstand, dass freiheitliche Gesellschaften in einem erhöhten Maße den Bedrohungen von Kriminalität und Terrorismus ausgesetzt sind.

Die Vorzüge von Freiheiten und das Ausleben freiheitlich-demokratischer Werte werden somit auch dadurch erkauft, dass ein gewisses durch sie geschaffenes Missbrauchspotenzial akzeptiert und auch in einem gewissen Maße toleriert werden muss.

Eine Regulation des Darknets durch staatliche Institutionen ist somit zwar notwendig, darf jedoch nicht zur Folge haben, dass durch sie die Schaffung anonymer Rückzugsorte verhindert wird, da anderweitig eine Infragestellung unserer Freiheitsrechte an sich droht.[114]

113 Hierzu exemplarisch: *Grob,* Neue Zürcher Zeitung vom 06.03.2009.

114 *Moßbrucker,* APUZ vom 10.11.2017.

Literaturverzeichnis

Aldrige, Judith Askew, Rebecca	Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement, International Journal of Drug Policy 2017, 101, abrufbar unter: https://www.sciencedirect.com/science/article/pii/S0955395916303140 (Zuletzt abgerufen am 25.03.2018)
Aldridge, Judith Décary-Hétu, David	Hidden wholesale: The drug diffusing capacity of online cryptomarkets, PDF-Datei abrufbar unter: https://www.sciencedirect.com/science/article/pii/S0955395916301335 (Zuletzt abgerufen am 25.03.2018)
Angulo, Sharay	Activists and journalists in Mexico complain of goverment spying, Reuters vom 20.06.2017, abrufbar unter: https://www.reuters.com/article/us-mexico-spyware/activists-and-journalists-in-mexico-complain-of-goverment-spying-idUSKBN19A30Y (Zuletzt abgerufen am 25.03.2018)
Bock, Stefanie Harrendorf, Stefan	Strafbarkeit und Strafwürdigkeit tatvorbereitender computervermittelter Kommunikation, ZSTW 2014, 337
Boehm, Franziska Pech, Paulina	Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung – Eine erste juristische Einschätzung, MMR 2014, 75
Brühl, Jannis	Zurück in die Nullerjahre: De Maizière reanimiert die Killerspiel-Debatte, Süddeutsche Zeitung vom 23.07.2016, abrufbar unter: www.sueddeutsche.de/digital/amoklauf-in-muenchen-zurueck-in-die-nuller-jahre-de-maizire-reanimiert-killerspiel-debatte-1.3092117 (Zuletzt abgerufen am 25.03.2018)
Candea, Stefan Dahlkamp, Jürgen Schmitt, Jörg Ulrich, Andreas Wiedmann-Schmidt, Wolf	How EU Failures Helped Paris Terrorists Obtain Weapons, Spiegel Online vom 24.03.2016, abrufbar unter: www.spiegel.de/international/europe/following-the-path-of-the-paris-terror-weapons-a-1083461.html (Zuletzt abgerufen am 25.03.2018)
Chertoff, Michael Simon, Tobby	The Impact of the Dark Web on Internet Governance and Cyber Security, abrufbar unter: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf (Zuletzt abgerufen am 25.03.2018)

Christin, Nicolas Soska, Kyle	Measuring the Longitudinal Evolution oft he Online Anonymous Marketplace Ecosystem, abrufbar unter: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf (Zuletzt abgerufen am 25.03.2018)
Ciancaglini, Vincenzo Balduzzi, Marco McArdle, Robert Rösler, Martin	Das Deep Web erkunden, abrufbar unter: www.trendmicro.de/media/wp/tl-forschungspapier-deep-web-whitepaper-de.pdf (Zuletzt abgerufen am 25.03.2018)
Christin, Nicolas	Traveling the Silk Road: A measurment analysis of a large anonymous online marketplace, https://arxiv.org/pdf/1207.7139.pdf (Zuletzt abgerufen am 25.03.2018)
Décary-Hétu, David Laferrière, Dominique	Discrediting Vendors in Online Criminal Markets, abrufbar unter: http://daviddhetu.openum.ca/files/sites/39/2016/05/Decary-Hetu-And-Laferriere-revised.pdf (Zuletzt abgerufen am 25.03.2018)
Epakto, Larisa	Mexican Drug Cartels New Target: Bloggers, vom 13.10.2011, abrufbar unter: https://www.pbs.org/newshour/world/mexico-bloggers (Zuletzt abgerufen am 25.03.2018)
Europäische Beobachtungsstelle für Drogen und Drogensucht	Europäischer Drogenbericht 2017 – Trends und Entwicklungen, abrufbar unter: https://www.dbdd.de/fileadmin/user_upload_dbdd/05_Publikationen/PDFs/EDR-2017_DE.pdf (Zuletzt abgerufen am 25.03.2018)
Europol	Intellectual Property Crime on the Darknet, abrufbar unter: https://www.europol.europa.eu/publications-documents/intellectual-property-crime-darknet (Zuletzt abgerufen am 25.03.2018)
Europol	Internet Organised Crime Thread Assesment (IOCTA) 2016, abrufbar unter: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (Zuletzt abgerufen am 25.03.2018)
Europol	Internet Organised Crime Threat Assesment (IOCTA) 2017, abrufbar unter: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (Zuletzt abgerufen am 25.03.2018)

Federl, Fabian	Wie kommt ein 18-Jähriger an eine Waffe?, Der Tagesspiegel vom 25.07.2016, abrufbar unter: https://www.tagesspiegel.de/politik/waffen-kauf-im-darknet-wie-kommt-ein-18-jaehriger-an-eine-waffe/13925060.html (Zuletzt abgerufen am 25.03.2018)
Fünfsinn, Helmut Ungefuk, Georg Krause, Benjamin	Das Darknet aus Sicht der Strafverfolgungsbehörden, Krim 2017, 440
Gercke, Marco	Die Entwicklung des Internetstrafrechts 2015/2016, ZUM 2016, 825
Gibbs, Samuel Beckett, Lois	Dark web marketplaces AlphaBay and Hansa shut down, The Guardian vom 20.07.2017, abrufbar unter: https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down (Zuletzt abgerufen am 25.03.2018)
Goebel, Jacqueline Berke, Jürgen	Wie Kriminelle die Packstation missbrauchen, Wirtschaftswoche vom 22. Dezember 2015, abrufbar unter: https://www.wiwo.de/unternehmen/dienstleister/deutsche-post-wie-kriminelle-die-packstation-missbrauchen/12734012.html (Zuletzt abgerufen am 25.03.2018)
Greenberg, Andy	Global police spring a trap on thousands od ark web users, Wired vom 20.07.2017, abrufbar unter: https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/ (Zuletzt abgerufen am 25.03.2018)
Greenberg, Andy	Operation Bayonet: Inside the sting that hijacked an entire dark web drug market, Wired vom 08.03.2018, abrufbar unter: https://www.wired.com/story/hansa-dutch-police-sting-operation/ (Zuletzt abgerufen am 25.03.2018)
Grob, Ronnie	Das Internet fördert die Demokratie, Neue Zürcher Zeitung vom 06.03.2009, abrufbar unter: https://www.nzz.ch/das_internet_foerdert_die_demokratie-1.2150453 (Zuletzt abgerufen am 25.03.2018)
Hostettler, Otto	Darknet – Die Schattenwelt des Internets, 1. Auflage, Zürich 2017
Intelliagg	Shining a light on the dark web, abrufbar unter: https://media.scmagazine.com/documents/224/deeplight_(1)_55856.pdf (Zuletzt abgerufen am 26.03.2018)
Joecks, Wolfgang Miebach, Klaus	Münchener Kommentar zum Strafgesetzbuch, Band 3 & 4, 3. Auflage, München 2017
Kindhäuser, Urs Neumann, Ulfrid Paeffgen, Hans-Ullrich	Kommentar zum Strafgesetzbuch, 5. Auflage, Baden-Baden 2017

Perry, Mike Clark, Erinn Murdoch, Steven Koppen, Georg	The Design and Implementation of the TOR Browser [DRAFT], abrufbar unter: https://www.torproject.org/projects/torbrowser/design/ (Zuletzt abgerufen am 25.03.2018)
Kochheim, Dieter	Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 1. Auflage 2015
Koops, Bert-Jaap Goodwin, Morag	Cyberspace, the cloud, and cross-border criminal investigation, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 (Zuletzt abgerufen am 25.03.2018)
Krause, Benjamin	Ermittlungen im Darknet – Mythos und Realität, NJW 2018, 678
Krause, Benjamin	„Retrograde“ Auskunftsverlangen der Strafverfolgungsbehörden an Postdienstleister – Zugleich Besprechung von BGH, Beschl. V. 27.10.2016 – 1 BGs 107/16, NZWiSt 2017, 60
Kruithof, Kristy Aldridge, Judith Décary-Hétu, David Sim, Megan Dujso, Elma Hoorens, Stijn	Internet-facilitated drugs trade, abrufbar unter: https://www.wodc.nl/binaries/2671-volledige-tekst_tcm28-124626.pdf (Zuletzt abgerufen am 25.03.2018)
Kudlich, Hans	Münchener Kommentar zur Strafprozessordnung, Band 1 §§ 1 – 150 StPO, 1. Auflage, München 2014
Makrushin, Denis	Was kostet eine DDoS-Attacke, abrufbar unter: https://de.securelist.com/the-cost-of-launching-a-ddos-attack/72496 (Zuletzt abgerufen am 25.03.2018)
Martin, James	Lost on the Silk Road: Online drug distribution and the ‚Cryptomarket‘, Criminology & Criminal Justice 2014, 351, abrufbar unter: journals.sagepub.com/doi/pdf/10.1177/1748895813505234 (Zuletzt abgerufen am 25.03.2018)
Mey, Stefan	Darknet – Waffen, Drogen, Whistleblower, 1. Auflage, München 2017
Mey, Stefan	Das “Gute“ Darknet, Heise Online vom 16.11.2017, abrufbar unter: https://www.heise.de/tp/features/Das-gute-Darknet-3888203.html (Zuletzt abgerufen am 25.03.2018)
Meywirth, Carsten	Crime-as-a-Service, Krim 2016, 355

Moore, Daniel Rid, Thomas	Cryptopolitik and the Darknet, abrufbar unter: https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085 (Zuletzt abgerufen am 25.03.2018)
Moßbrucker, Daniel	Netz der Dissidenten. Die Helle Seite im Darknet, APUZ vom 10.11.2017, abrufbar unter: www.bpb.de/apuz/259139/netz-der-dissidenten?p=all (Zuletzt abgerufen am 25.03.2018)
Murdock, Jason	Hitman for hire: How the dark web contract-killer seite BesaMafia was exposed by a hacker, International Business Times vom 13.05.2016, abrufbar unter: www.ibtimes.co.uk/hitman-hire-how-dark-web-contract-killer-site-besamafia-was-exposed-by-hacker-1560001 (Zuletzt abgerufen am 25.03.2018)
O'Neill, Patrick Howell	How Tor is building a new Dark Net with help from the U.S. military, The Daily Dot vom 20.04.2015, abrufbar unter: https://www.dailydot.com/layer8/next-generation-tor-darpa/ (Zuletzt abgerufen am 25.03.2018)
Owen, Gareth Savage, Nick	The Tor Dark Net, abrufbar unter: https://www.cigionline.org/sites/default/files/no20_0.pdf (Zuletzt abgerufen am 20.03.2018)
Paoli, Giacomo Persi Aldrige, Judith Ryan, Nathan Warnes, Richard	Behind the Curtain – The illicit trade of firearms, explosives and ammunition on the dark web, abrufbar unter: https://de.scribd.com/document/354452956/Behind-the-curtain (Zuletzt abgerufen am 25.03.2018)
Ronser, Yotam London, Sean Mendelboim, Avaid	Backdoor Plots: The Darknet as a Field for Terrosism, INSS Insight No. 464 vom 23. September 2013, abrufbar unter: www.inss.org.il/publication/backdoor-plots-the-darknets-as-a-field-for-terrorism/ (Zuletzt abgerufen am 25.03.2018)
Schlag, Gabi Wenz, Benno	Die helle Seite des Darknet, Deutschlandfunk vom 12.02.2018, abrufbar unter: www.deutschlandfunk.de/investigativer-journalismus-die-helle-seite-des-darknet.2907.de.html?dram:article_id=410574 (Zuletzt abgerufen am 25.03.2018)
Schulze, Matthias	Clipper Meets Apple vs. FBI - A Comparison of the Cryptography Discourses from 1993 and 2016, Media and Communication 2017, 54
Sieber, Ulrich Satzger, Helmut Heintschel-Heinegg, Bernd von	Europäisches Strafrecht, 2. Auflage, Baden-Baden 2014

Stam, Fabian	Die Datehhehlerei nach § 202d StGB – Anmerkungen zu einem sinnlosen Straftatbestand, StV 2017, 488.
Teichmann, Fabian	Terrorismusfinanzierung – Teil 3: die Bedeutung von Kryptowährungen, Krim 2018, 30
TOR Project	TOR Annual Report 2012, abrufbar unter: https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf (Zuletzt abgerufen am 25.03.2018)
Weimann, Gabriel	Terrorist Migration the the Dark Web, abrufbar unter: www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html (Zuletzt abgerufen am 25.03.2018)
Weisser, Niclas-Frederic	Strafprozessuale Auskunftsersuchen über Postsendungen, wistra 2016, 387
Williams,	Polonium-210: Poison used to kill Russian spy for sale online, Daily Star vom 24.07.2016, abrufbar unter: https://www.dailystar.co.uk/news/latest-news/532369/Poison-used-kill-Russian-spy-sale-online-Polonium-agent-web-dark-dead-fatal-Litvinenko (Zuletzt abgerufen am 27.03.2018)
Witsch, Kathrin	Unternehmen im Würgegriff der Cyberkriminellen, Wirtschaftswoche vom 26.05.2016, abrufbar unter: https://www.wiwo.de/technologie/darknet-unternehmen-im-wuergegriff-der-cyberkriminellen/13630890-all.html (Zuletzt abgerufen am 25.03.2018)
Wolff, Heinrich Amadeus Brink, Stefan	Beck'scher Onlinekommentar Datenschutzrecht, 22. Edition, Stand: 01.11.2017, München 2017
Wolter, Jürgen	Systematischer Kommentar zur Strafprozessordnung, Band 2 §§ 94 – 136a StPO, 5. Auflage, München 2016