Deanonymisierung im Tor-Netzwerk – Technische Möglichkeiten und rechtliche Rahmenbedingungen

Sandra Wittmer, Florian Platzer, Martin Steinebach und York Yannikos

Zusammenfassung

Eine anonyme Nutzung des Internets wird durch die Verwendung sogenannter „Darknet-Technologien“ wie der Tor-Software ermöglicht und ist hierzulande grundrechtlich geschützt. Neben zahlreichen positiven Verwendungszwecken werden solche Technologien allerdings oft auch zur anonymen Begehung von Straftaten eingesetzt. Da ein Verbot von Anonymisierungstechnologien sowohl aus technischer, als auch aus rechtlicher Sicht abzulehnen ist, wendet sich dieser Beitrag den Möglichkeiten der Strafverfolgung im Tor-Netzwerk zu. Es werden Vorgehensweisen zur Identifizierung tatverdächtiger Personen vorgestellt und aus rechtlicher Perspektive bewertet, ob diese von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären. Anhand dieser Erkenntnisse soll eine Diskussionsgrundlage für strafrechtliche Ermittlungen im Tor-Netzwerk geschaffen werden, ohne die Legitimität einer anonymen Nutzung des Internets grundsätzlich in Frage zu stellen.

S. Wittmer (✉)
TU Darmstadt, Darmstadt, Deutschland
E-mail: sandra.wittmer@sit.fraunhofer.de

F. Platzer · M. Steinebach · Y. Yannikos
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: florian.platzer@sit.fraunhofer.de

M. Steinebach
E-mail: martin.steinebach@sit.fraunhofer.de

Y. Yannikos
E-mail: york.yannikos@sit.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_8

Schlüsselwörter

Tor • Deanonymisierung • Technische Möglichkeiten • Rechtliche Rahmenbedingungen • Strafverfolgung • Darknet • Cybercrime

1 Einleitung

Tor – ursprünglich ein Akronym für „The Onion Router" – ist eine Darknet-Technologie zur Anonymisierung von Internet-Datenverkehr.[1] Die Tor-Software hat zum Ziel, ihren Nutzer*innen Anonymität und Zensurfreiheit im Internet bereitzustellen. In diesem Kapitel werden die technischen Grundlagen der Software erläutert und auf die Rolle des Tor-Netzwerks bei der Begehung von Straftaten eingegangen. Außerdem wird die Bedeutung einer anonymen Nutzung des Internets diskutiert.

1.1 Was ist das Tor-Netzwerk?

Anonyme Netzwerke wie Tor ermöglichen eine hinsichtlich zuordenbarer IP-Adressen anonyme Internet-Kommunikation und mittels der im Tor-Protokoll unterstützten „hidden services" auch den Betrieb von anonymen Servern. Dies wird dadurch erreicht, dass der gesamte Datenverkehr mehrfach verschlüsselt und über Datenpfade geleitet wird, die aus mindestens drei Tor-Knoten bestehen.[2] Dieses mehrlagige Verschlüsselungsschema – jeder Tor-Knoten „schält" eine Schicht der Verschlüsselung ab und leitet den entschlüsselten Teil an den nächsten Tor-Knoten weiter – ist dabei namensgebend für das Onion Routing (zu deutsch „Zwiebelrouting", vgl. Abb. 1). Bei den verwendeten Tor-Knoten, welche auch Tor-Relays oder Tor-Nodes genannt werden, handelt es sich um Rechner, die von Unterstützer*innen des Tor-Netzwerks freiwillig für die Weiterleitung des Datenverkehrs zur Verfügung gestellt werden. Jeder Tor-Knoten erhält dabei nur die Information, von welchem Tor-Knoten die aktuellen Datenpakete gesendet wurden und an welchen Tor-Knoten die Datenpakete als nächstes weitergeleitet werden müssen. Auf diese Weise wird verhindert, dass Dritte nachvollziehen können, wer mit wem und über was im Internet kommuniziert.

[1] Zur Kritik am Präfix „dark" und den damit einhergehenden negativen Assoziations- und Deutungsrahmen vgl. *Bovermann* (2019) [6], Framing-Check: Darknet, Süddeutsche Zeitung (03.05.2019), https://www.sueddeutsche.de/kultur/framing-darknet-tor-anonym-internet-silk-road-1.4367011 (letzter Zugriff: 10.10.2020).

[2] Hierzu ausführlich *Dingledine/Mathewson/Syverson* (2004) [9], Tor: The second-generation onion router, Naval Research Lab Washington DC 2004.

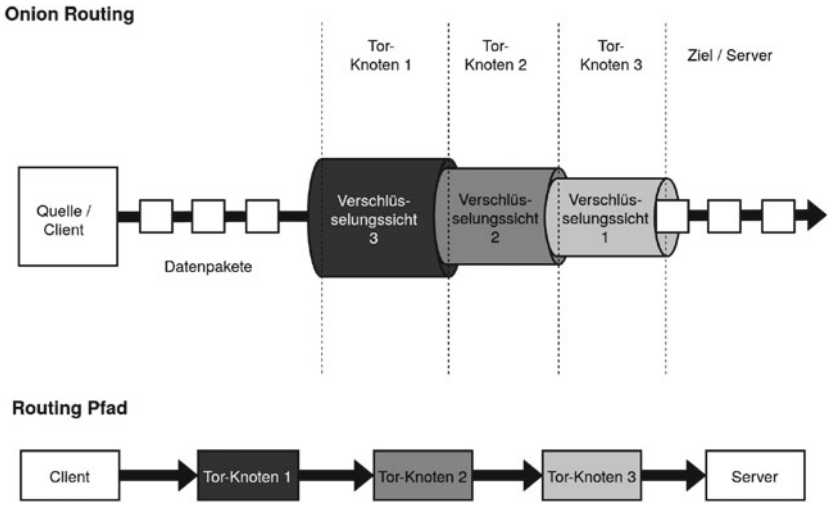

Abb. 1 Prinzip des Onion-Routings

1.2 Grundrechtlicher Schutz von Anonymität im Internet

Zu den positiven Verwendungszwecken von Anonymisierungstechnologien wie der Tor-Software zählt der freie Zugriff auf Informationen in autoritären politischen Umgebungen, wodurch etwa die Arbeit von Journalist*innen und Whistleblower*innen weltweit erleichtert wird. Außerdem lässt sich von der in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG durch das Grundrecht auf informationelle Selbstbestimmung geschützten Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen, durch den Einsatz der Tor-Software ideal Gebrauch machen.[3] Verfassungsrechtlich wird die Vertraulichkeit von Telekommunikationsvorgängen darüber hinaus auch durch das Fernmeldegeheimnis aus Art. 10 Abs. 1 Var. 3 GG gewährleistet, worunter neben den konkreten Inhalten der Kommunikation auch die näheren Umstände – also ob, wann und vor allem wer mit wem kommuniziert hat – fallen.[4] Hinzu kommt, dass sogenannte „chilling effects", welche die Nichtausübung von Grund- und Freiheitsrechten aus Furcht vor staatlicher Überwachung bezeichnen, durch die Verwendung von Anonymisierungssoftware

[3] Siehe hierzu bereits *Rückert* (2018) [24], Politische Studien 479/2018, S. 17.

[4] Vgl. BVerfGE 125, 260, 309 (Vorratsdatenspeicherung).

vermieden werden können.[5] Der Einsatz von Anonymisierungsdiensten wie der Tor-Software ist hierzulande demnach grundrechtlich geschützt und hat zahlreiche gesellschaftlich wünschenswerte Verwendungszwecke vorzuweisen.

1.3 Missbrauch der Tor-Software zur Begehung von Straftaten

Oftmals wird die Tor-Software jedoch auch dazu genutzt, Straftaten im Internet möglichst anonym zu begehen. In den letzten Jahren hat sich im Tor-Netzwerk daher eine Vielzahl neuartiger Kriminalitätsphänomene etabliert, die Strafverfolgungsbehörden auf der ganzen Welt vor Herausforderungen stellen. Webseiten mit tausenden Mitgliedern, über die verschiedene illegale Handelsgüter angeboten werden, sind hierfür bekannte Beispiele. Diese Webseiten funktionieren wie konventionelle E-Commerce-Plattformen im Clearnet, wohingegen dort praktisch alles gehandelt wird, was sich im legalen Marktgeschehen nicht veräußern lässt.[6] Die staatliche Verpflichtung, solche strafbare Aktivitäten effektiv zu verfolgen, wird durch den Einsatz der Tor-Software jedoch erheblich erschwert. Identifizierungsansätze, die bei Ermittlungen im Internet standardmäßig zur Anwendung kommen, bleiben im Tor-Netzwerk infolge des Onion-Routing erfolglos. Klassische Ermittlungsinstrumente – wie zum Beispiel Datenabfragen nach den §§ 14, 15 TMG oder strafprozessuale Auskunftsverlangen i. S. v. § 100j StPO – stehen den Ermittler*innen daher nicht zur Verfügung. So kommt es, dass auf Webseiten im Tor-Netzwerk ganz offen illegale Inhalte angeboten werden, ohne dass die betreffenden Plattformen von den Strafverfolgungsbehörden abgeschaltet werden können.

1.4 Ablehnung der Forderung nach einem „Darknet-Verbot"

Der Vorschlag, eine Nutzung von Anonymisierungstechnologien aus diesem Grund gänzlich zu verbieten, ist allerdings abzulehnen. Einerseits wäre ein solches Verbot bereits aus technischer Sicht nicht realisierbar, da neben der Tor-Software weitere Anonymisierungsdienste wie I2P, Freenet oder JonDo existieren, die alle auf unterschiedlichen Technologien basieren. Man müsste für jedes dieser anonymen Netzwerke eine eigene Strategie entwerfen, um sie „abschalten" zu können. Anonyme

[5] Hierzu ausführlich *Bartl/Moßbrucker/Rückert* (2019) [2], Angriff auf die Anonymität im Internet, S. 18–19.

[6] Vgl. *Fünfsinn/Ungefuk/Krause* (2017) [11], Kriminalistik 2017, 440 (442).

Netzwerke sind jedoch gerade darauf ausgerichtet, zensurresistent zu sein und werden aus diesem Grund dezentral betrieben. Die technische Infrastruktur von Tor basiert beispielsweise auf über 6.500 verschiedenen Tor-Knoten, die über die ganze Welt verteilt sind.[7] Ein Verbot von Darknet-Technologien könnte in der Praxis daher nur umgesetzt werden, indem versucht wird, den Zugriff auf die betreffenden Netzwerke zu blockieren.[8] Hinzu kommt, dass ein Verbot von Anonymisierungstechnologien auch aus rechtlicher Perspektive abzulehnen wäre. Dass das Darknet in freiheitlich-demokratischen Rechtsordnungen „keinen legitimen Nutzen" haben kann,[9] ist in Anbetracht des grundrechtlichen Schutzes von anonymer Internetkommunikation entschieden zurückzuweisen. Es ist gerade als Privileg freiheitlich-demokratischer Gesellschaften anzusehen, dass Menschen fernab von staatlicher Überwachung im Internet miteinander kommunizieren können.[10] Das Spannungsfeld zwischen der staatlichen Verpflichtung, strafbare Aktivitäten im Tor-Netzwerk effektiv zu verfolgen und dem Recht darauf, sich im Internet durch den Einsatz von Darknet-Technologien anonym zu bewegen, kann daher nicht einseitig durch ein Verbot von Anonymisierungsdiensten gelöst werden.

2 Technische Möglichkeiten der Strafverfolgung im Tor-Netzwerk und deren rechtliche Bewertung

Da ein Verbot von Darknet-Technologien sowohl aus technischer, als auch aus rechtlicher Perspektive abzulehnen ist, wendet sich dieser Beitrag den Möglichkeiten einer effektiven Strafverfolgung im Tor-Netzwerk zu. Zu diesem Zweck werden

[7] Vgl. Tor Metrics, Number of relays, abrufbar unter https://metrics.torproject.org/networksize.html (letzter Zugriff: 28.09.2020).

[8] Im Falle von Tor wäre es zwar möglich, die IP-Adressen der öffentlich gelisteten Tor-Knoten zu blockieren, allerdings bietet die Software genau aus diesem Grund sogenannte „Bridge-Knoten" an, die in diesen Konstellationen als nicht-öffentliche Einstiegspunkte in das Netzwerk genutzt werden können. Diese können außerdem mit sogenannten „Pluggable Transports" kombiniert werden, um sich mit dem Tor-Netzwerk verbinden zu können, ohne dass die Nutzung der Software für Dritte – beispielsweise staatliche Stellen – überhaupt erkennbar ist.

[9] So etwa der parlamentarische Staatssekretär beim Bundesinnenministerium Günter Krings (CDU); zitiert nach *Borchers* (2019) [5], Europäischer Polizeikongress: Weg mit dem Darknet, Heise Online (20.02.2019), abrufbar unter https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Weg-mit-dem-Darknet-4313276.html (letzter Zugriff: 06.09.2019).

[10] Ausführungen zur Bedeutung von Anonymität in liberalen Verfassungsstaaten finden sich bei *Kersten* (2017) [15], JuS 2017, 193–203.

Ermittlungsansätze vorgestellt, die aus technischer Sicht zur Identifizierung tatverdächtiger Personen beitragen können. Da strafrechtliche Ermittlungen dem Prinzip vom Vorbehalt des Gesetzes genügen müssen, werden diese Ansätze sodann aus rechtswissenschaftlicher Perspektive bewertet und hinterfragt, ob sie von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären. Ziel ist es, eine Diskussionsgrundlage für mögliche Vorgehensweisen bei der Strafverfolgung im Tor-Netzwerk zu schaffen, ohne die Legitimität einer anonymen Nutzung des Internets grundsätzlich in Frage zu stellen.

2.1 Betrieb von Honeypot-Servern

Eine Möglichkeit zur Identifizierung von tatverdächtigen Personen im Tor-Netzwerk ist in dem Aufsetzen und Betreiben von Honeypot-Servern zu sehen. Ein Honeypot ist eine gefälschte Computerressource, mit deren Hilfe Angreifer*innen angelockt werden sollen. Da Honeypot-Server durchgängig überwacht werden können, kommen sie häufig zum Einsatz, um Informationen über Angriffsmuster einzuholen.[11]

2.1.1 Technische Beschreibung

Über einen Honeypot-Server könnten Ermittlungsbehörden einen gefälschten Darknet-Marktplatz aufsetzen, über den zum Schein Drogen oder Waffen angeboten werden. Dadurch wären sie in der Lage, zu beobachten, welche Plattform-Mitglieder sich für welche illegalen Produkte interessieren, welche Versandart ausgewählt wird und welche Kontakt- beziehungsweise Lieferadressen auf den Webseiten angegeben werden. Diese Informationen könnten sodann als Anknüpfungspunkte für weitergehende strafrechtliche Ermittlungen herangezogen werden. Allerdings können sich Handelsplattformen im Tor-Netzwerk nur etablieren, wenn tatsächlich inkriminierte Güter über die in Rede stehenden Webseiten gehandelt werden. Plattformen, über die nur zum Schein illegale Waren angeboten werden, würden in der Praxis daher schnell als „Fake-Marktplätze“ enttarnt werden. Möglich wäre es jedoch, echte Plattformen von zuvor bereits ermittelten Tatverdächtigen zu übernehmen und zum Zwecke der Strafverfolgung über Honeypot-Server weiterzubetreiben, wie es etwa bei der Übernahme des Online-Marktplatzes „Hansa Market“ durch niederländische Ermittler*innen der Fall war.[12] Bis zur Abschaltung der Webseite ließen die

[11] Siehe hierzu *Moore* (2016) [10], Detecting ransomware with honeypot techniques.

[12] Vgl. *Europol* (2017) [10], Massive blow to criminal Dark Web activities after globally coordinated operation, abrufbar unter https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (letzter Zugriff: 24.01.2020).

Behörden sämtliche über „Hansa Market“ angebahnte Handelsgeschäfte weiterlaufen, wodurch tausende Informationen über ausländische Plattform-Kund*innen gesammelt und an Europol übergeben werden konnten.[13]

2.1.2 Rechtliche Einordnung

Hierzulande wäre eine Übernahme von echten Darknet-Plattformen wie „Hansa Market“ und deren Weiterführung über behördliche Honeypot-Server rechtlich allerdings nicht möglich. Durch den Betrieb von Online-Plattformen, auf denen tatsächlich ein Austausch krimineller Waren stattfindet, werden nämlich verschiedene Straftatbestände aus dem Kern- und Nebenstrafrecht verwirklicht.[14] Wer Drogen-Marktplätze und andere kriminell ausgerichtete Online-Plattformen im Tor-Netzwerk betreibt, macht sich folglich strafbar. Hierzulande sind Ermittlungsbeamt*innen jedoch grundsätzlich nicht berechtigt, zum Zwecke der Strafverfolgung selbst Straftaten zu begehen. Zwar kennt auch die deutsche Rechtsordnung gesetzliche Ausnahmeregelungen von diesem Grundsatz. Für das Betreiben von Online-Plattformen im Tor-Netzwerk ist dies jedoch nicht der Fall. In den Niederlanden, USA und Australien sind solche Ermittlungshandlungen hingegen zulässig. Dass ein Weiterbetrieb krimineller Plattformen über Honeypot-Server jedoch auch im Ausland erhebliche rechtliche Schwierigkeiten mit sich bringt, hat der Fall der Kinderporno-Tauschbörse „Childsplay“ deutlich gemacht. Die Webseite wurde für ganze elf Monate nach der Verhaftung des Plattform-Administrators von australischen Ermittlungsbehörden weiterbetrieben.[15] Da in dieser Zeit kinderpornografische Dateien von den Plattform-Mitgliedern weltweit verbreitet und ausgetauscht werden konnten, wurde das Vorgehen der Ermittler*innen vom Kinderhilfswerk der Vereinten Nationen als ein Verstoß gegen die UN-Kinderrechtskonvention gewertet.[16] Auch Vertreter*innen von Amnesty International verurteilten das Vorgehen der australischen Ermittler*innen als menschenrechtswidrig und inakzepta-

[13] Vgl. *Böhm* (2017) [4], Ermittler zerschlagen zwei der größten Darknet-Marktplätze, Spiegel Online vom 20.07.2017, abrufbar unter https://www.spiegel.de/netzwelt/netzpolitik/darknet-ermittler-zerschlagen-grosse-marktplaetze-alphabay-und-hansa-a-1158933.html (letzter Zugriff 29.09.2020).

[14] Hierzu ausführlich *Greco* (2019) [12], ZIS 2019, 435–450; *Safferling/Rückert* (2018) [27], Analysen & Argumente 291 (2018), S. 1–15; *Ceffinato* (2017) [7], JuS 2017, 403–408; *Bachmann/Nergiz* (2019) [1], NZWiSt 2019, 241–248.

[15] Vgl. *Schulz* (2017) [28], Australiens Polizei betrieb riesige Kinderporno-Plattform, Spiegel Online vom 11. 10. 2017, abrufbar unter http://www.spiegel.de/panorama/justiz/australien-polizei-ermitteltemit-eigener-kinderporno-plattform-a-1172503.html (letzter Zugriff: 15.09.2020).

[16] Vgl. *Knoph Vigsnæs* et al. (2017) [16], VG vom 9.10.2017, UNICEF: Clear violation of UN children’s convention. International humanitarian organizations express strong reaction to

bel.[17] In Deutschland wäre eine Übernahme und Weiterführung von kriminellen Online-Marktplätzen und Kinderporno-Tauschbörsen über Honeypot-Server jedenfalls unzulässig.

2.2 Betrieb von Phishing-Webseiten

Eine Alternative zum Aufsetzen und Betreiben von Honeypot-Servern könnte das Abgreifen von Login-Informationen über sogenannte Phishing-Webseiten darstellen. Beim Phishing werden sensible persönliche Daten ausgespäht, indem sich ein*e Angreifer*in als vertrauenswürdige*r Dritte*r ausgibt[18] und eine gefälschte Webseite aufsetzt. Werden auf dieser Webseite Login-Informationen wie Account-Namen und Passwörter eingegeben, können die Betreiber*innen der Phishing-Webseiten die Daten ausspähen und selbst verwenden.

2.2.1 Technische Beschreibung

Ermittlungsbehörden könnten die Webseiten bekannter Darknet-Plattformen fälschen und die Kund*innen dieser Plattformen auf die manipulierten Phishing-Webseiten locken. Sollten sie dort ihre Login-Informationen eingeben, würden diese nicht an den Darknet-Dienst geschickt, sondern direkt an die Ermittler*innen weitergeleitet werden. Mit den ausgespähten Login-Informationen könnten sich diese sodann auf den echten kriminellen Plattformen und Marktplätzen anmelden und auf die Accounts der Plattform-Kund*innen zugreifen. Dadurch könnten die Ermittler*innen an beweiserhebliche Informationen gelangen, wie zum Beispiel in der Vergangenheit getätigte Käufe und Verkäufe, Lieferadressen oder Bitcoin-Wallets der Plattfom-Kund*innen.

2.2.2 Rechtliche Einordnung

Aus rechtlicher Perspektive ermächtigt die Online-Durchsuchung i. S. v. § 100b StPO Ermittlungsbehörden zwar unter besonderen Voraussetzungen dazu, in informationstechnische Systeme tatverdächtiger Personen einzugreifen, um an deren

---

Australia's undercover police operation, abrufbar unter https://www.vg.no/nyheter/utenriks/i/L8ly4/unicef-clear-violation-of-un-childrens-convention (letzter Zugriff 15.09.2020).

[17] Vgl. *Knoph Vigsnæs* et al. (2017) [16], VG vom 9.10.2017, UNICEF: Clear violation of UN children's convention. International humanitarian organizations express strong reaction to Australia's undercover police operation, abrufbar unter https://www.vg.no/nyheter/utenriks/i/L8ly4/unicef-clear-violation-of-un-childrens-convention (letzter Zugriff 15.09.2020).

[18] Hierzu ausführlicher *Jagatic/Johnson/Jakobsson/Menczer* (2007) [13], Social phishing, in: Communications of the ACM 50(10) (2007), S. 64–100.

Zugangsdaten und Passwörter zu gelangen.[19] Beim Aufsetzen von Phishing-Webseiten wird jedoch nicht mithilfe von forensischer Software in ein informationstechnisches System i. S. v. § 100b Abs. 1 StPO *eingegriffen.* Vielmehr würden die Betroffenen durch eine technische Manipulation dazu gebracht werden, ihre Login-Informationen täuschungsbedingt an die ermittelnden Behörden weiterzuleiten. Für das Betreiben von Phishing-Webseiten kann § 100b Abs. 1 StPO daher nicht als Ermächtigungsgrundlage herangezogen werden. Ebenso wenig könnte das Abgreifen von Zugangsdaten und Passwörtern auf § 100 h Abs. 1 S. 1 Nr. 2 StPO gestützt werden, welcher die Verwendung technischer Mittel zu Observationszwecken regelt. Denn der Betrieb der beschriebenen Phishing-Webseiten würde gerade nicht der Lokalisierung oder Beobachtung der ausgespähten Personen dienen, sondern lediglich das Abgreifen ihrer Login-Informationen bezwecken, um diese im Anschluss für weitergehende Ermittlungen auf den Plattformen zu verwenden. Auch ein Rückgriff auf die Ermittlungsgeneralklausel aus §§ 161 Abs. 1 S. 2 i. V. m. 163 Abs. 1 S. 2 StPO könnte die ermittelnden Beamt*innen nicht pauschal zum Aufsetzen und Betreiben von Phishing-Webseiten ermächtigen. Ein solches Vorgehen würde in vielen Fällen auch Personen betreffen, gegen die kein Anfangsverdacht i. S. v. § 152 Abs. 2 StPO besteht. Wie etwa die 2016 vom Netz genommene Webseite „Deutschland im DeepWeb“ deutlich macht, werden einige der Webseiten, über die im Tor-Netzwerk Straftaten angebahnt und abgewickelt werden, nämlich auch als Treffpunkte für den anonymen Austausch über Nachrichten aus Politik und Wirtschaft, IT-Sicherheit und andere strafrechtlich irrelevante Themen genutzt.[20] Die Registrierung als Nutzer*in auf einer solchen Webseite ist daher allein nicht ausreichend, um einen Anfangsverdacht i. S. v. § 152 Abs. 2 StPO gegen sämtliche auf einer Plattform registrierten Personen zu begründen. Das pauschale Abgreifen von Login-Informationen über Phishing-Webseiten wäre nach geltender Rechtslage daher unzulässig.

2.3 Automatisierte Auswertung öffentlich zugänglichen Informationsquellen (Open Source Intelligence)

Neben dem Betrieb behördlicher Honeypot-Server und Phishing-Webseiten stellt die automatisierte Auswertung öffentlich zugänglicher Informationsquellen einen

[19] *Soiné* (2018) [32], NStZ 2018, 497 (502).

[20] Siehe hierzu auch die Ausführungen des LG Karlsruhe, Urteil vom 19.12.2018, 4 KLs 608 Js 19.580/17, Rn. 431 = StV 2019, 400 (402).

weiteren technischen Ermittlungsansatz dar, der zur Identifizierung tatverdächtiger Personen im Tor-Netzwerk beitragen könnte.

2.3.1 Technische Beschreibung

Zur Identifizierung von tatverdächtigen Personen im Tor-Netzwerk kann es zielführend sein, Informationen wie verwendete Account-Namen, E-Mail-Adressen oder öffentliche Forenbeiträge zusammenzutragen und diese Datensätze mit Hilfe spezieller Analysesoftware auszuwerten.[21] Im Rahmen dieses Verfahrens, das als Open Source Intelligence (kurz OSINT) bezeichnet wird, werden sämtliche Informations- und Datenquellen verwendet, die im Internet – also sowohl im Clear- als auch im Darknet – frei zugänglich sind und für deren Zugriff keine besondere Legitimation benötigt wird.[22] Auf diese Weise können detaillierte Bewegungs- und Persönlichkeitsprofile über gesuchte Personen erstellt werden, die Ansatzpunkte für weitergehende Ermittlungsmaßnahmen bieten. Unter Umständen lassen sich sogar eindeutige Verknüpfungen zwischen den verwendeten Online-Profilen und der tatsächlichen Identität der gesuchten Personen herstellen, wie es etwa im Falle des Betreibers der Handelsplattform „Silk Road" der Fall war.[23]

2.3.2 Rechtliche Einordnung

In welchen Grenzen hierzulande personenbezogene oder personenbeziehbare Daten aus dem Clear- und Darknet in strafprozessualen Ermittlungsverfahren erhoben und verarbeitet werden dürfen, ist eine in der strafrechtlichen Praxis relevante, rechtswissenschaftlich jedoch bislang nur spärlich diskutierte Frage.[24] Feststeht, dass für die automatisierte Sammlung und Auswertung von OSINT-Daten eine Ermächtigungsgrundlage erforderlich ist, da hierdurch in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG eingegriffen wird. Auch wenn dies auf den ersten Blick nahe liegt, kommt § 98a StPO (Rasterfahndung) als strafprozessuale Befugnisnorm für die Sammlung und Auswertung von OSINT-Daten allerdings nicht in Betracht.[25] Zwar ergibt sich eine gewisse „Verwandtschaft" zu § 98a StPO vor allem daraus, dass im Rahmen beider Verfahren

[21] Siehe hierzu bereits *Sinn* (2019) [30], Ermittlungen im Darknet, S. 148.

[22] Siehe hierzu *Day/Gibson/Ramwell* (2016) [8], Fusion of OSINT and non-OSINT data, in: Open Source Intelligence Investigation 2016, S. 133–152.

[23] Zu den Ermittlungen des FBI im Falle von „Silk Road" siehe *Tanriverdi* (2013) [26], Drogenhandel, Mordversuch – und den Klarnamen angegeben, Süddeutsche Zeitung vom 4.10.2013, abrufbar unter https://www.sueddeutsche.de/digital/mutmasslicher-betreiber-der-drogen-plattform-silk-road-drogenhandel-mordversuch-und-den-klarnamen-angegeben-1.1786870 (letzter Zugriff: 08.10.2020).

[24] Siehe hierzu *Rückert* (2017) [25], ZStW 2017, 302–333.

[25] *Rückert* (2017) [25], ZStW 2017, 302 (316).

verschiedene Datensätze zu Ermittlungszwecken maschinell miteinander abgeglichen werden.[26] Allerdings werden im Rahmen von § 98a StPO keine öffentlich zugänglichen Datensätze verwendet, während bei der Auswertung von OSINT-Daten ausschließlich auf Informationen zugegriffen wird, die von jedermann im Internet aufgerufen und eingesehen werden können. Obwohl auf die Ermittlungsgeneralklausel aus §§ 161 Abs. 1 S. 2 i. V. m. 163 Abs. 1 S. 2 StPO bloß geringfügige Grundrechtseingriffe gestützt werden können, ist diese daher grundsätzlich als Rechtsgrundlage für die automatisierte Auswertung von OSINT-Informationen in Betracht zu ziehen. Erwähnenswert ist in diesem Zusammenhang beispielsweise die von der niederländischen Forschungseinrichtung TNO entwickelte Analysesoftware „Dark Web Monitor", die seit Juli diesen Jahres durch die Zentralstelle Cybercrime Bayern (ZCB) in Bamberg getestet wird.[27]

2.4 Ausnutzen von Dokument-Exploits

Eine weitere Möglichkeit, um Personen im Tor-Netzwerk zu identifizieren, stellt das Ausnutzen von Dokument-Exploits dar. Lässt sich beispielsweise eine Datei im Microsoft-Word-Format mit einem unsichtbar eingebetteten Link präparieren, der beim Öffnen des Dokuments ohne Rückfrage an die betrachtende Person aufgerufen wird, so kann dieses Dokument als Angriffswerkzeug zur Deanonymisierung von Tor-Nutzer*innen eingesetzt werden.

2.4.1 Technischer Hintergrund

Im Rahmen strafrechtlicher Ermittlungsverfahren ist das Ausnutzen solcher Dokument-Exploits als „IP-Tracking" bekannt. Dabei stellen Ermittlungsbehörden Dateien über das Internet zum Abruf bereit, die mit einer Lesebestätigungsfunktion versehen sind.[28] Diese Lesebestätigungsfunktion besteht aus funktionslosen, transparenten Bildern oder anderen Dateieinbettungen.[29] Wird das präparierte Dokument geöffnet, werden die Dateieinbettungen von einem externen Server nachgeladen, ohne dass der dabei anfallende Datenverkehr von der Tor-Software anonymisiert wird. Die IP-Adresse des Internetanschlusses, von dem aus die Datei aufgerufen

[26] *Rückert* (2017) [25], ZStW 2017, 302 (316).

[27] Vgl. *Bayerisches Staatsministerium der Justiz,* Pressemitteilung vom 27.07.2020, Mehr Licht ins Darknet: Dark Web Monitor soll Strafverfolgungsbehörden bei Ermittlungen im Darknet verstärken, abrufbar unter https://www.justiz.bayern.de/presse-und-medien/pressemitteilungen/archiv/2020/69.php? (letzter Zugriff: 08.10.2020).

[28] Vgl. *Krause* (2016) [17], NStZ 2016, 139.

[29] Vgl. *Krause* (2016) [17], NStZ 2016, 139.

wurde, kann daher an den externen Server übertragen und schließlich an die Ermittlungsbehörden weitergeleitet werden. Typischerweise eignen sich für derartige Einbettungen Dokumentenformate wie Word oder PDF eher als reine Multimediaformate für Bild und Video wie JPG oder MP4. Aber auch für Multimediaformate beziehungsweise für Software, die zur Verarbeitung und Betrachtung von Bildern und Videos eingesetzt wird, sind in der Vergangenheit Schwachstellen bekannt geworden, die theoretisch zu Deanonymisierungszwecken ausgenutzt werden könnten.

2.4.2 Rechtliche Betrachtung

Aus rechtlicher Perspektive besteht Uneinigkeit darüber, ob das „IP-Tracking" zum Zwecke der Strafverfolgung als Verwendung eines sonstigen für Observationszwecke bestimmten technischen Mittels i. S. v. §100 h StPO[30] oder als Erhebung von Verkehrsdaten i. S. v. §100 g StPO[31] anzusehen ist. Dennoch bleibt festzuhalten, dass für ein entsprechendes Vorgehen bereits nach geltender Rechtslage eine ausreichende rechtliche Grundlage besteht, die in der Strafverfolgungspraxis vielseitige Ermittlungsansätze bietet. Beispielsweise hat der Bundestag im Januar 2020 der Verwendung künstlicher kinderpornografischer Dateien im Rahmen strafrechtlicher Ermittlungsverfahren zugestimmt.[32] Seither können Ermittlungsbeamt*innen computergenerierte Abbildungen verwenden, um sich Zugriff auf entsprechend gesicherte Webseiten im Tor-Netzwerk zu verschaffen.[33] Denkbar wäre es, diese computergenerierten Abbildungen mit entsprechenden Dokument-Exploits zu versehen, sodass die IP-Adressen derjenigen Personen, die auf die von den Ermittlungsbehörden hochgeladenen Dateien zugreifen, dokumentiert und als Anknüpfungspunkte für weitere Ermittlungsmaßnahmen genutzt werden können.

[30] So etwa *Krause* (2016) [17], NStZ 2016, 139 (144); *Bär* (2020) in: BeckOK-StPO [17], §100 g, Rn. 22; *Bruns* (2019) in: KK-StPO [14], §100 g, Rn. 20.

[31] So etwa der BGH-Ermittlungsrichter mit Beschl. v. 23.9.2014 - 1 BGs 210/14 = BeckRS 2015, 17557 (allerdings auf der Grundlage von §100 g aF.).

[32] Ausführlich zu den Neuregelungen der §184b Abs. 5 S. 2 StGB und §110d StPO siehe *Rückert/Goger* (2020) [23], MMR 2020, 373–378.

[33] Zum Phänomen der sogenannten „Keuschheitsproben" auf Online-Plattformen im Tor-Netzwerk siehe *Wittmer/Steinebach* (2019) [33], MMR 2019, 650–653.

2.5 Quellen-Telekommunikationsüberwachung und Online-Durchsuchung

Zudem kann eine Anonymisierung von Kommunikationsdaten im Tor-Netzwerk dadurch umgangen werden, dass die betreffenden Daten abgefangen werden, bevor sie verschlüsselt oder nachdem sie entschlüsselt wurden.

2.5.1 Technischer Hintergrund

Über das Tor-Netzwerk geroutete Datenpakete werden so verschlüsselt, dass jeder Tor-Knoten nur die Information erhält, von welchem Tor-Knoten die aktuellen Datenpakete gesendet wurden und an welchen Tor-Knoten die Datenpakete weitergeleitet werden müssen. Auf diese Weise wird der über das Tor-Netzwerk geleitete Datenverkehr anonymisiert. Dieser Effekt kann jedoch umgangen werden, wenn die Datenpake abgefangen und ausgewertet werden, bevor sie verschlüsselt oder nachdem sie entschlüsselt wurden. Aus technischer Sicht kann dies erreicht werden, indem auf den Rechnern der zu überwachenden Personen eine forensische Software installiert wird, die unbemerkt Bildschirmaufnahmen tätigt oder Tastatureingaben protokolliert.

2.5.2 Rechtliche Bewertung

Aus rechtlicher Perspektive ist es denkbar, ein solches Vorgehen auf die im Sommer 2017 neu in die StPO aufgenommenen Ermittlungsbefugnisse der §§ 100a, b StPO zu stützen. § 100a Abs. 1 S. 2 StPO (Quellen-Telekommunikationsüberwachung) ermächtigt Ermittlungsbehörden etwa dazu, in informationstechnische Systeme verdächtiger Personen einzugreifen, wenn dies notwendig ist, um die Überwachung und Aufzeichnung von telekommunikationsbezogenen Daten in unverschlüsselter Form zu ermöglichen. Unter den Voraussetzungen des § 100b StPO (Online-Durchsuchung) dürfen die Ermittler*innen darüber hinaus auch sonstige, nicht kommunikationsbezogene Daten der Betroffenen erheben. Insofern kann eine Umgehung der Anonymisierung von Kommunikationsdaten im Tor-Netzwerk bereits auf Grundlage der geltenden strafprozessualen Ermittlungsbefugnisse erreicht werden. Um die genannten Ermittlungsmaßnahmen einzuleiten, müssen den Behörden allerdings bereits diejenigen Personen bekannt sein, deren Geräte überwacht werden sollen. Daher ist weder die Quellen-Telekommunikationsüberwachung aus § 100a StPO, noch die Online-Durchsuchung aus § 100b StPO dazu geeignet, zu einer initialen Identifizierung von tatverdächtigen Personen im Tor-Netzwerk beizutragen. Dennoch können Ermittlungsbehörden durch Maßnahmen i.S.d. §§ 100a, b StPO Informationen erhalten, die eine Identifizierung weiterer tatverdächtiger Personen ermöglichen.

2.6 Monitoring von Datenpaketen

Ein gänzlich anderer Ermittlungsansatz, der eine initiale Identifizierung von Tor-Nutzer*innen ermöglichen könnte, ist das Monitoring von Datenpaketen. Dabei werden versandte Datenpakete überwacht und nachvollzogen, wie diese Pakete über das Netzwerk weitergeleitet werden. Stehen ausreichend viele Tor-Knoten unter der Kontrolle ein und derselben – beispielsweise staatlichen – Stelle, können die versendeten Datenpakete sodann anhand statistischer Analysen korreliert und unter Umständen sowohl deren Versender*innen als auch Empfänger*innen ausfindig gemacht werden.

2.6.1 Technische Beschreibung

Diese Angriffe werden in der Informatik als Korrelationsangriffe oder „Timing-Analysen" bezeichnet und sind ein bekanntes Problem im Tor-Netzwerk.[34] Allerdings kann durch ein solches Vorgehen nur in Erfahrung gebracht werden, welche Personen über Tor miteinander kommunizieren. Wird von den Beteiligten eine Ende-zu-Ende-Verschlüsselung eingesetzt, bleiben die Kommunikationsinhalte selbst wiederum geheim. Hinzu kommt, dass nur eine global agierende, äußerst einflussreiche Institution im Stande wäre, ausreichend viele Tor-Knoten zu betreiben, um solche Korrelationsangriffe erfolgreich umsetzen zu können. Nach derzeitigem Stand ist dies allerdings nicht der Fall. Selbst geheimdienstliche Allianzen wie die „Five Eyes" wären nur in der Lage, einen kleinen, zufälligen Teil der über das Tor-Netzwerk gerouteten Datenpakete zu überwachen.[35] Die NSA äußerte sich in den von Edward Snowden geleakten „Tor-Stinks"-Dokumenten sogar dahingehend, dass es in der Praxis wohl niemals möglich sein wird, alle Tor-Nutzer*innen im Rahmen von „Timing-Analysen" gleichzeitig überwachen zu können.[36]

2.6.2 Rechtliche Einordnung

Auch aus rechtlicher Perspektive wäre das Monitoring von Datenpaketen zu Strafverfolgungszwecken als unzulässig einzustufen. Dies liegt daran, dass in einer globalen Überwachung und Rückverfolgung von Datenpaketen bereits keine strafprozessuale Maßnahme gesehen werden kann. Voraussetzung für die Einleitung eines strafrechtlichen Ermittlungsverfahrens ist gem. §152 Abs. 2 StPO nämlich das

[34] Siehe hierzu etwa *Platzer/Schäfer/Steinebach* (2020) [22]), Critical traffic analysis on the tor network, in: Proceedings of the 15th International Conference on Availability, Reliability and Security 2020, S. 1–10.

[35] Siehe hierzu *Nurmi/Niemelä* (2017) [21], Tor de-anonymisation techniques. In: International Conference on Network and System Security, S. 657–671.

[36] Vgl. „Tor-Stinks" -Präsentation der NSA, abrufbar unter https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf (letzter Zugriff: 09.10.2020).

Vorliegen tatsächlicher Anhaltspunkte dafür, dass die von einer Ermittlungsmaßnahme betroffenen Personen eine verfolgbare Straftat begangen haben. In Anbetracht dessen, dass die Verwendung von Anonymisierungstechnologien wie der Tor-Software hierzulande ein grundrechtlich geschütztes Verhalten darstellt und zahlreichen positiven Verwendungszwecken dient, können die Nutzer*innen der Tor-Software jedoch nicht pauschal verdächtigt werden, das Tor-Netzwerk zur Anbahnung und Abwicklung von Straftaten zu nutzen.

2.7 Sonstige Ansätze

Neben den bisher aufgezeigten Ermittlungsmöglichkeiten existieren noch weitere Ansätze, die zur Identifizierung tatverdächtiger Personen im Tor-Netzwerk herangezogen werden können. Aus technischer Perspektive sind etwa Methoden des Forensic Hackings zu nennen. Hierunter ist eine Form des „ethical hackings" zu verstehen, das eng verwandt mit Strategien wie dem Penetration Testing ist.[37] Analog zu bekannten Hackingangriffen werden dabei Systemschwachstellen wie Implementierungs- oder Protokollfehler ausgenutzt, was dazu führen kann, dass eine Anonymisierung von IP-Adressen im Tor-Netzwerk scheitert. Hinzu kommen zahlreiche Ermittlungsansätze, die über keinen technischen Hintergrund verfügen und in diesem Beitrag daher nicht erwähnt wurden. Hierzu zählt beispielsweise der Einsatz von verdeckt ermittelnden Beamt*innen, die auf den Plattformen und Foren Testkäufe von illegalen Waren tätigen oder versuchen, verdächtige Personen im Rahmen angeblicher An- und Verkaufsgespräche zum Umstieg auf nicht-anonyme Kommunikationsmittel zu bewegen.[38]

3 Zusammenfassung

Eine anonyme Nutzung des Internets wird durch die Verwendung sogenannter „Darknet-Technologien" wie der Tor-Software ermöglicht und ist hierzulande grundrechtlich geschützt. Neben zahlreichen positiven Verwendungszwecken werden Anonymisierungstechnologien allerdings oft auch zur Begehung von Straftaten eingesetzt. Da ein Verbot von Darknet-Technologien jedoch sowohl aus technischer, als auch aus rechtlicher Sicht abzulehnen ist, wendet sich dieser Beitrag den Mög-

[37] Siehe hierzu *Simpson/Backman/Corley* (2020) [29], Hands-on ethical hacking and networkdefense.

[38] Siehe hierzu *Krause* (2018) [18], NJW 2018, 678–681.

lichkeiten der Strafverfolgung im Tor-Netzwerk zu. Es wurden Vorgehensweisen zur Identifizierung tatverdächtiger Personen im Tor-Netzwerk vorgestellt und aus rechtlicher Perspektive beurteilt, ob diese von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären. Das Betreiben behördlicher Honeypot-Server und Phishing-Webseiten zur Überwachung von Darknet-Plattformen wurde dabei als technisch möglich, aber in Deutschland rechtlich unzulässig eingestuft. Das Monitoring von Datenpaketen zu Strafverfolgungszwecken wurde sowohl aus technischen, als auch aus rechtlichen Gründen abgelehnt. Im Gegensatz dazu wurde der Einsatz von OSINT-Technologien zu Ermittlungszwecken als technisch möglich und rechtlich zulässig angesehen. Gleiches gilt hinsichtlich der Standortermittlung von verdächtigen Personen mittels „IP-Tracking". Zudem kann eine Verschleierung von IP-Adressen auch durch Ermittlungshandlungen wie der Quellen-Telekommunikationsüberwachung umgangen werden. Obwohl die Verwendung der Tor-Software strafrechtliche Ermittlungen erheblich erschwert, konnte gezeigt werden, dass technische Ermittlungsansätze existieren, die zur Deanonymisierung von tatverdächtigen Personen im Tor-Netzwerk herangezogen werden können. Die aufgezeigten Vorgehensweisen sollen als Diskussionsgrundlage für zukünftige Ermittlungshandlungen im Tor-Netzwerk dienen, ohne jedoch die Legitimität einer anonymen Nutzung des Internets grundsätzlich in Frage zu stellen.

Danksagung Das dieser Veröffentlichung zugrundeliegende Verbundprojekt „Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet" (PANDA) wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 13N14355 und 13N14356 gefördert. Die Verantwortung für den Inhalt dieses Beitrags liegt bei den Autor*innen.

Literatur

1. Bachmann, M., Arslan, N.: „Darknet"-Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber? S. 241–248. NZWiSt (2019)
2. Moritz, B., Moßbrucker, D., Rückert, C.,: Angriff auf die Anonymität im Internet, Reporter ohne Grenzen e.V., Berlin 2019. https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/20190630_Darknet_Paragraf_StN-Bartl-Mossbrucker-Rueckert.pdf. Zugegriffen: 31. Juli 2020
3. Graf, P. (Hrsg.): Beck'scher Online-Kommentar zur StPO mit RiStBV und MiStra, 37. Aufl. 1.7.2020 (zitiert: *Bearbeiter*in* in: BeckOK-StPO). Verlag C.H. Beck, München 2020
4. Böhm, M.: Ermittler zerschlagen zwei der größten Darknet-Marktplätze, Spiegel. https://www.spiegel.de/netzwelt/netzpolitik/darknet-ermittler-zerschlagen-grosse-marktplaetze-alphabay-und-hansa-a-1158933.html. Zugegriffen: 20. Juli 2017

5. Borchers, D.: Europäischer Polizeikongress: Weg mit dem Darknet, Heise. https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Weg-mit-dem-Darknet-4313276.html. Zugegriffen: 20. Febr. 2019
6. Bovermann, P.: Framing-Check: „Darknet", Süddeutsche Zeitung. www.sueddeutsche.de/kultur/framing-darknet-tor-anonym-internet-silk-road-1.436701. Zugegriffen: 3. Mai 2019
7. Ceffinato, T.: Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern. JuS 403–408 (2017)
8. Day, T., Gibson, H., Ramwell, S.: Fusion of OSINT and non-OSINT data. In: Open Source Intelligence Investigation , S. 133–152. Springer International Publishing, Basel (2016)
9. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. Naval Research Lab, Washington DC (2004)
10. Europol: Pressemitteilung vom 20.07.2017, Massive blow to criminal Dark Web activities after globally coordinated operation. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation. Zugegriffen: 20. Juli 2017
11. Fünfsinn, H., Ungefuk, G., Krause, B.: Das Darknet aus Sicht der Strafverfolgungsbehörden. Kriminalistik **7**, 440–445 (2017)
12. Greco, L.: Strafbarkeit des Unterhaltens einer Handels- und Diskussionsplattform insbesondere im sog. Darknet ZIS 2019, 434–450 (2019)
13. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Communications of the ACM 50(10), 64–100 (2007)
14. Hannich, R. (Hrsg.): Karlsruher Kommentar zur StPO, 8. Aufl. (zitiert: *Bearbeiter*in* in: KK-StPO). C. H. Beck, München (2019)
15. Kersten, J.: Anonymität in der liberalen Demokratie. JuS 193–203 (2017)
16. Knoph Vigsnæs, M., Høydal, H.F., Einar, O.S., Remøe Hansen, N.: VG , UNICEF: Clear violation of UN children's convention. International humanitarian organizations express strong reaction to Australia's undercover police operation, abrufbar unter. https://www.vg.no/nyheter/utenriks/i/L8ly4/unicef-clear-violation-of-un-childrens-convention. Zugegriffen: 9. Okt. 2017
17. Krause, B.: IP-Tracking durch Ermittlungsbehörden: Ein Fall für §100g StPO?–Zugleich Besprechung des BGH-Beschl. v. 23. Sept. 2014–1 BGs 210/14, S. 139–144, NStZ (2016)
18. Krause, B.: Ermittlungen im Darknet – Mythos und Realität. NJW 678–681. C. H. Beck, München (2018)
19. Locker, T., Hoppenstedt, M.: Jagd auf 'Elysium': Das Ende der größten deutschen Kinderporno-Plattform, VICE. https://www.vice.com/de/article/panv87/jagd-auf-elysium-das-ende-der-grossten-deutschen-kinderporno-plattform Zugegriffen: 7 März 2019
20. Moore, C.: Detecting ransomware with honeypot techniques. In: Cybersecurity and Cyberforensics Conference (CCC), S. 77–81, IEEE (2016)
21. Nurmi, J., Niemelä, M.S.: Tor de-anonymisation techniques. In: International Conference on Network and System Security, S. 657–671. Springer International. Basel (2017)
22. Platzer, F., Schäfer, M., Steinebach, M.: Critical traffic analysis on the tor network. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, S. 1–10 (2020)

23. Rückert, C., Goger, T.: Neue Waffe im Kampf gegen Kinderpornografie im Darknet. MMR 373–378 (2020)
24. Rückert, C.: Blick in eine Schattenwelt. Schaden und Nutzen des „anonymen" Internets, Politische Studien 479/2018, S. 12–21, abrufbar unter https://www.hss.de/download/publications/PS_479_Digitale_Revolution_03.pdf
25. Rückert, C.: Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, S. 302–333, ZStW (2017)
26. Tanriverdi, H.: Drogenhandel, Mordversuch–und den Klarnamen angegeben, Süddeutsche Zeitung, abrufbar unter www.sueddeutsche.de/digital/mutmasslicher-betreiber-der-drogen-plattform-silk-road-drogenhandel-mordversuch-und-den-klarnamen-angegeben-1.1786870. Zugegriffen: 4. Okt. 2013
27. Safferling, C., Rückert, C.: Das Strafrecht und die Underground Economy. In: Konrad-Adenauer-Stiftung e.V. (Hrsg.), Analysen & Argumente, Ausgabe 291, abrufbar unter https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_51506_1.pdf/5f5a7ec0-2bb8-6100-6d65-b3ba55564d72?version=1.0&t=1539647924448. Zugegriffen: Febr. 2018
28. Schulz, B.: Australiens Polizei betrieb riesige Kinderporno-Plattform, Spiegel, abrufbar unter http://www.spiegel.de/panorama/justiz/australien-polizei-ermitteltemit-eigener-kinderporno-plattform-a-1172503.html. Zugegriffen: 11. Okt. 2017
29. Simpson, M.T., Backman, K., Corley, J.: Hands-on Ethical Hacking and Network Defense. Cengage Learning. Course Technology, Boston, MA (2010)
30. Sinn, A.: Ermittlungen im Darknet. In: Gest, G.M., Sinn, A. (Hrsg.) Organisierte Kriminalität und Terrorismus im Rechtsvergleich, Schriften des Zentrums für europäische und internationale Strafrechtsstudien, Bd. 10, S. 141–159. V&R Unipress, Universitätsverlag Osnabrück (2019)
31. Snowden, E.: „Tor Stinks"-Präsentation der National Security Agency of the United States of America. https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf
32. Soiné, M.: Die strafprozessuale Online-Durchsuchung. NStZ 497–504 (2018)
33. Wittmer, S., Steinebach, M.: Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet. Rechtliche Rahmenbedingungen und technische Umsetzbarkeit, MMR 650–653 (2019)