/// Schaden und Nutzen des „anonymen“ Internets

DAS DARKNET: BLICK IN EINE SCHATTENWELT

CHRISTIAN RÜCKERT /// Über das „dunkle Netz“ kursieren zahlreiche Mythen und Gerüchte. Von den einen wird es als Plattform für kriminelle Machenschaften verteufelt, von den anderen als wichtiges Werkzeug im Kampf um die Meinungs- und Pressefreiheit gelobt.

Die Entmystifizierung des „dunklen Internets“

Darknet. Bereits der Name impliziert dunkle Machenschaften, Schattenwirtschaft, das „Böse“ im Netz. Über keinen Teil des Internets kursieren mehr Gerüchte und Mythen und kaum ein Teil bekommt derzeit mehr mediale Aufmerksamkeit. Der Begriff des Darknets findet sich längst nicht mehr nur in wissenschaftlichen Abhandlungen sowie Blogs und Foren der IT-Nerds. Er ist in der überregionalen Tagespresse, auf politischen Diskussionsveranstaltungen und im öffentlich-rechtlichen Fernsehen angekommen. Sogar eine Tatort-Episode beschäftigte sich mit dem „dunklen Teil“ des Internets. Aus Perspektive der Strafverfolgungsbehörden wird das Darknet als neue Herausforderung in ihrem Kampf gegen die Kriminalität betrachtet. Auf den dort existierenden Schwarzmärkten werden Drogen, Waffen und Kreditkartendaten gehandelt und kinderpornografisches Material getauscht. Die Verschleierung der IP-Adressen durch die Darknet-Technologie erschwert die Ermittlung der Tatverdächtigen.

Freiheitsaktivisten und Journalisten preisen das Darknet dagegen als wichtiges Werkzeug im Kampf gegen autokratische Systeme und für die Meinungs-, Informations- und Pressefreiheit. Doch was ist eigentlich dieses Darknet? Wie funktioniert es? Ist seine Nutzung verboten? Wie sollte die Gesellschaft mit dem neuen Phänomen des Schwarzmarkthandels im Darknet umgehen? Der folgende Beitrag soll Antworten auf diese Fragen geben und die „dunkle Seite“ des Internets ans Tageslicht holen und entmystifizieren.

Um das Darknet bestehen viele **MYTHEN.**

Mit wenigen Klicks in eine dunkle und geheimnisvolle Schattenwelt– was verbirgt sich wirklich im Darknet?

Was ist eigentlich das Darknet?

Um Schaden und Nutzen des Darknets einordnen zu können, muss man zunächst dessen grundlegende Funktionsweise verstehen. Unter dem Begriff versteht man einen besonderen Teil der Internetinfrastruktur. Grob lässt sich das Internet in drei Teile gliedern:[1]

Surface Web

Hierunter sind alle Inhalte im Internet zu verstehen, die durch die Nutzung von Standard-Suchmaschinen gefunden und durch einen Klick auf das Suchergebnis direkt aufgerufen werden können.

Deep Web

Dieses liegt unter dem Surface Web und darunter versteht man Inhalte, die nicht direkt über eine Suchmaschine gefunden und aufgerufen werden können. Hierzu zählen Bezahlinhalte wie z. B. kommerzielle Datenbanksysteme oder Videostreaming-Dienste oder Foren und Seiten sozialer Netzwerke, auf die man erst nach Registrierung und Anmeldung zugreifen kann.

Darknet

Das Darknet ist ein Teil des Deep Webs mit zwei besonderen Eigenschaften. Die Inhalte sind nur aufrufbar, wenn der Nutzer einen besonderen Browser verwendet, der die IP-Adresse des Nutzers verschleiert. Zudem verwenden auch die Betreiber der Darknet-Seiten eine spezielle Software, welche die IP-Adresse und damit den Serverstandort verbirgt.

Die Verschleierungs- und Verschlüsselungstechnologie, die sich (überwiegend) hinter dem Begriff Darknets verbirgt, ist das Tor-Netzwerk. Dieses besteht im Wesentlichen aus drei Elementen:[2]

Tor-Knoten

Tor-Knoten sind Rechner, die freiwillig von Nutzern für die anderen Tor-Nutzer zur Verfügung gestellt werden. Die Knoten dienen im Netzwerk als Relais-Stationen, an denen der Datenverkehr über

Netzwerkverbindungen zu beliebigen anderen Knoten umgeleitet werden kann.

Tor-Browser

Der Tor-Browser ist ein Internet-Browser und erfüllt zunächst alle Funktionen, die auch ein „normaler" Browser anbietet. Das heißt, man kann mit dem Tor-Browser auch „normal" im Surface Web surfen. Zusätzlich hat der Tor-Browser bereits einige Sicherheitsfunktionen vorinstalliert. Die Besonderheit ist jedoch die Verschleierung der IP-Adresse des Nutzers.

Der Tor-Browser verhindert, dass der Server des Internetdienstanbieters die IP-Adresse des Internetnutzers kennt. Zu diesem Zweck leitet der Tor-Browser die vom Rechner des Nutzers verschickten Daten über insgesamt drei Tor-Knoten (siehe zuvor) um. Der Rechner verbindet sich mit dem ersten Knoten (Entry-Node). Dieser schickt die Daten weiter an den zweiten Knoten (Middle-Node) und dieser leitet die Daten an den letzten Tor-Knoten (Exit-Node). Der Exit-Node verbindet sich schließlich mit dem Server des Dienstanbieters. Der Server des Dienstanbieters kennt somit nur die IP-Adresse des Exit-Nodes.

Als zusätzliche Sicherungsmaßnahme sorgt der Tor-Browser dafür, dass kein Tor-Knoten den gesamten Weg der Daten zurückverfolgen kann. Hierfür verschlüsselt er die versendeten Daten dreifach. Jeder beteiligte Knoten bekommt vom Tor-Browser nur den Schlüssel für eine einzige Schicht mitgeteilt. Entschlüsselt nun der Entry-Node die erste Verschlüsselungsschicht, erhält er nur die Information, an welchen Middle-Node er die Daten weitersenden soll. Der Middle-Node kann die zweite Schicht entschlüsseln und erfährt lediglich, welcher Exit-Node das nächste Ziel ist. Dieser entfernt mit seinem Schlüssel

EXKURS ZUR IP-ADRESSE:[3]

Die IP-Adresse ist eine Art Telefonnummer für Geräte, die über das Internet Daten verschicken. Sie wird vom Internetanbieter automatisch vergeben, wenn der Nutzer seinen Router mit dem Internet verbindet. Die IP-Adresse dient bei einer Kommunikation über das Internet, z. B. beim Versenden einer E-Mail, zur Adressierung der versendeten Daten und ist somit dem Rechner des Empfängers bekannt. Vereinfacht gesagt „spricht" der Rechner des Internetnutzers beim Aufrufen einer Homepage mit dem Server des Homepagebetreibers. Bei dieser Kommunikation kennen beide Beteiligte gegenseitig die IP-Adresse. Der jeweilige Internetanbieter weiß, welchem Router er welche IP-Adresse zu welchem Zeitpunkt zugeordnet hat und kann anhand seiner Kundenbestandsdaten bestimmen, wo sich der jeweilige Router und damit auch der Rechner bzw. Server befindet. Deshalb sollen die Internetanbieter durch das Gesetz zur Vorratsdatenspeicherung verpflichtet werden, u. a. die IP-Adressen ihrer Kunden über einen bestimmten Zeitraum zu speichern. Wenn Strafverfolgungsbehörden nun „verdächtige" IP-Adressen gefunden haben, z. B durch die Beschlagnahme eines Servers mit illegalen Inhalten, können sie die gefundenen IP-Adressen der Nutzer von den Internetanbietern mit den dort gespeicherten Adressen abgleichen lassen (Verkehrsdatenabfrage). So können die genauen Standorte der Rechner ermittelt werden, mit denen illegale Inhalte abgerufen wurden.

Mit dem **TOR-BROWSER** ist die IP-Adresse des Internetznutzers nicht mehr nachvollziehbar.

die letzte Schicht und erfährt, an welchen Dienstanbieter er die Daten versenden soll. Diese letzte Verbindung wird zumindest dann verschlüsselt, wenn die Homepage des Dienstanbieters eine https-Verbindung anbietet.

Um den Weg der Daten nachzuvollziehen müsste ein Angreifer somit alle drei Tor-Knoten kontrollieren. Um die Wahrscheinlichkeit zu verringern, dass alle drei genutzten Knoten unter der Kontrolle eines Angreifers stehen, wechselt der Tor-Browser ca. alle 10 Minuten die genutzten Tor-Knoten. Auch ein Angreifer, der „an der Leitung" lauscht, könnte jeweils nur die an der belauschten Datensendung beteiligten Knoten identifizieren und nicht den ganzen Weg nachvollziehen. Dementsprechend können die Strafverfolgungsbehörden die IP-Adresse des Nutzers weder über eine Sicherstellung des Servers des Dienstanbieters noch durch eine Kontrolle einzelner Tor-Knoten oder eine klassische Telekommunikationsüberwachung „in der Leitung" ermitteln.

Hidden Services im Tor-Netzwerk

Der Tor-Browser schützt somit zwar die Identität des Nutzers, nicht jedoch die des Dienstanbieters. Der Rechner des Nutzers kennt dessen IP-Adresse. Allerdings bietet Tor auch für die Dienstanbieter eine Möglichkeit, ihre IP-Adresse zu verschleiern. Hierzu können diese einen Hidden Service betreiben. Da der Dienst für die Nutzer auffindbar und erreichbar sein muss, erfordert dies jedoch mehr technische Finesse. Stark vereinfacht kann man sich das Betreiben eines Hidden Services wie in einem Agentenfilm mit toten Briefkästen, geheimen Botschaften und versteckten Treffpunkten vorstellen. Der Dienstanbieter bestimmt einige Tor-Knoten als tote Briefkästen (Introduction Points). Zu diesen baut er

EXKURS ZUR ASYMMETRISCHEN VERSCHLÜSSELUNG:[4]

Der öffentliche Schlüssel ist Teil eines Schlüsselpaares, das bei der Methode der asymmetrischen Verschlüsselung zum Einsatz kommt. Man kann sich diese Methode am ehesten als Schatztruhe mit zwei verschiedenen Schlüsseln vorstellen. Der öffentliche Schlüssel kann die Truhe absperren, der private Schlüssel schließt die Truhe wieder auf. Wenn man also eine Nachricht in die Truhe legt und die Truhe mit dem öffentlichen Schlüssel abschließt (= Verschlüsselung der Nachricht), kann nur der Inhaber des privaten Schlüssels die Truhe aufsperren (= Entschlüsselung der Nachricht) und die Nachricht lesen. Den privaten Schlüssel hält der Inhaber der Schlüssel geheim, den öffentlichen Schlüssel teilt er anderen Personen mit, damit diese Nachrichten verschlüsseln können, die nur er selbst entschlüsseln und lesen kann. So können Daten und Nachrichten verschlüsselt werden, ohne dass ein gemeinsamer Schlüssel ausgetauscht werden muss. Der Austausch eines gemeinsamen Schlüssels birgt nämlich das Risiko, dass ein Angreifer den Austausch abfängt und damit die Nachrichten entschlüsseln kann.

eine Tor-Verbindung auf (also über drei Tor-Knotenpunkte, wie dargestellt) und weist sie an, ankommende Anfragen an ihn weiterzuleiten. Die Adressen der toten Briefkästen legt er gemeinsam mit seinem öffentlichen Schlüssel auf einem Verzeichnisserver ab.

Mit Hidden Services kam auch der **DIENSTANBIETER** verschleiert werden.

Ein Nutzer, der den Hidden Service kontaktieren möchte, sucht sich den öffentlichen Schlüssel und die Adressen der toten Briefkästen auf dem Verzeichnisserver. Dies erledigt der Tor-Browser von selbst, wenn der Nutzer die .onion-Adresse des Hidden Services kennt. Dabei handelt es sich um die Adresse, die in die Adresszeile des Tor-Browsers eingegeben werden muss, um den Hidden Service zu erreichen. Da sich das Darknet im Deep Web befindet, können die .onion-Adressen grundsätzlich nicht durch Suchmaschinen gefunden werden. Allerdings existieren Verzeichnisse wie z. B. das Hidden Wiki oder das Undernet Directory, welche .onion-Adressen bereithalten. Der Tor-Browser des Nutzers kontaktiert dann einen der toten Briefkästen und legt dort eine geheime Botschaft ab, die er mit dem öffentlichen Schlüssel des Hidden Services verschlüsselt (wir erinnern uns: somit kann nur noch der Inhaber des privaten Schlüssels, also der Inhaber des Hidden Services die geheime Botschaft entschlüsseln).

Die Botschaft enthält die Adresse eines vom Nutzer gewählten geheimen Treffpunkts (= Tor-Knoten, Rendezvous-Point) im Tor-Netzwerk und eine geheime Passphrase. Der tote Briefkasten teilt dem Hidden Service (über eine Tor-Verbindung) mit, dass eine Botschaft für ihn bereit liegt. Der Hidden Service holt sich die Nachricht, entschlüsselt sie, entnimmt die geheime Passphrase und legt diese auf dem geheimen Treffpunkt im Tor-Netzwerk ab. Der geheime Treffpunkt informiert schließlich den Nutzer darüber, dass die Kommunikation mit dem Hidden Service beginnen kann.

Anhand der abgelegten geheimen Passphrase kann der Nutzer prüfen, ob er wirklich mit dem Hidden Service spricht. Die Kommunikation läuft nun vermittelt durch den Treffpunkt-Knoten jeweils über Tor-Verbindungen zu Nutzer und Server. Da der Nutzer nur eine Tor-Verbindung zum geheimen Treffpunktsknoten aufbaut, kennt er nun auch nicht mehr die IP-Adresse des Servers des Dienstanbieters. Weil auch alle anderen Verbindungen des Hidden Services (zu den toten Briefkästen und zum Verzeichnisserver) über eine Tor-Verbindung laufen, kennt auch keiner der anderen beteiligten Punkte die Identität des Servers. So bleibt auch die Identität des Dienstanbieters verschleiert.

Darknet: Darf man das und brauchen wir das?

Viele Menschen assoziieren mit Maßnahmen zur Verdeckung der eigenen Identität Geheimagenten, Paranoiker und Kriminelle. Deshalb wird oft die Frage aufgeworfen, ob bereits die Nutzung des Darknets strafbar sei. Die Antwort lautet (noch): Nein! Es existieren (in Deutschland) keine Vorschriften, die

den Gebrauch des Tor-Netzwerks verbieten würden. Man kann sogar noch einen Schritt weitergehen. Die Nutzung des Tor-Netzwerks ist durch die Grundrechte in unserer Verfassung geschützt. Die Telekommunikationsfreiheit nach Art. 10 des Grundgesetzes (GG) schützt jede Form der individuellen Kommunikation, wozu auch das Versenden von E-Mails, Messenger-Nachrichten, Internetchats und das Aufrufen von Webseiten zählen, vor der Kenntnisnahme durch staatliche Behörden. Geschützt ist dabei nach der Rechtsprechung des Bundesverfassungsgerichts nicht nur der Inhalt, sondern auch die Umstände der Kommunikation, also z. B., wer mit wem, wann und über welche Kommunikationsart kommuniziert hat.[5] Daneben werden personenbezogene Daten ganz allgemein durch das Recht auf informationelle Selbstbestimmung (abgeleitet aus Art. 2 Abs. 1, 1 Abs. 1 GG) geschützt. Teil dieses Rechts ist es, selbst darüber zu bestimmen, was mit den eigenen personenbezogenen Daten geschieht und wer von ihnen Kenntnis nimmt bzw. hat. Der Einzelne kann auch entscheiden, ganz oder zum Teil anonym zu bleiben.[6] Demnach ist die Nutzung des Tor-Netzwerks nur die Ausübung grundgesetzlich garantierter Freiheiten.

Auch über das schlichte (und berechtigte) Interesse am Schutz der eigenen Identität hinaus kann es gute Gründe geben, seinen Standort und seine Identität im Internet zu verschleiern.[7] Dies gilt zuvorderst für die Arbeit von Menschenrechtsaktivisten und Journalisten in autokratischen Systemen. Durch die Verschleierung des eigenen Standorts bei der Kommunikation untereinander und mit Dritten sowie bei der Veröffentlichung von Material im Internet wird es den Machthabern in solchen Systemen erschwert, die Aktivisten und Journalisten zu verfolgen. Auch die Sperrung bestimmter Internetdienste durch Länder wie China kann durch das Angebot der Dienste im Darknet umgangen werden. Gleichsam sind Journalisten weltweit für ihre Arbeit darauf angewiesen, ihren Quellen und Informanten – nicht zuletzt Whistleblowern – Vertraulichkeit garantieren zu können. Hierfür ist u. a. die Möglichkeit einer anonymen Kommunikation ein wichtiger Baustein. Und schließlich können Internetnutzer durch die Verschleierung ihres Standorts der Datensammelwut internationaler (Internet-) Konzerne zumindest ein kleines Bollwerk entgegensetzen.

Die Nutzung des Tor-Netzwerks zur Wahrung der **ANONYMITÄT** ist nicht strafbar.

Missbrauch des Darknets durch Kriminelle

Selbstredend ist aber auch das Missbrauchspotenzial der Tor-Technologie riesig.[8] Die Möglichkeit, anonym im Internet zu surfen und anonym Dienstleistungen anzubieten, ist besonders für Kriminelle attraktiv. Deshalb hat sich eine stetig wachsende Schattenwirtschaft im Darknet etabliert (Underground Economy). Auf hochprofessionell organisierten Marktplätzen, die in ihrer Struktur den bekannten Marktplätzen im Surface Web wie z. B. Amazon, eBay etc. ähneln, bieten Verkäufer alle Arten illegaler Güter feil. Der

Schwerpunkt liegt auf dem Vertrieb von Betäubungsmitteln. Mittlerweile spielt sich ein Großteil des Drogenhandels zwischen Verkäufer und Konsument (der „Großhandel" zwischen Lieferant und Verkäufer scheint derzeit noch nicht in großem Stil im Darknet abgewickelt zu werden) auf den Handelsplätzen des Darknets ab. Große praktische Bedeutsamkeit haben daneben der Handel mit Daten, z. B. Kreditkarten, und der Austausch von kinder- und jugendpornografischem Material. Dazu kommen Waffenhandel, das Angebot krimineller Dienstleistungen wie z. B. Vermietung von Botnetzen für DDoS-Attacken, und Auftragsmord (in Deutschland ist aber noch kein Fall bekannt geworden, in dem es tatsächlich zur Ausführung eines im Darknet beauftragten Tötungsdelikts gekommen ist). Quantitativ betrachtet kann man wohl davon ausgehen, dass über die Hälfte aller Angebote, die als Hidden Service betrieben werden, kriminellen Zwecken dient.[9]

Die strafrechtliche Verfolgung der Händler und Administratoren der Darknet-Marktplätze ist dabei schwierig. Aufgrund der Verschleierung der IP-Adressen kommen die Ermittler mit einer Abfrage der Verkehrsdaten bei Internetanbietern nicht weiter. Die Vorratsdatenspeicherung schafft hier somit auch keine Abhilfe. Mangels Kenntnis der Serverstandorte können diese auch nicht beschlagnahmt und ausgewertet werden. Auskunftsanfragen der Strafverfolgungsbehörden werden die Marktplatzbetreiber wohl nicht beantworten. Schließlich ist eine Telekommunikationsüberwachung wegen der Verschlüsselung der Datenübertragung im Tor-Netzwerk nicht erfolgversprechend. Moderne Maßnahmen wie das IP-Tracking mittels Lesebestätigungen oder Anhängen in E-Mails sowie das „Unterschieben" eines staatlichen Spähprogramms sind oftmals ebenfalls nur schwierig durchführbar.[10]

Die **ANONYMISIERUNGSTECHNOLOGIE** im Darknet erschwert die Verfolgung krimineller Handlungen.

Weiter erschwert werden die Ermittlungen dadurch, dass die Underground Economy virtuelle Kryptowährungen wie Bitcoin und Monero als Zahlungsmittel verwendet. In diesen Systemen erstellen und verwalten die Nutzer ihre „Konten" selbst. Es gibt keine zentralen Verwaltungseinheiten und die Strafverfolgungsbehörden können daher keine Auskünfte über die Nutzer bei Finanzinstituten erlangen. Ermittlungen sind zwar in der Blockchain (gemeinsames „Kontobuch" aller Nutzer) möglich, jedoch sind die Daten dort pseudonymisiert, sodass eine Identifizierung der Nutzer sehr schwierig ist.[11]

Erfolgversprechend erscheint derzeit vor allem „klassische" Polizeiarbeit wie z. B. verdeckte Ermittlungen und Scheinkäufe auf Handelsplattformen und Ermittlungen an den Schnittstellen zur Realwelt, z. B. die Überwachung von Postpackstationen, an welche die Betäubungsmittel geliefert werden.[12] Schließlich agieren die Täter der Underground Economy über Landesgrenzen hinweg. Oftmals müssen Ermittlungen deshalb international geführt werden, durch Rechtshilfeersuchen an ausländische

Staaten, gemeinsame Ermittlungsgruppen oder – im europäischen Rechtsraum – mit Unterstützung von Europol und anderen Formen der polizeilichen und justiziellen Zusammenarbeit in der EU.

Wie sollte unsere Gesellschaft reagieren?

Der Befund für das Darknet lautet also: Es ist krank, aber nicht alles davon ist befallen. Wie soll unsere Gesellschaft und unser Staat hierauf reagieren? Angesichts des Ausmaßes der Nutzung des Darknets zur Begehung von Straftaten und den Herausforderungen, vor denen Polizei und Justiz stehen, wird sicherlich über ein Verbot seiner Nutzung und gegebenenfalls auch der virtuellen Kryptowährungen diskutiert werden. Abgesehen davon, dass die Durchsetzung eines solchen Verbots aber faktisch unmöglich ist, wäre es wohl auch verfassungsrechtlich gar nicht möglich. Die Nutzung des Darknets ist grundrechtlich geschützt und wird überdies auch für den Schutz grundgesetzlich garantierter Freiheiten eingesetzt. Somit wäre ein Totalverbot sicherlich nicht mit dem Verhältnismäßigkeitsprinzip des Grundgesetzes vereinbar. Weiterhin bedeutet ein pauschales Verbot moderner und weltweit genutzter Technologie auch ein Hemmnis für die technischen Innovationsmöglichkeiten des Wirtschaftsstandorts Deutschland. Und schließlich wäre auch das (außen-)politische Signal eher ungünstig. Das pauschale Verbot von Anonymisierungstechnologie steht einem freiheitlich-demokratischen Rechtsstaat nicht gut zu Gesicht.

Der Koalitionsvertrag zwischen CDU/CSU und SPD enthält die Erwägung, einen neuen Straftatbestand zu schaffen, der den Betrieb von Hidden Services zur Ermöglichung der Begehung von Straftaten durch die Nutzer eigenständig kriminalisieren soll.[13] Ob dieser allerdings wirklich notwendig ist, ist fraglich, da bereits durch die bestehenden Strafnormen ein entsprechendes Verhalten weitestgehend erfasst ist und eine weitere Ausdehnung der Vorfeldkriminalisierung bedenklich erscheint.[14] Außerdem darf nicht übersehen werden, dass einige Darknet-Plattformen, vor allem Foren, auch dem freien Austausch von Meinungen und damit der Verwirklichung von Art. 5 Abs. 1 GG dienen. Hier wären also „Kollateralschäden“ für die Meinungs- und Informationsfreiheit zu befürchten. Dies sollte im anstehenden Gesetzgebungsverfahren vermieden werden.

Wie also dann reagieren? So, wie es bereits geschieht: mit personeller und technischer Aufrüstung von Polizei und Justiz sowie mit Fortbildung und Forschung zum Darknet und den virtuellen Kryptowährungssystemen. Die (universitäre) Forschung sollte effektive technische Lösungsansätze für Ermittlungen im Darknet und in virtuellen Kryptowährungssystemen entwickeln, welche gleichzeitig die Grund- und Menschenrechte hinreichend wahren. Die Polizei- und Justizbehörden benötigen spezialisiertes Personal, eine technische Ausstattung, die annähernde „Waffengleichheit“ mit den Cyber-Kriminellen

Zur **BEKÄMPFUNG** bedarf es personeller und technischer Maßnahmen.

ermöglicht und Fortbildungen für Polizisten, Staatsanwälte und Richter. Bayern hat wie andere Bundesländer und der Bund auch hier mit der Einrichtung der Zentralstelle Cybercrime Bayern an der Generalstaatsanwaltschaft Bamberg sowie spezialisierten Einheiten bei den Polizeiinspektionen und dem Landeskriminalamt bereits die ersten Schritte unternommen. Um jedoch die notwendigen Fachkräfte zu gewinnen, sollte das Tarifsystem für den öffentlichen Dienst, zumindest partiell, flexibilisiert werden, um mit den Angeboten aus der Wirtschaft besser konkurrieren zu können. Rechtspolitisch muss über die Erforderlichkeit und Art der Umsetzung von Reformen an Strafgesetzbuch und Strafprozessordnung zur Reaktion auf die digitale Revolution diskutiert werden. Auf der Ebene der Justizministerkonferenz (mit den Justizministern des Bundes und der Länder) geschieht dies unter Einbeziehung von Expertenwissen bereits.

Die internationale **ZUSAMMENARBEIT** muss noch weiter verbessert werden.

Zur Bekämpfung der grenzüberschreitenden Kriminalität muss die internationale Zusammenarbeit noch weiter verbessert werden. Es gibt zwar mit der polizeilichen und justiziellen Zusammenarbeit in Europa, mit gemeinsamen Ermittlungsgruppen und mit den Regeln über erleichterte Rechtshilfeverfahren in der Cybercrime Convention bereits einige Instrumente, aber diese reichen noch nicht aus. Dem grenzüberschreitenden Zugriff auf Datenbestände durch Strafverfolgungsbehörden steht oftmals das Territorialitätsprinzip entgegen.[15] Dies kann angesichts der Fortentwicklung des Cloud-Computings strafrechtliche Ermittlungen (nicht nur) im Darknet erheblich behindern. Hier müssen vor allem zwei Lösungsansätze diskutiert werden: Die Überarbeitung bestehender und der Abschluss neuer völkerrechtlicher Abkommen, die den grenzüberschreitenden Zugriff regeln und eine Reformierung des Territorialitätsprinzips bezüglich des Standorts von Datenbeständen. Die ausschließliche Anknüpfung an den physischen Speicherort entspricht nicht mehr der technischen Realität, in der Datenbestände in Sekundenschnelle weltweit „umgezogen" werden und Dateien sogar aufgespalten und an verschiedenen Standorten gespeichert werden.[16] ///

/// DR. CHRISTIAN RÜCKERT

ist Akademischer Rat a. Z. am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht, Friedrich-Alexander-Universität Erlangen Nürnberg.

Anmerkungen

[1] Grundlegend dazu Bergman, Michael: White Paper: The Deep Web: Surfacing Hidden Value, JEP 2001, Band 7, Heft 1.

[2] Die Darstellung ist aus Verständlichkeitsgründen vereinfacht; Details über die Funktionsweise bei https://www.torproject.org/about/overview.html.en, Stand: 12.3.2018.

[3] Ebenfalls aus Verständlichkeitsgründen stark vereinfacht; einen guten Überblick geben Kirchberg-Lennartz, Barbara / Weber, Jürgen: Ist die IP-Adresse ein personenbezogenes Datum? DuD 2010, S. 479-481.

[4] Für die genaue Funktionsweise siehe Lapp, Thomas, in: Handbuch IT- und Datenschutzrecht, hrsg. von Astrid Auer-Reinsdorff und Isabell Conrad, § 30 Rn 48 ff., München, 2. Aufl., 2016.

[5] Ständige Rechtsprechung vgl. BVerfGE 125, 260 (309).

[6] Einen guten Überblick geben Murswiek, Dietrich / Rixen, Stephan: Grundgesetz, hrsg. von Michael Sachs, Art. 2 Rn 72 ff., München, 8. Aufl., 2018; BGH, NJW 2017, 2416.

[7] Detailliert zum Folgenden Moßbrucker, Daniel: Netz der Dissidenten, in: APuZ 46-47/2017, S. 16-22.

[8] Ausführlich zur Kriminalität im Darknet und deren Verfolgung: Safferling, Christoph / Rückert, Christian: Das Strafrecht und die Underground Economy, in: Analysen & Argumente 291, hrsg. von der Konrad-Adenauer-Stiftung; Krause, Benjamin: Ermittlungen im Darknet, in: NJW 2018, S. 678-681.

[9] Vgl. Krause: Ermittlungen im Darknet, S. 678 ff. (m.w.N.).

[10] Vgl. Krause, Benjamin: IP-Tracking durch Ermittlungsbehörden: Ein Fall für § 100g StPO?, in: NStZ 2016, S. 139-144 (zum IP-Tracking) sowie Ders.: Ermittlungen im Darknet, S. 678 ff. (zum Ganzen).

[11] Zu Ermittlungen in virtuellen Kryptowährungssystemen Safferling, Christoph / Rückert, Christian: Telekommunikationsüberwachung bei Bitcoins, in: MMR 2015, S. 788-794.

[12] Details bei Safferling / Rückert: Das Strafrecht und die Underground Economy.

[13] Koalitionsvertrag, 19. Legislaturperiode, S. 128.

[14] Ausführlich dazu Safferling / Rückert: Das Strafrecht und die Underground Economy.

[15] Überblick bei Graf, Jürgen-Peter, in: BeckOK StPO, hrsg. v. Ders., § 100a Rn 242 ff., München, 29. Ed., 2018.

[16] Vgl. zu einem entsprechenden Vorhaben https://uk.reuters.com/article/uk-eu-data-order/europe-seeks-power-to-seize-overseas-data-in-challenge-to-tech-giants-idUKKCN1GA0LN, Stand: 12.3.2018.