Analysen & Argumente

Konrad Adenauer Stiftung

FEBRUAR 2018
AUSGABE 291

Das Strafrecht und die Underground Economy

Christoph Safferling | Christian Rückert

Zum Mitnehmen

- Das Tor-Netzwerk, Verschlüsselungstechnologien und Kryptowährungen erschweren die Strafverfolgung im Internet.
- Lösungsansätze bieten Ermittlungen an der Schnittstelle von virtueller und realer Welt, personelle und technische verdeckte Ermittlungen im Darknet und in virtuellen Kryptowährungssystemen sowie der Einsatz modernster Technologien.
- Mit dem behördlichen Einsatz von Spähsoftware nutzt der Staat dieselben IT-Schwachstellen aus wie kriminelle Hacker – ein Verhalten, das er eigentlich bekämpfen will. Die bisherigen rechtlichen Regelungen für den „Bundestrojaner" weisen handwerkliche Mängel auf. Zugleich erschweren die gesetzlichen Anforderungen die Anwendung staatlicher Spähprogramme.
- Die Bildung internationaler Ermittlungsgruppen erleichtert den Zugriff auf Daten ausländischer Server.
- Das Strafrecht bietet bereits jetzt wirksame Instrumente zur Bekämpfung der Underground Economy. Den Betrieb von Darknet-Foren oder -Marktplätzen generell unter Strafe zu stellen, wäre rechtsstaatlich bedenklich.

INHALT

Der Schwarzmarkthandel verschiedener illegaler Güter im Darknet (sog. Underground Economy) rückt zunehmend in den Fokus nationaler wie internationaler Strafverfolgungsbemühungen, politischer Debatten und internationaler Forschungskooperationen. Die Nutzung der (neuen) Technologie des Tor-Netzwerks und der dort befindlichen „Hidden Services" bietet für Verkäufer und Käufer illegaler Güter die Möglichkeit, ihre Geschäfte über das Massenkommunikationsmedium des Internets anbahnen bzw. abwickeln zu können, dabei jedoch gleichzeitig weitgehend anonym zu bleiben. Mit den virtuellen Kryptowährungssystemen (Bitcoin etc.) existiert seit einigen Jahren eine Möglichkeit, auch die Bezahlung der gekauften Waren anonym über das Internet vorzunehmen. Die Nutzung der neuen Technologien stellt die Strafverfolgungsbehörden dabei vor nicht unerhebliche Schwierigkeiten, weil sie auf einige „klassische" Ermittlungsmethoden zur Strafverfolgung im Internet und zur Verfolgung der „Spur des Geldes" nicht zurückgreifen können. Weitere Herausforderungen für die Strafverfolgung stellen die zunehmende Verschlüsselung sowohl von Kommunikationsmitteln als auch der Speicher von Endgeräten dar. Ein Zugriff auf die Daten ist oft nur unter großem technischem und personellem Ressourceneinsatz möglich.

Die Entwicklung neuer und kreativer Methoden zur Ermittlung gegen die Underground Economy im Darknet werfen sowohl rechtsdogmatische als auch rechtspolitische Fragen auf. Rechtsdogmatisch ist zu klären, ob für neue Ermittlungsmethoden bereits Rechtsgrundlagen in der Strafprozessordnung vorhanden sind und – wenn dies nicht der Fall ist – wie solche neuen Rechtsgrundlagen aussehen könnten bzw. müssten. Die Rechtspolitik muss sich vor allem mit dem Spannungsfeld zwischen der Unterstützung technischer Innovation, der IT-Sicherheit der Bürger und einer effektiven Strafverfolgung beschäftigen und dieses – soweit möglich – auflösen. Vor bislang ungelösten Problemen steht das Strafrecht auch bei der Frage der Strafbarkeit der beteiligten Personen. Was muss der Einzelne über die Geschäfte wissen, die über seine Plattform abgewickelt werden, um dafür (mit-)verantwortlich zu sein? Wie weit darf die Vorfeldkriminalisierung gehen, um die Underground Economy zu regulieren und verbotenes Verhalten zu unterbinden?

Phänomenologie: Darknet, Bitcoins und Underground Economy

1. Darknet und Underground Economy

Das sog. Darknet bezeichnet einen speziellen Teil der Internet-Infrastruktur. Diese kann grob in drei Kategorien eingeteilt werden:[1]

- *Surface Web*: Wird von Standardsuchmaschinen wie Google, Bing etc. gefunden und kann ohne weitere Identifikationsanforderungen aufgerufen werden.
- *Deep Web*: Wird von Suchmaschinen nicht indexiert und erfordert entweder exakte Kenntnis der Adresse oder – häufiger – Identifikation des Nutzers (z.B. Datenbanken).
- *Darknet*: Teil des Deep Web, der nur über spezielle Browser-Software erreichbar ist, welche die IP-Adresse des Nutzers verschleiert (zumeist Tor-Browser).

2. Überblick über die technischen Grundlagen des Darknets am Beispiel von Tor

Die Tor-Technologie anonymisiert Nutzer und Anbieter im Darknet.

Der primäre Zweck der Nutzung des Tor-Netzwerks besteht darin, die IP-Adresse der Nutzer und damit deren physischen Standort zu verschleiern. Technisch gesehen geschieht dies auf zwei unterschiedlichen Wegen für die Nutzer der Darknet-Markets auf der einen und die Anbieter/Betreiber der Darknet-Markets auf der anderen Seite.

a. Der Tor-Browser der Nutzer leitet das Signal zur Kommunikation mit dem Server des Darknet-Markets über drei verschiedene Relaisstationen um. Der Rechner des Nutzers kontaktiert dabei den sog. Entry-Node, dieser leitet das Signal an den sog. Middle-Node und dieser schließlich an den sog. Exit-Node weiter, der letztendlich die Kommunikation an den Server des Darknet-Markets vermittelt. Die Tor-Nodes werden dabei von freiwilligen Teilnehmern auf der ganzen Welt betrieben. Das Signal, das durch dieses Tor-Netzwerk geleitet wird, ist dreifach asymmetrisch verschlüsselt. Der Tor-Browser verschlüsselt das Signal jeweils mit den öffentlichen Schlüsseln der Nodes. Somit kann jeder Node nur diejenige Verschlüsselungsschicht entschlüsseln, zu der er den zugehörigen privaten Schlüssel besitzt. Hierdurch erhält jeder Node nur die notwendige Information, wo das empfangene Datenpaket herkommt und wohin es weitergesendet werden soll. Lediglich die letzte Verbindung von Exit-Node zum Server des Markets ist unverschlüsselt – allerdings wird auch hier eine verschlüsselte Verbindung aufgebaut, wenn der Server diese (https) anbietet.[2] Auf diese Weise wird zweierlei gewährleistet: Jede beteiligte Station kennt jeweils nur die Station, von der das Kommunikationssignal kommt und diejenige, an die sie es weiterleitet. Gleiches gilt für den Server des Darknet-Markets. Nur der Rechner des Nutzers kennt alle IP-Adressen. Hierdurch kann durch einen „Angreifer" (z.B. Strafverfolgungsbehörden) keine Verbindung zwischen der IP-Adresse des Nutzers und der Nutzung des Darknet-Markets hergestellt werden (weder durch die geloggten IP-Adressen bei den Relaisstationen oder dem Darknet-Market noch durch eine Verkehrsdatenabfrage beim Provider des Nutzers). Außerdem kann eine Telekommunikationsüberwachung „in der Leitung" die gesendeten Datenpakete nur in verschlüsselter und damit unlesbarer Form ausleiten.

b. Die IP-Adressen-Verschleierung des Anbieters des Darknet-Markets gestaltet sich etwas komplizierter. Dieser muss einen sog. Hidden Service im Tor-Netzwerk aufsetzen. Das funktioniert (stark vereinfacht) folgendermaßen: Der Anbieter hinterlässt auf einem Darknet-Server die „.onion-Adresse", unter der sein Service im Darknet auffindbar ist, und Informationen über weitere Darknet-Knoten, über die Kontakt mit ihm aufgenommen werden kann (sog. Introduction Points). Der Nutzer lädt diese Information herunter und bestimmt einen weiteren Darknet-Knoten als „Treffpunkt" mit dem Anbieter (sog. Rendezvous Point). Der Nutzer lässt dem Anbieter über eine Tor-Verbindung zum Introduction Point die Adresse des Rendezvous Point zukommen. Anbieter und Nutzer bauen dann jeweils eine Tor-Verbindung (s.o.) zum Rendezvous Point auf, der nun die Ende-zu-Ende verschlüsselte Kommunikation zwischen Anbieter und Nutzer vermittelt. Beide können nun miteinander kommunizieren, ohne die IP-Adresse des anderen zu kennen.[3]

Die einfache Anwendbarkeit des Tor-Browsers begünstigt die Underground Economy.

c. Trotz der hinter Tor stehenden komplexen Technologie ist die Anwendung durch Nutzer und Anbieter tatsächlich sehr einfach. Der Tor-Browser funktioniert für den Nutzer ähnlich wie andere bekannte Browser (Firefox, Chrome, Internet Explorer etc.). Für das Einrichten eines Hidden Services genügen allgemeine Kenntnisse über den technischen Aufbau von Internet-Seiten und eine sehr gut verständliche Schritt-für-Schritt-Anleitung[4]. Zum Erreichen eines Hidden Services muss der Nutzer lediglich die „.onion-Adresse" des Services in seinen Browser eingeben. Das Darknet bietet somit für Verkäufer und Käufer illegaler Güter ein hohes Maß an Anonymität bei gleichzeitig einfacher Bedienung. Dies eröffnet den Händlern einen deutlich größeren Absatzmarkt als bei vergleichbar anonymen Realwelt-Verkaufsmethoden.

3. Virtuelle Kryptowährungen als Hauptzahlungsmittel der Underground Economy

Virtuelle Kryptowährungen wie Bitcoin sind das Hauptzahlungsmittel der Underground Economy. Sie eignen sich dabei vor allem deshalb, weil die Kryptowährungssysteme ohne Banken oder andere zentral verwaltende Stellen auskommen: „Konten" werden durch ein Zwei-Schlüssel-System ersetzt, bei dem die Bitcoin-Adresse (also die „Kontonummer") vom öffentlichen Schlüssel abgeleitet und die Signatur zur Signierung von Transaktionen aus dem privaten Schlüssel berechnet wird. Die Schlüsselpaare werden dabei von der Bitcoin-Software selbst in nahezu beliebiger Anzahl erstellt, so dass nur der hinter ihnen stehende Nutzer weiß, dass die Bitcoin-Adressen ihm zugeordnet sind. Die Verwaltung der Schlüssel erfolgt über spezielle Software, sog. Wallets. Die Verifizierung von Transaktionen – im Buchgeldsystem von den beteiligten Banken vorgenommen – erfolgt in Kryptowährungssystemen über ein gemeinsames Transaktionshauptbuch, die sog. Blockchain. Dort werden – in Datenblöcken verpackt – von freiwilligen Nutzern (den sog. Minern, die als Belohnung vom System neu generierte Bitcoins gutgeschrieben bekommen) alle jemals getätigten Transaktionen eingetragen, so dass jeder Nutzer jederzeit weiß, welcher Bitcoin-Adresse wie viele Bitcoins aktuell zugeordnet sind. Die Datenblöcke stehen dabei in einem besonderen mathematischen Zusammenhang mit den vorhergehenden Datenblöcken, so dass eine Manipulation an der Transaktionsliste entweder sofort auffallen würde (da sich durch die Manipulation in einem Datenblock auch die Daten in den nachfolgenden Datenblöcken ändern würden) oder das „Umschreiben" aller nachfolgenden Datenblöcke erfordert. Dies ist ab einer gewissen Anzahl nachfolgender Datenblöcke aufgrund der hierzu notwendigen immensen Rechenleistung so gut wie unmöglich.[5]

Bitcoins ermöglichen die anonyme Bezahlung im Darknet.

4. Die Underground Economy: Foren und Marktplätze

Im Darknet hat sich eine florierende Schattenwirtschaft entwickelt. Gehandelt werden nahezu alle illegalen Güter. Die größte praktische Bedeutsamkeit für Strafverfolger weist dabei der Verkauf von Betäubungsmitteln[6] und Waffen sowie das Angebot von Cybercrime-Dienstleistungen (sog. crime-as-a-service, z.B. die Anmietung von Bot-Netzen oder das Durchführen von DDoS-Attacken) und strafrechtlich relevanten Datensätzen (z.B. Kreditkartendaten, ganze Identitäten etc.) auf.[7]

Die Infrastruktur des Handels im Darknet lässt sich grob in zwei „Geschäftsmodelle" einteilen: Foren und echte Darknet-Marktplätze. Den echten Marktplätzen kommt dabei in der Verfolgungspraxis die deutlich größere Bedeutung zu.

a. Im Darknet existieren *Foren*, die von ihren Betreibern gezielt als „Treffpunkt" für Nutzer mit kriminellen Absichten eingerichtet und betrieben werden. Wie das Beispiel des mittlerweile vom Netz genommenen „Deutschland im Deep Web"-Forums zeigt, dienen solche Foren ihren Nutzern zwar auch zum Austausch über „legale" Themen (z.B. politische Debatten); der auch vom Betreiber verfolgte Hauptzweck besteht jedoch in der Zurverfügungstellung einer Kommunikationsinfrastruktur, über welche die Nutzer ihre strafrechtlich relevanten Geschäfte anbahnen und abwickeln können. So stellte auch der Täter des Amoklaufs im Münchener Olympia-Einkaufszentrum den Kontakt zu dem Waffenhändler, von dem er die Tatwaffe erwarb, über „Deutschland im Deep Web" her.[8] Häufig findet sich in den Foren lediglich das erste Angebot des Verkäufers. Die weitere Verhandlung und die Abwicklung der Geschäfte erfolgt zumeist über verschlüsselte Kommunikationstools direkt zwischen Verkäufer und Käufer. An den illegalen Geschäften selbst sind die Forenbetreiber in der Regel nicht beteiligt und haben auch kein eigenes wirtschaftliches Interesse an ihnen. Das Betreiben der Foren

Darknet-Foren dienen oft der Anbahnung strafrechtlich relevanter Geschäfte.

erfolgt eher aus ideellem oder politischem Interesse an „besonders freiem Handel". In einigen Fällen finanzieren sich die Betreiber über freiwillige Spenden.

b. Die *Darknet-Marktplätze* wie z.B. Silkroad 1 und 2, AlphaBay, Hansa Market (alle mittlerweile von Ermittlungsbehörden geschlossen) oder Dream Market entsprechen in Aufbau und Organisation klassischen Internet-Marktplätzen. Es handelt sich um hochprofessionell programmierte und designte Online-Marktplätze, auf denen Verkäufer ihre Waren mit Bildern, Beschreibungen und Preisen präsentieren können und bei denen Käufer den Bestellvorgang vollständig über den Marktplatz selbst abwickeln können. Daneben verfügen diese Handelsplätze häufig auch über zusätzliche Funktionen wie z.B. ein Bewertungssystem der Verkäufer, Betrugserkennungssysteme oder einen Treuhandservice für die Abwicklung der Bezahlung zwischen Verkäufer und Käufer. Programmiert und betrieben werden solche Handelsplätze häufig von einer kleinen Gruppe von Administratoren, die über einen vollständigen Systemzugriff verfügen. In der Hierarchieebene darunter gibt es zumeist einige Moderatoren, die die Arbeit der Administratoren unterstützen oder sogar einzelne Teile der Pflege des Marktplatzes (z.B. das Bewertungssystem für Verkäufer) selbständig betreuen. Weder die Administratoren noch die Moderatoren sind in der Regel an den Geschäften der Verkäufer und Käufer direkt beteiligt oder nehmen selbst illegale Geschäfte über die Plattform vor. Allerdings verfügen einige Plattformen über ein (ausdifferenziertes) Provisionssystem, über das die Betreiber an den Geschäften der Verkäufer monetär beteiligt werden.

In der Regel sind die Administratoren und Moderatoren der Darknet-Plattformen nicht direkt an den illegalen Geschäften beteiligt.

Tatsächliche und rechtliche Probleme bei Ermittlungen im Darknet und gegen die Underground Economy

1. Verfassungsrechtliche Grundlagen

Trotz der zunehmenden Nutzung der Darknet- und Bitcoin-Technologie durch kriminelle Akteure zu strafrechtlich relevanten Zwecken darf zweierlei nicht vergessen werden: Erstens dienen beide Technologien auch gesellschaftlich wertvollen Zwecken (z.B. Kommunikation von und mit Dissidenten, Freiheitskämpfern, Journalisten und Whistleblowern in autokratischen Systemen)[9] und berechtigten Interessen (z.B. Anonymisierung der eigenen legalen Internetnutzung gegenüber Dienstanbietern und staatlichen Behörden). Zweitens ist die Nutzung von Tor und Bitcoins grundrechtlich geschützt.

Darknet und Kryptowährungen können nicht grundsätzlich verboten werden.

Ganz grundsätzlich sind alle personenbezogenen Daten, also solche bei denen sich ein Bezug zu einer konkreten Person – wenn auch erst mit Hilfe von technischen Analysewerkzeugen – herstellen lässt,[10] vom Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) geschützt. Staatliche Behörden benötigen daher eine gesetzliche Eingriffsgrundlage zur Erhebung personenbezogener Daten. Die Übermittlung von Daten (auch solchen ohne Personenbezug) zwischen Individuen ist von der Telekommunikationsfreiheit nach Art. 10 Abs. 1 GG erfasst. Somit sind die Daten „in der Leitung" vor staatlichem Zugriff geschützt. Ein Eingriff muss sich auch hier auf eine Eingriffsgrundlage (z.B. § 100a StPO) stützen lassen. Schließlich schützt das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) vor dem staatlichen Zugriff auf IT-Systeme.[11] Die Nutzung des Tor-Netzwerks und der Hidden Services kann somit auch als bloße technische Umsetzung bzw. Sicherstellung der grundgesetzlich geschützten Vertraulichkeit der Kommunikation zwischen Individuen im Internet betrachtet werden.[12] Gleiches gilt für die Verschlüsselung von Speichern in Endgeräten: Hier schützt die Technik gerade die Vertraulichkeit und die Integrität

des jeweiligen informationstechnischen Systems. Bitcoins unterfallen außerdem dem Eigentumsschutz von Art. 14 Abs. 1 GG; der gewerbliche Handel mit ihnen ist von der Berufsfreiheit geschützt (Art. 12 Abs. 1 GG).[13]

2. Herausforderungen durch „Anonymität" in Darknet und virtuellen Kryptowährungssystemen

Die Nutzung des Tor-Browsers und der Hidden Services im Tor-Netzwerk durch Händler und Käufer illegaler Waren stellt die Ermittlungsbehörden gerade in Kombination mit der Nutzung virtueller Kryptowährungssysteme zur Abwicklung der Zahlung vor neue Herausforderungen:

Die klassischen Ermittlungswerkzeuge helfen nicht weiter.

Die IP-Adresse, welche unter „normalen" Umständen zur Identifikation eines Internetnutzers dient, wird durch das Tor-Netzwerk verschleiert. Somit können die Ermittler weder die von Seitenbetreibern gespeicherten IP-Adressen noch die im Rahmen der Vorratsdatenspeicherung nach §§ 113a, b TKG gespeicherten Verkehrsdaten zu einer Identifikation des Standorts des tatverdächtigen Internetnutzers heranziehen. Durch die Selbstgenerierung der Schlüsselpaare und das Fehlen von Banken oder anderen Verwaltungsinstanzen sind die Nutzer in virtuellen Kryptowährungssystemen pseudonym. Außerdem stehen den Ermittlern viele der bislang zur Verfolgung der „Geldspur" eingesetzten Ermittlungswerkzeuge nicht zur Verfügung. So können weder Auskünfte von Banken verlangt (§§ 161, 95 StPO) noch Bankmitarbeiter als Zeugen vernommen oder Bankunterlagen beschlagnahmt (§§ 94 ff. StPO) werden. Ebenso wenig ist eine automatisierte Kontostammdatenabfrage nach § 24c KWG erfolgversprechend und es existiert kein Verdachtsmeldungssystem oder eine automatische Kontenüberwachung nach dem GWG.[14]

3. Herausforderungen durch Verschlüsselung von Kommunikation und Endgeräten

Weitere Hürden für strafprozessuale Ermittlungen – auch, aber nicht nur im Rahmen von Ermittlungen gegen die Underground Economy – stellen sich durch die zunehmende Verschlüsselung sowohl von Kommunikationsverbindungen als auch von Endgeräten (PCs, Smartphones, Tablets etc.).

Mit der Spähsoftware macht sich der Staat Methoden zu eigen, die er eigentlich bekämpft.

Durch die Verschlüsselung von Kommunikationsverbindungen erbringt eine traditionelle Telekommunikationsüberwachung (TKÜ) keine verwertbaren Erkenntnisse mehr, weil die ausgeleiteten Datenpakete nicht lesbar sind. Der Gesetzgeber hat hier versucht, Abhilfe zu schaffen, indem er die sog. Quellen-TKÜ in § 100a Abs. 1 S. 2, S. 3 StPO geregelt hat. Hierbei wird das Sender- und/oder das Empfängergerät mit einer speziellen Spähsoftware („Bundestrojaner") infiltriert. Dieses Programm greift die Kommunikationsdaten unmittelbar auf dem Gerät ab, entweder (auf dem Sendergerät) bevor diese verschlüsselt und verschickt werden oder (auf dem Empfängergerät) nachdem diese empfangen und entschlüsselt wurden. Ob diese neue Befugnisnorm in der Praxis allerdings eine große Wirkung entfaltet, ist derzeit noch unklar. Zum einen ist die Norm – gerade was die konkrete Durchführung einer Quellen-TKÜ angeht – mit einigen handwerklichen Mängeln behaftet.[15] Zum anderen muss auch abgewartet werden, ob und wie eine Spähsoftware programmiert werden kann, die den gesetzlichen Anforderungen im vollen Umfang genügt und ob es regelmäßig gelingt, diese Software auf dem Zielrechner aufzuspielen.[16] In diesem Zusammenhang ist rechtspolitisch brisant, dass die Behörden auf dieselben Schwachstellen in der IT-Sicherheit angewiesen sind, wie sie kriminelle Hacker ausnutzen. Der Staat nimmt de facto am „Exploit-Markt" teil, den er eigentlich bekämpfen soll. Wie zukünftig das Verhältnis der Ermittlungsbehörden zum Bundesamt für die Sicherheit in der

IT-Technik (BSI), das den Auftrag hat, die IT-Sicherheit der deutschen Bürger zu verbessern, ausgestaltet sein wird, ist vor diesem Hintergrund politisch klärungsbedürftig. Fragwürdig erscheint insbesondere die Idee, Hersteller von Rechnern und Software zu verpflichten, spezielle Schnittstellen für den Zugriff durch Ermittlungsbehörden (sog. Backdoors) einzurichten und vorzuhalten.[17]

Eine ähnliche Problemlage ergibt sich bei der Verschlüsselung des Speichers von Endgeräten. Wenn die Geräte mittels Passwort, PIN oder Fingerabdruckscanner gesperrt sind, ist der Speicher des Gerätes verschlüsselt und die Daten sind nicht les- und somit nicht auswertbar. Die Verwertbarkeit der Daten hängt dann von der technischen Qualität der Verschlüsselungssoftware und den technischen Möglichkeiten der Strafverfolgungsbehörden ab. Ob die Einrichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) hier eine merkbare Verbesserung gebracht hat, ist den Verfassern leider nicht bekannt. Da jedoch der Erfolg der Ermittlungstätigkeit nicht davon abhängen darf, ob die Entschlüsselungs- oder die Verschlüsslungstechnik im konkreten Fall zufällig besser ist, bedarf die Problematik allgemeinerer Lösungsansätze: Zunächst kann hier die in § 100b StPO neu geregelte Online-Durchsuchung Abhilfe schaffen. Diese erlaubt – ähnlich wie die Quellen-TKÜ – das Aufspielen eines Spähprogramms auf Endgeräten, um diese über einen gewissen Zeitraum vollständig zu überwachen und Daten direkt vom Gerät auszuleiten und damit eine etwaige Verschlüsselung zu umgehen. Allerdings ist die Norm des § 100b StPO gesetzestechnisch noch problematischer, als diejenige des § 100a StPO: So ist z.B. die Voraussetzung, dass das Spähprogramm, soweit möglich, *technisch sicherstellen* muss, dass keine Kernbereichsdaten erhoben werden (§ 100d Abs. 3 StPO), technisch nicht umsetzbar. Möglich wäre höchstens eine „Live-Durchsicht" durch einen menschlichen Ermittler. Dies ist aber keine *technische Sicherstellung* und außerdem würden die Kernbereichsdaten im Rahmen der Live-Durchsicht ausgeleitet und damit erhoben. Im Übrigen stellen sich die gleichen technischen Schwierigkeiten wie im Rahmen der Quellen-TKÜ. Lässt sich das Gerät – wie die meisten modernen Smartphones – durch einen Fingerabdruck entsperren, ist es natürlich denkbar, den Eigentümer bzw. Nutzungsberechtigten des Smartphones (notfalls mittels unmittelbaren Zwangs) dazu zu bewegen, seinen Finger auf den Scanner zu legen. Unklar ist allerdings, ob die Strafprozessordnung für eine solche Maßnahme eine entsprechende Rechtsgrundlage bereithält. § 81a StPO, die Befugnis zur körperlichen Untersuchung, scheidet dabei offensichtlich aus, weil die Maßnahme sowohl nach ihrem insoweit eindeutigen Wortlaut als auch nach ihrem Sinn und Zweck auf die *Untersuchung des Körpers* und nicht auf die Untersuchung anderer Beweise *mittels des Körpers* gerichtet ist.[18]

Die gesetzlichen Anforderungen an ein staatliches Spähprogramm sind zum Teil praktisch nicht umsetzbar.

§ 81b StPO enthält die Befugnis, zu erkennungsdienstlichen Zwecken oder zur Durchführung des Strafverfahrens Fingerabdrücke des Beschuldigten auch gegen dessen Willen aufzunehmen. In der strafrechtlichen Literatur wird die Ansicht vertreten, die Norm umfasse auch die Befugnis, den Beschuldigten zur Entsperrung seines Smartphones mittels seines Fingerabdrucks zu zwingen.[19] Das überzeugt aber nicht. Der Gesetzgeber hat diese Art ihrer Anwendung bei der Verabschiedung der Norm nicht erkannt, sondern nur an einen Eingriff in das Recht auf informationelle Selbstbestimmung gedacht. Wird das Smartphone mit Zwang entsperrt, erhalten die Ermittlungsbeamten Zugang zu einem informationstechnischen System; somit ist auch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme berührt.[20] Wegen des Wesentlichkeitsvorbehalts muss aber der Gesetzgeber entscheiden, ob § 81b StPO auch Eingriffe in dieses Grundrecht ermöglichen soll. In der Zwischenzeit ist § 81b StPO zur zwangsweisen Smartphone-Entsperrung nicht anwendbar.[21]

4. Grenzenlosigkeit des Darknets

Die Bildung internationaler Ermittlungsgruppen erleichtert den Zugriff auf Daten ausländischer Server.

Als Teil des Internets ist auch das Darknet nicht an Ländergrenzen gebunden. Server, Betreiber und Nutzer von Darknet-Handelsplätzen befinden sich häufig (zumindest auch) im Ausland. Daher stellen sich die gleichen völkerrechtlichen Fragen wie bei sonstigen Ermittlungen im Internet, insbesondere ob und in welchem Umfang deutsche Ermittlungsbehörden Daten von ausländischen Servern erheben dürfen. Die *Cybercrime Convention* sowie sonstige europa- und völkerrechtliche Abkommen zur zwischenstaatlichen Rechtshilfe schaffen hier keine befriedigende Abhilfe. Empfehlenswert ist daher die Bildung von internationalen Ermittlungsgruppen, in denen die Behörden der jeweiligen Länder über entsprechende Ermittlungsbefugnisse in ihren Heimatländern verfügen.[22]

Bei Ermittlungserfolgen stellt sich ferner die Frage, ob deutsches Strafrecht auf den ermittelten Sachverhalt überhaupt anwendbar ist. Nach der Grundregel der §§ 3, 9 StGB muss hierfür der Handlungs- oder der Erfolgsort in Deutschland liegen. Dies ist insbesondere dann der Fall, wenn die Täter strafrechtlich relevante Handlungen in Deutschland vornehmen – z.B. bei der (Durch-)Lieferung von Waren[23] –, wenn die Plattform von Deutschland aus betrieben wird oder sich die Bitcoin-Wallet auf einem deutschen Server befindet. Für den Handel mit bestimmten illegalen Waren, insbesondere für den besonders praxisrelevanten Bereich des Handels mit Betäubungsmitteln, gilt das deutsche Strafrecht unabhängig vom Handlungs- oder Erfolgsort, vgl. § 6 Nr. 5 StGB.[24]

5. Lösungsansätze

Die aus Sicht der Autoren derzeit erfolgversprechenden Ermittlungskonzepte lassen sich in drei Gruppen einteilen:

Die Ermittlungen gegen die Underground Economy sollten sich auf die Schnittstelle zur Realwelt konzentrieren.

a. Ermittlungsansatz kann zunächst die Schnittstelle zur Realwelt sein:[25] Ein Großteil der illegalen Güter besteht in körperlichen Gegenständen, wie z.B. Betäubungsmitteln oder Waffen. Diese müssen zum Kunden gelangen. Derzeit geschieht dies zumeist über den Postweg – nicht selten werden als Lieferadresse Postpackstationen verwendet. Hier könnte die Ermittlungsarbeit durch eine – vom Bundesinnenministerium vor kurzem vorgeschlagene – Videoüberwachung der Stationen erleichtert werden.[26] Auch die durch den illegalen Handel eingenommenen Bitcoins müssen irgendwann wieder den Weg in die „reale" Welt finden: Entweder indem diese „ausgecasht", also in Realwährung gewechselt werden oder beim Erwerb von Waren und Dienstleistungen (was allerdings bislang nur sehr eingeschränkt möglich ist). Daher sollten sich sowohl Repressions- als auch Präventionskonzepte im Zusammenhang mit virtuellen Kryptowährungssystemen auf die Realweltakteure konzentrieren, die einen solchen Umtausch anbieten. Konzepte, wie dasjenige der 5. Europäischen Geldwäscherichtlinie,[27] welche die Dienstleister zur Speicherung von Nutzerdaten und zur Überwachung des Nutzerverhaltens verpflichten, sind allerdings durch die faktische Grenzenlosigkeit der virtuellen Währungssysteme und die Unüberwachbarkeit aller Schnittstellen (z.B. können Bitcoins auch zwischen Privatpersonen gegen Bargeld getauscht werden)[28] leicht zu umgehen. Eine bessere Alternative bietet das vom Forschungsprojekt BITCRIME vorgeschlagene Transaktionsblacklisting-System.[29] Dieses nutzt die technische Eigenschaft des Bitcoin-Netzwerks, dass jede Transaktionskette durch die Blockchain bis zur Entstehung der Bitcoins zurückverfolgt werden kann. Transaktionen, die mit kriminellen Handlungen zusammenhängen (z.B. die Bezahlung illegaler Waren), können somit „geblacklistet" werden. Gelistete Transaktionen oder auf diese zurückgehende Transaktionen dürfen dann von

Ein Transaktionsblacklisting-System kann Geldwäsche mittels Kryptowährungen erschweren.

Dienstleistern/Händlern (z.B. Wechselbörsen, Online-Handelsplattformen) nicht bzw. nur zum Teil gegen Realwährung oder Waren eingetauscht werden. Hierdurch würde die Nutzung virtueller Kryptowährungssysteme für Kriminelle weniger attraktiv werden, da sie ihre Krypto-Coins nicht mehr „versilbern" könnten.

b. Ferner kommen zahlreiche Varianten einer verdeckten Online-Ermittlung im Darknet in Betracht. Als einfachste Maßnahme können Ermittler in den frei zugänglichen Darknet-Handelsplattformen auf „Online-Streife" gehen und dort nach Hinweisen auf Tatbeteiligte und Realweltermittlungsansätze (siehe a) suchen. Rechtsgrundlage ist hier die Ermittlungsgeneralklausel nach §§ 161, 163 StPO.[30] Als „echte" verdeckte Ermittlung kommt vor allem das „Einschleusen" von Polizeibeamten als Käufer, Verkäufer oder sogar Moderatoren/Administratoren auf Darknet-Handelsplätzen in Betracht. Die rechtliche Abgrenzung zwischen sog. nicht öffentlich ermittelnden Polizeibeamten (noeP, Rechtsgrundlage: §§ 161, 163 StPO) und verdeckten Ermittlern (Rechtsgrundlage: § 110a StPO) ist dabei fließend und wird von der h.M. anhand von drei Kriterien bestimmt:[31] 1. tatsächliche Intensität der überwundenen Zugangsbeschränkung (Passwortschutz, Identitätsfeststellung etc.); 2. Dauerhaftigkeit und Nutzungsanzahl der Legende; 3. Eigeninitiative des Ermittlers im Forum/auf der Handelsplattform (z.B. aktive Aufforderung zu Geschäften oder lediglich „Mitlesen"). Im Bereich internationaler Ermittlungen existieren Rechtsgrundlagen für den grenzüberschreitenden Einsatz verdeckter Ermittler in verschiedenen völkerrechtlichen Abkommen.[32]

Im Spannungsfeld zwischen Ermittlungseffektivität und Rechtsstaatlichkeit strafrechtlicher Ermittlungsverfahren stellt sich den verdeckten Ermittlern ein altbekanntes Problem im neuen Gewand: Verdeckte Ermittler dürfen nach deutschem Recht keine Straftaten begehen.[33] Im Bereich des Handels bzw. Austauschs von illegalen Gütern im Darknet (vor allem in Kinderpornografie-Tausch-Foren) wird von den Nutzern häufig eine sog. Keuschheitsprobe verlangt, bei welcher der Nutzer sich selbst strafbar machen muss bzw. strafrechtlich relevantes Material (z.B. Bilder und Videos i.S.v. §§ 184b, 184c StGB) hochladen muss.[34] Ein ähnliches Problem stellt sich, wenn der verdeckte Ermittler oder der nicht öffentlich ermittelnde Polizeibeamte am Handel mit Gütern teilnimmt, bei denen bestimmte Umgangsformen (wie Handeltreiben, Ankaufen, Inverkehrbringen, Besitzen etc.) strafrechtlich verboten sind. In den praktisch wichtigsten Fällen – bei Betäubungsmitteln und Waffen – wird die Problematik bereits durch die bestehende Rechtslage aufgelöst, indem das BtMG in § 4 Abs. 2 Bundes- und Landesbehörden im Rahmen ihrer dienstlichen Tätigkeit von einer Erlaubnispflicht zum Umgang mit Betäubungsmitteln befreit und das WaffG nach § 55 Abs. 1 für Polizeibehörden nicht anwendbar ist. Auch der „neue" § 202d StGB, der die Datenhehlerei unter Strafe stellt, enthält eine Ausnahme für Strafverfolgungsbehörden in Abs. 3 S. 2 Nr. 1. In einigen Fällen steht bereits der Handlungszweck der verdeckten Ermittlung und Sicherstellung der Tatbestandsverwirklichung entgegen (so z.B. bei §§ 258a, 146 Abs. 1 Nr. 2 StGB, Anstiftung und Beihilfe).[35] Schließlich kann in Einzelfällen zur Rechtfertigung oder Entschuldigung auf §§ 32, 34, 35 StGB zurückgegriffen werden.[36] Die verbleibenden Konstellationen sind, angesichts der andernfalls bestehenden Korrumpierungsgefahr der verdeckten Ermittler und des rechtsstaatlichen Gebots an Strafverfolgungsbehörden, nicht selbst zur Rechtsgutsgefährdung beizutragen, hinzunehmen. Einer Erweiterung der Befugnisse bedarf es daher derzeit nicht.

Der rechtliche Spielraum für verdeckte Ermittlungen im Darknet ist im Großen und Ganzen ausreichend.

Auch „technische" verdeckte „Ermittler" sind ein vielversprechender Ansatz. Als Beispiel mag hier das Ermittlungsverfahren im Zusammenhang mit der Darknet-Handelsplattform „Hansa Market" dienen, in dem holländische Ermittler die

Plattform heimlich übernahmen und so Daten über Verkäufer und Käufer sammelten.[37] Ebenso ist es denkbar, über den Betrieb eigener Tor-Knotenpunkte und Bitcoin-Nodes die über diese laufenden Kommunikationsdaten zu erheben und diese zu Ermittlungszwecken zu verwenden.[38] Insbesondere bei der Übernahme und dem Weiterbetrieb von Darknet-Marktplätzen (oder sogar bei der Einrichtung behördeneigener „Fake"-Marktplätze) erscheint jedoch problematisch, dass die Behörden hierbei letztlich Beihilfe zum Handel mit illegalen Waren leisten und – anders als in den Fällen klassischer Scheinkäufe – auch nicht verhindern können, dass die illegalen Güter in Umlauf geraten.

c. Schließlich muss zur Bekämpfung der Underground Economy im Darknet auch auf neueste Technologie zurückgegriffen werden bzw. deren Einsatz muss sowohl aus IT-forensischer als auch aus juristischer Sicht weiter erforscht werden. In Betracht kommen z.B. verschiedene Methoden des IP-Trackings,[39] die Anlage und der Ausbau von internationalen Ermittlungsdatenbanken (inklusive der Auslotung, ob ein Ankauf von Forensikdatenbanken von Privatunternehmen sinnvoll und rechtmäßig ist) und Forensisches Web Mining, das eine automatisierte Datenerhebung durch spezielle Web Crawler mit einer automatisierten Datenauswertung und -verknüpfung durch heuristische und statistische Methoden des Data Minings verbindet (sog. Online-Rasterfahndung).[40]

Die Ermittlungsbehörden müssen technisch aufgerüstet werden.

Die strafrechtliche Verantwortlichkeit der Handelsplattformbetreiber im Darknet

Probleme bereitet der Strafverfolgungspraxis auch die materiell-strafrechtliche Erfassung der Forums- und Marktplatzbetreiber. Diese – zum Teil äußerst komplexen – Problemkreise und Lösungsvorschläge können hier lediglich skizziert werden:

1. Auch die Betreiber von Darknet-Foren und -Marktplätzen sind sog. Host-Provider i.S.v. §§ 1 Abs. 1 S. 1, 2 S. 1 Nr. 1, 10 TMG, weil sie als Kommunikations- und Informationsanbieter lediglich Software und physischen Speicherplatz zur Nutzung durch andere (Verkäufer und Käufer) zur Verfügung stellen. Dementsprechend gilt für sie auch das Haftungsprivileg aus §§ 7, 10 TMG, so dass sie nicht zur Untersuchung ihrer Plattformen auf rechtswidrige Inhalte hin verpflichtet sind und diese nur bei positiver Kenntnis löschen müssen.[41] Unabhängig vom Streit über Reichweite und dogmatische Verortung der §§ 7 ff. TMG im strafrechtlichen Kontext spielen die Haftungsprivilegien für die Strafbarkeit der Underground Economy nur eine untergeordnete Rolle. Die §§ 7 ff. TMG schränken nämlich nur die Handlungspflichten der Provider und damit deren Unterlassungsstrafbarkeit ein.[42] Der Schwerpunkt der Vorwerfbarkeit liegt bei den Betreibern der Foren und Marktplätze aber gerade nicht darin, die illegalen Inhalte nicht gelöscht zu haben, sondern die Infrastruktur für den illegalen Handel aktiv zur Verfügung zu stellen und zu betreiben.[43] Deshalb ist auch die – dogmatisch interessante und äußerst komplexe – Frage nach einer Garantenstellung durch die bloße Zurverfügungstellung von Infrastruktur in der Praxis nicht weiter relevant. Das Netzwerkdurchsetzungsgesetz ist dagegen schon nicht anwendbar, weil die Darknet-Handelsplattformen zur Verbreitung spezifischer und nicht beliebiger Inhalte bestimmt sind (§ 1 Abs. 1 S. 1, S. 3 NetzDG) und die „rechtswidrigen Inhalte" i.S.v. § 1 Abs. 3 NetzDG nicht den Handel mit illegalen Gütern erfassen.

Haftungsprivileg für die Betreiber für Darknet-Foren und -Marktplätze?

2. Da die Betreiber selbst nicht an den einzelnen Geschäften beteiligt sind, ist eine mittäterschaftliche Zurechnung mangels gemeinsamen Tatplans und mangels Willens zur Tatherrschaft regelmäßig ausgeschlossen.[44] Im Rahmen einer (nahe-

liegenden) Beihilfestrafbarkeit ist problematisch, dass das Zurverfügungstellen einer Internetplattform zunächst als „neutrale bzw. sozialadäquate Handlung" betrachtet werden kann. Der Differenzierungsansatz der h.M., der danach unterscheidet, ob der Teilnehmer mit direktem Vorsatz bei objektiv deliktischem Sinnbezug oder zumindest mit (verschärftem) Eventualvorsatz bei erkennbarer Tatgeneigtheit gehandelt hat, ist auf den anonymen und technisierten Ablauf im Rahmen eines Darknet-Marktplatzes oder -Forums nicht ohne Weiteres übertragbar.[45] Hier muss ein anderer (evtl. neuer) Weg zu § 27 StGB gesucht werden. Dass er dorthin führt, erscheint allerdings angesichts des rein auf die Ermöglichung und Förderung rechtswidriger Taten gerichteten Zwecks des Betriebs nicht zweifelhaft. Prozessual ist zu beachten, dass eine Verurteilung nach § 27 StGB stets den konkreten Nachweis einer fremden Haupttat voraussetzt, was angesichts der o.g. Ermittlungshindernisse nicht stets gelingen wird. Zumindest würde ein großes „Dunkelfeld" zurückbleiben. Nicht nur deshalb, sondern auch angesichts der teilweise erheblichen Gewinnspannen und der tatsächlichen Ermöglichung einer großen Vielzahl von fremden Straftaten, erscheint es – gerade im Vergleich zum drohenden Strafmaß der Haupttäter (Verkäufer und Käufer) – auch nicht in jedem Fall „gerecht", wenn den Betreibern die zwingende Strafmilderung des § 27 Abs. 2 S. 2 StGB zugutekommt. Die Unterscheidung zwischen aus idealistischen Motiven handelnden Forenbetreiber und dem aus rein wirtschaftlichen Gründen handelnden Marktplatzbetreiber (mit Treuhandservice und Provisionssystem) lässt sich dennoch im Rahmen der konkreten Strafzumessung durch die Tatgerichte abbilden. Lässt sich kein (Eventual-)Vorsatz nachweisen, kommt bei Eintritt eines Schadens (z.B. durch den Gebrauch der verkauften Schusswaffe zu einer Gewalttat) auch eine Strafbarkeit aufgrund fahrlässigen Verhaltens in Betracht.

(Bloße) Bestrafung der Betreiber wegen Beihilfe erscheint nicht immer schuldangemessen.

3. Auch eine Strafbarkeit der Betreiber wegen Bildung krimineller Vereinigungen nach § 129 StGB wird im Regelfall ausscheiden, weil der Vereinigungsbegriff mehr als bloß arbeitsteiliges Vorgehen erfordert, von der Rollenverteilung und dem Bestand der Mitglieder grundsätzlich unabhängig sein muss (vgl. § 129 Abs. 2 StGB) und es deshalb angesichts der regelmäßig recht kleinen Gruppe an Administratoren mit klarer Rollenverteilung an der besonderen Eigendynamik, welche kriminelle Vereinigungen ausmacht, fehlen wird. Schließlich ist auch unklar, ob eine lediglich auf die Förderung fremder rechtswidriger Taten gerichtete Vereinigung überhaupt von § 129 StGB erfasst ist.[46]

Betreiber von Darknet-Foren und -Marktplätzen als kriminelle Vereinigungen?

4. In einigen Deliktsbereichen hilft die dort herrschende Dogmatik bereits über die oben skizzierten Probleme hinweg:

a. Dies gilt vor allem für die besonders praxisrelevanten Bereiche: Das „Handeltreiben" mit Betäubungsmitteln i.S.v. § 29 Abs. 1 Nr. 1 BtMG erfasst durch seine extensive Definition „jedes eigennützige Bemühen, das darauf gerichtet ist, den Umsatz von Betäubungsmitteln zu ermöglichen oder zu fördern"[47]. Hiervon ist gerade auch die bloße „Vermittlung" von Geschäften mit Betäubungsmitteln erfasst,[48] unter die man auch das Errichten und Betreiben einer Darknet-Handelsplattform zum Zweck des Handels mit Betäubungsmitteln durch andere subsumieren kann. Hier ist aber zu beachten, dass die neuere Rechtsprechung trotz der weiten Definition eines täterschaftlichen Handeltreibens vermehrt auf die „klassischen" Abgrenzungskriterien zwischen Täterschaft und Teilnahme zurückgreift.[49] Allerdings lässt sich, zumindest bei den „echten" Marktplätzen mit Treuhand- und Provisionssystem, oftmals – unter Berücksichtigung der deliktspezifischen extensiven Täterschaftsform – auch ein täterschaftliches Handeltreiben bejahen. Für die übrigen Fälle steht noch § 29 Abs. 1 Nr. 10 BtMG zur Verfügung, der bereits

Die Ermöglichung des Handels mit Betäubungsmitteln und der Umgang mit kinder- und jugendpornografischem Material im Darknet ist bereits ausreichend strafrechtlich erfasst.

die Verschaffung oder öffentliche Mitteilung einer Gelegenheit zum Erwerb oder zur Abgabe von Betäubungsmitteln unter Strafe stellt. Es greifen zwar bezüglich § 29 Abs. 1 Nr. 10 BtMG viele der Qualifikationen der §§ 29a, 30 und 30a BtMG nicht ein, ein besonders schwerer Fall nach § 29 Abs. 3 Nr. 1 BtMG bleibt aber möglich. Ähnliches gilt für den Waffenhandel nach § 52 Abs. 1 Nr. 1 und Nr. 2 c) WaffG; die Legaldefinition in Anlage 1 A2 Nr. 9 erfasst auch die Vermittlung des Vertriebs.[50] Im Bereich des verbotenen Umgangs mit kinder- und jugendpornografischem Material (§§ 184b, 184 c StGB) trägt oftmals der weite Besitzbegriff zur Lösung bei, der bereits das Vorhandensein im (Cache-)Speicher ausreichen lässt.[51]

b. Im Bereich des Handels rechtswidrig erlangter Daten (z.B. Kreditkartendaten, Identitäten) ist dagegen eine bloße Vermittlungstätigkeit von den Tathandlungsvarianten der §§ 202c, 202d StGB nicht erfasst. In diesem Bereich verbleibt daher nur der Weg über die allgemeinen Zurechnungsnormen (s.o.) und damit zumeist eine Beihilfestrafbarkeit der Betreiber. Da allerdings ein Handeln mit Bereicherungsabsicht zumindest bei den Betreibern der „echten" Marktplätze häufig zu bejahen ist, kommen in einigen Fällen auch die §§ 44 Abs. 1 und 43 Abs. 2 BDSG in Betracht.

5. Ein neuer Straftatbestand könnte nach alledem nur darauf abzielen, die (mit Bereicherungsabsicht ausgeführte) Vermittlungstätigkeit der Betreiber von Darknet-Handelsplattformen allgemein aus dem Bereich der Beihilfe herauszulösen und eine eigene Deliktsform zu schaffen, die in Strafrahmen, besonders schweren Fällen und Qualifikationen danach differenziert, welche Art von illegalen Waren in den vermittelten Geschäften gehandelt werden. Ob es angesichts der gerade geschilderten bereits bestehenden Strafvorschriften tatsächlich ein echtes Bedürfnis gibt, darf allerdings derzeit bezweifelt werden. Und schließlich darf auch Folgendes nicht aus dem Blick geraten: Bereits die Bestrafung des eigentlichen Handels mit Drogen und Waffen bezweckt die Bekämpfung einer lediglich abstrakten Gefahr, nämlich der Verbreitung der als gefährlich erachteten Gegenstände. Die Herstellung der bloßen Möglichkeit des Abschlusses solcher Geschäfte durch andere Personen schafft somit lediglich die abstrakte Gefahr der abstrakten Gefährdung durch andere. Rechtspolitisch sollte sorgfältig überlegt werden, ob eine solche extensive Vorfeldkriminalisierung wirklich notwendig ist.

Es ist zweifelhaft, ob die Schaffung eines neuen Straftatbestandes zur Bekämpfung der Underground Economy notwendig und rechtspolitisch sinnvoll ist.

Zusammenfassung der Thesen

Zusammenfassend lassen sich aus den gemachten Ausführungen folgende rechtspolitische und rechtsdogmatische Thesen für den strafrechtlichen Umgang mit der sog. Underground Economy im Darknet ableiten:

1. Das Tor-Netzwerk und virtuelle Kryptowährungssysteme ermöglichen eine weitgehend anonyme Nutzung des Internets und eines Online-Bezahlsystems. Durch die stets besser werdende Verschlüsselungstechnologie gelingt es, Daten besser vor fremdem Zugriff zu schützen.

2. Die Nutzung solcher Technologien ist grundrechtlich umfassend geschützt. Staatliche Eingriffe bedürfen einer verfassungsmäßigen Rechtsgrundlage.

3. Diese Technologien werden in zunehmendem Maße auch von kriminellen Akteuren zur Begehung von Straftaten verwendet.

4. Im Darknet hat sich eine florierende Schattenwirtschaft (sog. Underground Economy) entwickelt, in der nahezu alle illegalen Güter gehandelt werden. Ein besonderer Fokus der Strafverfolgungsbehörden liegt auf dem Handel mit Betäubungsmitteln, Waffen und rechtswidrig erlangten Daten sowie Schadsoftware.

5. Die Strafverfolgung wird bei Ermittlungen gegen die Underground Economy im Darknet vor neue Herausforderungen gestellt, da viele Standardermittlungsmaßnahmen, wie die Vorratsdatenspeicherung und die Kontostammdatenauskunft, im Darknet und in virtuellen Kryptowährungssystemen versagen. Zusätzliche Schwierigkeiten ergeben sich durch die Verschlüsselung von Datenträgern und die faktische Grenzenlosigkeit des Darknets als Teil des Internets.

6. Die neuen strafprozessualen Befugnisse zur Quellen-TKÜ und Online-Durchsuchung machen den Staat faktisch zum Teilnehmer am „Exploit"-Markt. Das künftige Verhältnis zwischen den Strafverfolgungsbehörden und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist daher rechtspolitisch klärungsbedürftig.

7. Ob die Einrichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) eine merkbare Verbesserung der technischen Möglichkeiten der Strafverfolgungsbehörden zur Entschlüsselung verschlüsselter Datenträger bewirkt hat, ist den Verfassern nicht bekannt.

8. Lösungsansätze bieten Realweltermittlungen, personale und technische verdeckte Ermittlungen im Darknet und in virtuellen Kryptowährungssystemen sowie der Einsatz modernster Technologie, wie diejenige des Forensischen Web Minings. Die Erforschung solcher Technologien aus IT- und rechtswissenschaftlicher Sicht sollte vorangetrieben werden.

9. Die materiell-strafrechtliche Erfassung der Tätigkeit der Betreiber von Darknet-Handelsplattformen und -foren ist dem Grunde nach ausreichend. Probleme ergeben sich lediglich daraus, dass häufig „nur" eine Beihilfestrafbarkeit in Betracht kommt und eine Verurteilung wegen Mitgliedschaft in einer kriminellen Vereinigung regelmäßig ausscheidet. In den praktisch bedeutsamen Bereichen des Betäubungsmittel- und Waffenhandels werden diese Probleme jedoch teilweise bereits durch eine extensive Auslegung des Tatbestandsmerkmals des „Handeltreibens" gelöst.

10. Für eine eigenständige und allgemeine Kriminalisierung des Betriebs von Darknet-Handelsplattformen fehlt der Bedarf. Die Schaffung eines entsprechenden Straftatbestands wäre angesichts der damit verbundenen expansiven Vorfeldkriminalisierung auch rechtsstaatlich bedenklich.

1| *Überblick über die Begrifflichkeiten m.w.N. bei Rückert, ZStW 129 (2017), 302, 310 f.*
2| *Vgl. zum Ganzen: https://www.torproject.org/about/overview.html.en#overview [15.01.2018].*
3| *Detailliert: https://www.torproject.org/docs/onion-services.html.en [15.01.2018].*
4| *Vgl. https://www.torproject.org/docs/tor-onion-service.html.en [15.01.2018].*
5| *Statt vieler zum Ganzen: Antonopoulos, Mastering Bitcoin, 2015, S. 15 ff.*
6| *Tzanetakis, APuZ 2017, Heft 46–47, S. 41 ff.*
7| *Hostettler, APuZ 2017, Heft 46–47, S. 10 ff. m.w.N.*
8| *Vgl. https://motherboard.vice.com/de/article/a3zj4p/das-bka-hat-die-grosste-deutsche-darknet-seite-kassiert [15.01.2018].*
9| *Siehe hierzu Moßbrucker, APuZ 2017, Heft 46–47, S. 16 ff.*
10| *BVerfGE 118, 168, 184 f.; 120, 274, 312.*
11| *Zu allen drei Grundrechten: Heinson, IT-Forensik, S. 73 ff., 82 ff., 84 ff. m.w.N.*
12| *Überblick mit Nachweisen bei Rückert, ZStW 129 (2017), 302, 309 ff.*
13| *Zu diesen und weiteren Grundrechten im Kontext virtueller Kryptowährungen: Rückert, Virtual Currencies and Fundamental Rights, SSRN 2016, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2820634 [15.01.2018].*
14| *Vgl. Safferling/Rückert, MMR 2015, 788, 791; Grzywotz/Köhler/Rückert, StV 2016, 753, 758.*
15| *Siehe hierzu Freiling/Safferling/Rückert, JR 2018, 9 ff.*
16| *Freiling/Safferling/Rückert, JR 2018, 9 ff.*
17| *Zu dieser Diskussion, siehe http://www.rnd-news.de/Exklusive-News/Meldungen/November-2017/De-Maiziere-will-Ausspaehen-von-Privat-Autos-Computern-und-Smart-TVs-ermoeglichen [15.01.2018].*
18| *Vgl. Bäumerich, NJW 2017, 2718.*
19| *Bäumerich, NJW 2017, 2718; Dölker/Müller-Peltzer, in Taeger (Hrsg.), Internet der Dinge, 863, 872ff.*
20| *Bäumerich, NJW 2017, 2718, 2722.*
21| *A.A.: Bäumerich, NJW 2017, 2718.*
22| *Vgl. z.B. J-Cat von Europol: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce [15.01.2018].*
23| *Zu Besonderheiten bei sog. Transit-Delikten: MüKoStGB-Ambos, § 9 Rn 11, 23 m.w.N.*
24| *Zum Ganzen: Safferling, Internationales Strafrecht, 2011, S. 7 ff.*
25| *Zu den Ermittlungen im Fall „Shiny Flakes": Hostettler, APuZ 2017, Heft 46–47, S. 10, S. 15 m.w.N.*
26| *Vgl. http://www.wiwo.de/unternehmen/dienstleister/post-innenministerium-fordert-videoueberwachung-von-packstationen/20683218.html [15.01.2018].*
27| *Vgl. http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf [15.01.2018].*
28| *Vgl. z.B. http://bitcoin-treff.de [15.01.2018].*
29| *Vgl. https://www.vstr.rw.fau.de/files/2017/01/BITCRIME_HE_DE_EN.pdf [15.01.2018].*
30| *Vgl. Rückert, ZStW 129 (2017), 302, 306.*
31| *Diese Kriterien wurden von Carsten Rosengarten und Sebastian Römer aus der Rechtsprechung und Literatur herausgearbeitet, vgl. NJW 2012, 1764, 1767.*
32| *Überblick bei: Meyer-Goßner/Schmitt, § 110a Rn 2a.*
33| *Allg. Meinung, vgl. nur MüKoStPO-Günther, § 110c Rn 39 f. m.w.N.*
34| *Vgl. z.B. https://www.ndr.de/nachrichten/netzwelt/Wir-setzen-vor-allem-verdeckte-Ermittler-ein,darknet124.html [15.01.2018].*
35| *MüKoStPO-Günther, § 110c Rn 39 f.; Meyer-Goßner/Schmitt, § 110c Rn 4.*
36| *Meyer-Goßner/Schmitt, § 110c Rn 4.*
37| *Vgl. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation; https://www.thedailybeast.com/this-is-how-cops-trick-dark-web-drug-dealers-into-unmasking-themselves [15.01.2018].*
38| *Vgl. http://www.zeit.de/digital/datenschutz/2014-01/spionierende-exit-nodes-im-tor-netz-entdeckt; https://arstechnica.com/information-technology/2014/11/law-enforcement-seized-tor-nodes-and-may-have-run-some-of-its-own/ [15.01.2018].*
39| *Siehe Krause, NStZ 2016, 139.*
40| *Siehe Rückert, ZStW 129 (2017), 302.*
41| *Vgl. Hoffmann, in: Stiftung der Hessischen Rechtsanwaltschaft (Hrsg.), S. 49, 53 ff.*
42| *Dies verkennt offensichtlich Hoffmann, a.a.O.*
43| *So richtig: Ceffinato, Jus 2017, 403, 408 f.*
44| *Ceffinato, Jus 2017, 403, 408.*
45| *Vgl. zu automatisierten und anonymen Abläufen allgemein: Bode, ZStW 127 (2015), 937, 955.*
46| *Zum Ganzen ausführlich: Ceffinato, Jus 2017, 403, 408 m.w.N.*
47| *Vgl. Weber, BtMG, § 29 Rn 168 m.w.N.*
48| *Vgl. MüKoStGB-Oğlakcıoğlu, § 29 Rn 423 m.w.N.*
49| *Vgl. BGHSt 50, 252; 51, 219.*
50| *Erbs/Kohlhaas-Pauckstadt-Maihold, § 52 WaffG Rn 18 m.w.N.*
51| *Vgl. hierzu BeckOKStGB-Ziegler, § 184b Rn 15 mit Bespielen und Nachweisen.*

Die Autoren

Professor Dr. Christoph Safferling, LL.M. (LSE), hat seit 2015 den Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg inne. Zuvor war er Professor für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht an der Philipps-Universität Marburg.

Akad. Rat a.Z. Dr. Christian Rückert ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Konrad-Adenauer-Stiftung e. V.

Ansprechpartner:
Tobias Montag
Koordinator Innenpolitik
Team Innenpolitik
Hauptabteilung Politik und Beratung
Telefon: +49(0)30/26996-3377
E-Mail: Tobias.Montag@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

ISBN 978-3-95721-405-8

www.kas.de