Lukas Schneider

BEKÄMPFUNG VON ONLINE-SCHWARZMÄRKTEN MITTELS QUELLEN-TELEKOMMUNIKATIONSÜBERWACHUNG

VORWORT

Das vorliegende E-Book basiert auf meiner gleichnamigen Bachelorarbeit. Sie entstand zwischen Winter 2017 und Frühjahr 2018. Ich schrieb sie als Abschlussarbeit meines Medienmanagement-Studiums an der Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt. Mein Betreuer während dieses Unterfangens war Prof. Dr. Achim Förster. Da das Thema in meinem Umfeld auf großes Interesse stieß und mir zeigte, dass die Allgemeinheit darüber nur unzureichend informiert ist, habe ich mich dazu entschieden, die Arbeit als E-Book der Öffentlichkeit zugänglich zu machen.

Ich wünsche Ihnen eine spannend Lektüre.

Lukas Schneider

Estenfeld, den 24. Mai 2018

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

BtMG	Betäubungsmittelgesetz
F&E	Forschung und Entwicklung
GG	Grundgesetz
IP	Internet Protokoll
KrWaffKontrG	Kriegswaffenkontrollgesetz
MDMA	3,4-Methylendioxy-N-methylamphetamin
NSA	National Security Agency
PM	Private Message
Quellen-TKÜ	Quellen-Telekommunikationsüberwachung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
Tor	The Onion Router
VoIP	Voice over IP
WaffG	Waffengesetz
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

1. EINLEITUNG

1.1 AUSGANGSSITUATION UND FORSCHUNGSLEITENDE FRAGE

Am 17. August 2017 beschloss der Deutsche Bundestag ein Gesetz, durch das eine Überwachungsmaßnahme zugelassen wurde, die massive Eingriffe in die Privatsphäre von Bürgern ermöglicht: Die sogenannte Quellen-Telekommunikationsüberwachung, kurz Quellen-TKÜ. Bisher konnten Polizei und Sicherheitsbehörden lediglich Telefonate und SMS von Personen überwachen, die im Verdacht standen, bestimmte Straftaten begangen zu haben oder begehen zu wollen. Mit dem Quellen-TKÜ-Gesetz wird diese Überwachung auf die vollständige Telekommunikation des Verdächtigen ausgeweitet.

Damit sind auch Internet-Telefonie-Dienste und Messenger wie WhatsApp betroffen. Da aber besonders bei Letzteren die kommunizierten Inhalte oft per Ende-zu-Ende-Verschlüsselung geschützt werden, können sie nicht auf üblichem Wege ausgelesen werden. Deshalb wird bei der Quellen-TKÜ eine Überwachungssoftware auf dem Computer oder mobilen Endgerät des Verdächtigen installiert. Dieses Vorgehen wird in den Medien stark kritisiert, da es dadurch auch möglich ist, die überwachten Geräte komplett auszuspähen.

Ob die Kritik berechtigt und die Quellen-TKÜ eine geeignete Maßnahme zur Bekämpfung von Verbrechen ist, wird anhand eines ebenfalls aktuellen und medial präsenten Themas erörtert: Online-Schwarzmärkte.

Darknet-Seiten wie Dream Market oder Tochka ermöglichen es praktisch jedem Menschen mit Internetzugang, anonym Waffen, Betäubungsmittel, Falschgeld und weitere verbotene Güter zu erwerben. Dies geschieht ganz einfach von zu Hause aus, mit nur wenigen Klicks. Die Ware kommt per Post, bezahlt wird meist in Bitcoin. Dagegen vorzugehen ist sehr schwierig.

So gibt es beim herkömmlichen Drogenhandel Produzenten, Lieferanten, Zwischenhändler und Kleindealer. Das sind viele beteiligte Personen, die bei der Ausübung einer Straftat erwischt werden können. Bei Online-Schwarzmärkten

hingegen gibt es nur Käufer und Verkäufer. Des Weiteren bewegen sich die Nutzer solcher Seiten anonymisiert und durch Verschlüsselungen geschützt durch das Darknet. All das erschwert die Strafverfolgung enorm.

Unter diesen Gesichtspunkten stellt sich folgende forschungsleitende Frage: **„Wie sinnvoll ist die Quellen-Telekommunikationsüberwachung im Bezug auf die Bekämpfung von Online-Schwarzmärkten?“**.

1.2 GANG DURCH DIE ARBEIT

Um diese Frage zu beantworten, wird zunächst die Quellen-TKÜ betrachtet. Es wird darauf eingegangen, weshalb ihre Einführung als notwendig erachtet wurde und wie sie sich von der Online-Durchsuchung und der herkömmlichen Telekommunikationsüberwachung unterscheidet. Danach werden ihre rechtlichen und technischen Grundlagen dargelegt, um zu verdeutlichen was ihr erlaubt ist und wie sie funktioniert. Daraufhin wird die an ihr geäußerte Kritik in mehrere Bereiche unterteilt, vorgestellt und bewertet.

Anschließend wird auf Online-Schwarzmärkte eingegangen. Nach einer Erläuterung, wie auf diese Seiten zugegriffen werden kann und welche Vorteile sie ihren Nutzern bieten, werden die dort verfügbaren Waren und die damit verbundenen Straftatbestände vorgestellt. Darauf folgt, wie die Bezahlung genau abläuft und die Waren vom Verkäufer zum Kunden gelangen. Auch werden einige bekannte Online-Schwarzmärkte betrachtet. Der letzte Teil des Kapitels behandelt die bisherige Strafverfolgung in diesem Bereich; welche Erfolge erzielt wurden und welche Schwierigkeiten bei den Ermittlungen auftreten.

Nun wird die Quellen-TKÜ auf die Online-Schwarzmärkte angewandt. Dafür werden zunächst mögliche Zielpersonen für die Überwachungsmaßnahmen benannt und es wird betrachtet, wie sich diese identifizieren lassen. Daraufhin wird geprüft, bei welchen auf Online-Schwarzmärkten begangenen Straftaten eine Quellen-TKÜ überhaupt zulässig ist. Im Anschluss wird untersucht, auf welche Weise die Überwachungssoftware auf das betroffene Gerät aufgespielt wird und wie sich die Überwachung der Telekommunikationskanäle konkret gestaltet.

2. QUELLEN-TELEKOMMUNIKATIONSÜBERWACHUNG

2.1 DIE QUELLEN-TKÜ UND IHRE NOTWENDIGKEIT

Heutzutage sind informationstechnische Systeme weit verbreitet. Fast jeder hat ein Smartphone und kommuniziert damit neben dem normalen Telefonieren per SMS, Messenger-Apps und Internet-Telefonie. Auch Kriminelle greifen darauf zurück. Deshalb ist es unerlässlich, diese Kommunikationswege zu überwachen, um dadurch Straftaten zu verhindern oder aufklären zu können (BT-Drs. 18/2785, S. 46).

Allerdings nutzen viele Messenger-Apps, wie WhatsApp, Telegram und Threema und auch VoIP-Dienste, wie Facetime, eine Ende-zu-Ende-Verschlüsselung. Mit der bisher üblichen Telekommunikationsüberwachung lässt sich hier nur an verschlüsselte Daten kommen, die zu entschlüsseln viel Geld und Zeit kosten würde, oder schlicht nicht möglich ist (BT-Drs. 18/2785, S. 48). Denn bei der Ende-zu-Ende-Verschlüsselung können verschickte Nachrichten nur von Sender und Empfänger gelesen werden. Selbst die Unternehmen, die hinter den Messengern stehen, haben keine Möglichkeit auf die Kommunikation zuzugreifen, und können somit auch keine Daten an die Behörden weitergeben (Flade 2017a).

Ohne die Quellen-TKÜ gäbe es zwei Szenarien:

1. Die Polizei akzeptiert, dass sie an diese Informationen nicht herankommt. Kriminelle nutzen verschlüsselte Kommunikationskanäle in dem Wissen, dass sie vor einer Entdeckung sicher sind. Sämtliche Kommunikation mit strafrechtlich relevantem Inhalt verlagert sich auf Kanäle mit Ende-zu-Ende-Verschlüsselung, sodass auch durch die normale Telekommunikationsüberwachung kaum noch Straftaten aufgedeckt werden.

2. Die Entwickler von Messenger-Apps bauen gezielt Schwachpunkte in die Verschlüsselungen ein, die den Behörden eine Entschlüsselung der Kommunikationsinhalte ermöglichen. Da aber die Bundesregierung Verschlüsselung aufgrund der damit einhergehenden Datensicherheit unterstützt, kommt diese Möglichkeit nicht infrage. Denn solche absichtlich eingebauten Hintertüren könnten von Kriminellen, wie Hackern, ausgenutzt werden. Deshalb muss die Kommunikationsüberwachung noch vor der Verschlüsselung stattfinden, indem eine versteckte Software auf dem Zielgerät installiert wird (BT-Drs. 18/2785, S. 48f).

Die Quellen-TKÜ macht das möglich, und es ist dieses Abgreifen von Kommunikationsdaten direkt an der Quelle, also auf dem Smartphone oder PC, dem sie ihren Namen verdankt (Freiling 2016, S. 207). Bei der klassischen TKÜ ist es hingegen so, dass die Ermittlungsbehörden für gewöhnlich über den Kommunikationsdienstleister an die Daten gelangen.

Das Besondere an Quellen- und herkömmlicher TKÜ ist, dass es sich, anders als bei Vernehmungen oder Hausdurchsuchungen, um Ermittlungsmaßnahmen handelt, von denen der Betroffenen keine Kenntnis erlangt. Dadurch kann er die Ermittlungen nicht durch Lügen oder das Verweigern von Aussagen erschweren (Mitsch 2012, S. 146).

Die Telekommunikationsüberwachung ist demnach ein wichtiges Ermittlungswerkzeug, das durch die Quellen-TKÜ an die heutige Zeit, in der die Smartphone-Nutzung weit verbreitet ist, angepasst wird. Ähnlich sieht das auch Bundesinnenminister Thomas de Maizière. Er ließ verlauten, dass Verschlüsselung, durch die die Vertraulichkeit der Kommunikation geschützt werde, kein Freibrief für Verbrecher sein dürfe, die immer öfter selbst verschlüsselt kommunizieren. Mit dem neuen Quellen-TKÜ-Gesetz sei eine Befugnislücke in der Strafverfolgung geschlossen worden (Tagesschau 2017).

2.2 ABGRENZUNG ZUR TELEKOMMUNIKATIONSÜBERWACHUNG

Bei der Telekommunikationsüberwachung überwacht die Polizei E-Mails, Telefonate und SMS von verdächtigen Personen. Anders als bei der Quellen-TKÜ werden diese aber nicht direkt am Endgerät abgegriffen. Vielmehr erhalten die Behörden die gewünschten Informationen von den Anbietern der Telekommunikationsdienste, die nach § 100a Abs. 4 StPO zu dieser Auskunftserteilung verpflichtet sind (Flade 2017a). Die Kommunikationsinhalte, die TKÜ und Quellen-TKÜ ans Licht bringen sollen, sind die gleichen. Nur die Art der Informationsgewinnung ist unterschiedlich.

Die Telekommunikationsüberwachung ist eine Ermittlungsmaßnahme, die häufig angewendet wird. Alleine im Jahr 2015 wurde sie 32.000 Mal genutzt (Stöcker 2017). Da sowohl TKÜ als auch Quellen-TKÜ in § 100a StPO begründet sind, ist davon auszugehen, dass die Quellen-TKÜ in Zukunft ähnlich häufig angewendet werden wird. In weiten Teilen allerdings wird sie die herkömmliche TKÜ ablösen, da Kriminelle immer häufiger über verschlüsselte Kanäle miteinander kommunizieren (Bode 2012, S. 359).

2.3 ABGRENZUNG ZUR ONLINE-DURCHSUCHUNG

Bei der Online-Durchsuchung wird, ohne das Wissen des Eigentümers, auf einen Computer oder ein Smartphone zugegriffen, um die darauf gespeicherten Daten auszulesen (Kugelmann 2012, S. 206). Dies geschieht durch die unbemerkte Installation einer Überwachungssoftware auf dem betroffenen Gerät. Das klingt zunächst nach der Quellen-TKÜ, die auch von einer solchen Software Gebrauch macht. Doch der Unterschied der beiden Ermittlungsmaßnahmen zeigt sich nach dem Aufspielen der Software. Während die Quellen-TKÜ auf Kommunikationsinhalte abzielt, werden bei der Online-Durchsuchung sämtliche gespeicherten Inhalte ausgelesen (Tinnefeld/Buchner/Petri 2012, S. 108).

Also unter anderem Dokumente, Browserverläufe, installierte Apps und Programme, Videos und Audio-Dateien. Die Online-Durchsuchung ist demnach ein erheblich mächtigeres Werkzeug, als es Telekommunikationsüberwachung und Quellen-TKÜ sind, da sie in einem viel größeren Umfang Daten überwacht und ausliest. Sie bedeutet aber auch einen deutlich schwerwiegenderen Eingriff in die Privatsphäre des Betroffenen.

2.4 RECHTLICHE GRUNDLAGEN

2.4.1 Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Am 22. Juni 2017 nahm der Deutsche Bundestag den Gesetzesentwurf zu dem „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ an. Ursprünglich handelte das Gesetz unter anderem von audiovisuellen Aufzeichnungen von Beschuldigten im Ermittlungsverfahren, Änderungen im Befangenheitsrecht, Möglichkeiten zur Fristsetzung im Beweisantragsrecht, der Pflicht von Zeugen, bei der Polizei zu Erscheinen und der Verhängung von Fahrverboten als Strafmaßnahme. Über einen Änderungsantrag von CDU/CSU und SPD wurde dem Gesetzesentwurf die Rechtsgrundlage für die Quellen-TKÜ beigefügt (Beukelmann 2017, S. 440).

Dies geschah durch eine Erweiterung von § 100a Abs. 1 StPO, die besagt, dass die Überwachung und Aufzeichnung von Kommunikation auch erfolgen darf, indem mit technischen Mitteln auf informationstechnische Systeme zugegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen.

Aber auch einige andere, die Telekommunikationsüberwachung betreffende Paragraphen in der StPO wurden geändert oder ergänzt.

2.4.2 Anwendung der Quellen-TKÜ

Die Quellen-TKÜ darf laut § 100a Abs. 1 Nr. 1 StPO nur angewendet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine schwere Straftat begangen hat oder zu begehen versucht. Schwere Straftaten in diesem Sinne sind laut § 100a Abs. 2 StPO unter anderem Geldfälschung, Mord und Totschlag, Geldwäsche, Urkundenfälschung, Steuerhinterziehung, Bestechlichkeit und Bestechung, Verleitung zur missbräuchlichen Asylantragsstellung sowie einige Straftaten aus dem Betäubungsmittelgesetz, dem Waffengesetz und dem Gesetz zur Kontrolle von Kriegswaffen. Die Liste der Straftaten, die einen Einsatz der Quellen-TKÜ ermöglichen, ist äußerst umfangreich.

Ein Verdacht auf eine Straftat kann begründet werden mit Observationen, Zeugenaussagen, den Ergebnissen eines Schusswaffenvergleichs oder Beweisanzeichen wie Fingerabdrücken (Hauck, in: Löwe/Rosenberg, StPO, § 100a, Rnd. 50). Ist ein solcher Verdacht auf eine schwere Straftat gegeben, wird nach § 100e Abs. 1 StPO die Staatsanwaltschaft einen Antrag an das Gericht stellen, welches die Quellen-TKÜ anordnen kann.

Wenn Gefahr im Verzug ist, kann die Anordnung aber auch direkt von der Staatsanwaltschaft, ohne das Gericht, getroffen werden. Sinnvoll ist dieses schnelle Vorgehen, wenn beispielsweise eine Person im Verdacht steht, einen Terroranschlag zu planen, aber keine ausreichenden Beweise vorliegen, um eine Verhaftung zu rechtfertigen. Ein schnelles Durchführen der Quellen-TKÜ kann solche Beweise liefern.

Dass eine richterliche Anordnung vonnöten ist, um die Quellen-TKÜ als Ermittlungswerkzeug anzuwenden, ist sehr wichtig. Da sie bereits beim Verdacht auf eine große Anzahl verschiedener Straftaten zum Einsatz kommen kann, ist sie leicht zu missbrauchen. Doch durch die richterliche Anordnung wird verhindert, dass die Polizei das Überwachungsinstrument Quellen-TKÜ willkürlich einsetzt (Moser-Knierim 2014, S. 99).

Grundsätzlich darf die Quellen-TKÜ nach § 100e Abs. 1 Satz 4 StPO nicht länger als drei Monate angewendet werden. Eine Verlängerung um weitere drei Monate ist

allerdings möglich, sofern die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Die drei Monate beginnen mit Ergehen der richterlichen Anordnung (BT-Drs. 18/12785, S. 52).

2.4.3 Umfang der Quellen-TKÜ

Mit der Quellen-TKÜ darf Kommunikation direkt auf dem Endgerät eines Verdächtigen überwacht werden. Beim Anwenden der Ermittlungsmaßnahme muss aber sichergestellt sein, dass nur solche Inhalte ausgelesen werden, die mit der herkömmlichen TKÜ in verschlüsselter Form hätten abfangen werden können (BT-Drs. 18/12785, S. 49).

Der Grundgedanke hinter der Quellen-TKÜ ist folglich nicht bisherige Überwachungsmaßnahmen auszuweiten, sondern sie an den technischen Fortschritt und das Aufkommen von Verschlüsselungstechnologien anzupassen. Nachrichten, die vor der richterlichen Anordnung der Quellen-TKÜ versendet oder empfangen wurden, dürfen nicht ausgelesen werden. Daraus folgt, dass es der Überwachungssoftware möglich sein muss, zwischen Nachrichten, die vor und die nach der richterlichen Anordnung der Überwachung versendet wurden, zu unterscheiden. Möglich ist das anhand der Metadaten der Kommunikationsinhalte. Sie geben an, wann eine Nachricht gesendet, empfangen und gelesen wurde. Falls alle auf dem Endgerät enthaltenen Kommunikationsinhalte ausgelesen werden sollen, unabhängig vom Zeitpunkt ihres Versendens, kann und muss auf die Online-Durchsuchung zurückgegriffen werden (BT-Drs. 18/12785, S. 50).

Mit der Quellen-TKÜ kann demnach nicht nur laufende Kommunikation überwacht werden. Als laufende Kommunikation gelten beispielsweise Gespräche mittels VoIP, das Versenden und Empfangen von E-Mails, Chats im Internet oder per Messenger (Buermeyer 2013). Auch ruhende Kommunikation, Kommunikationsinhalte, deren Übermittlung in der Vergangenheit liegt, darf ausgelesen werden, wenn der Übertragungsvorgang nach der Anordnung der Quellen-TKÜ geschehen ist. Aus technischer Sicht ist ruhende Kommunikation allerdings keine Telekommunikation, da diese nach § 3 Nr. 22 TKG der Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen ist. Kommunikationsinhalte, die die Übermittlung noch vor oder bereits hinter sich haben, sind nach dem Telekommunikationsgesetz keine Telekommunikation.

Der für die Quellen-TKÜ erweiterte § 100a Abs. 1 StPO ist geschickt formuliert. Die Endgeräte, die zu überwachen zulässig ist, werden informationstechnische Systeme genannt. Es ist nicht ausdrücklich von Smartphones oder Computern die Rede. Vielmehr kann der Begriff auf alle Geräte, mit denen Kommunikation möglich ist, bezogen werden. Sogar Geräte, die es noch gar nicht gibt und erst entwickelt werden müssen, sind informationstechnische Geräte (Beuth/Biermann 2017). Hierdurch ist sichergestellt, dass der § 100a Abs. 1 StPO nicht angepasst werden muss, falls in Zukunft eine neue, bisher noch nicht existente Klasse von Endgeräten erscheint.

Die Quellen-TKÜ lässt sich nicht nur gegen den Verdächtigen einsetzen. Laut § 100a Abs. 3 StPO darf sie sich auch gegen Personen richten, bei denen anzunehmen ist, dass sie Mitteilungen vom Beschuldigten empfangen, in seinem Namen Nachrichten entgegennehmen oder weitergeben, oder deren informationstechnisches System vom Beschuldigten benutzt wird. Was nach einer willkürlichen Erweiterung des Einflussbereichs der Quellen-TKÜ klingt, ist tatsächlich unerlässlich. Denn zur Kommunikation gehören immer zwei Personen. Nachrichten, die der Verdächtige empfängt, wurden schließlich von Jemandem geschrieben und abgeschickt. Dieser wird folglich automatisch von der Quellen-TKÜ mitüberwacht, zumindest der Teil seiner Kommunikationsinhalte, die zwischen ihm und dem Verdächtigen übermittelt werden. Ohne § 100a Abs. 3 StPO, der diese Überwachung von Dritten genehmigt, wäre die gesamte Quellen-TKÜ als unzulässig einzustufen.

2.5 TECHNISCHE GRUNDLAGEN

Um die Quellen-TKÜ durchzuführen, muss zunächst die Spionagesoftware auf dem Endgerät des Verdächtigen installiert werden. Dies kann durch Ferninstallation erfolgen oder durch kriminalistische List. Das wäre zum Beispiel, wenn der Betroffene in einem Café sitzt, ein Ermittler ihm unbemerkt das Smartphone aus der Tasche zieht, die Software im Nebenzimmer aufspielt und das Gerät dann heimlich zurückbringt. In die Wohnung des Verdächtigen einzudringen, um die Überwachungssoftware zu installieren, ist nicht erlaubt (BT-Drs. 18/12785, S. 52).

In verschlüsselter Form sind die Kommunikationsdaten nutzlos. Aber Nachrichten müssen zunächst einmal geschrieben und dann auch gelesen werden. Sie sind demzufolge in unverschlüsselter Form auf dem Bildschirm des überwachten Gerätes sichtbar. Hier sollen die Informationen ausgelesen werden (Sokolow 2017a).

Der tatsächliche Zugriff auf die Kommunikationsinhalte kann auf verschiedene Arten erfolgen. Bei Internet-Telefonie können die Gespräche mitgeschnitten, gespeichert und an die Behörden gesendet werden. Bei schriftlicher Kommunikation, etwa per Messenger-Apps, lassen sich die Tastatureingaben mittels Key-Logger aufzeichnen (BeckOK/Graf StPO § 100a Rn. 107b).

Ein Key-Logger greift nicht auf gespeicherte Daten zu, sondern zeichnet alle Tastaturanschläge auf dem Gerät auf (Abate 2011, S. 124).

Mit moderner Spionagesoftware ist heutzutage allerdings bereits deutlich mehr möglich. Es lassen sich in regelmäßigen Abständen Screenshots erstellen, was eine Alternative zu Key-Loggern ist. Hier liegen die Kommunikationsinhalte im Bildformat vor. Kamera und Mikrofon lassen sich aus der Ferne kontrollieren, was sich bei Videochats und Internet-Telefonie als nützlich erweist. Des Weiteren lässt sich, mittels IP-Adresse und der Zeitzone des Endgeräts, ein grober Standort des Verdächtigen ermitteln (Freiling 2016, S. 205-207).

Es bieten sich demnach mehrere Wege, um mittels Quellen-TKÜ an Kommunikationsinhalte zu gelangen, die man mit der herkömmlichen Telekommunikationsüberwachung nur in verschlüsselter Form hätte abgreifen können.

2.6 KRITIK AN DER QUELLEN-TKÜ

2.6.1 Art der Einführung

Das Gesetz, das die Änderungen in der StPO enthält, die die Quellen-Telekommunikationsüberwachung ermöglichen, wurde in einem Änderungsantrag in einen bereits bestehenden Gesetzesentwurf zur Änderung der StPO eingebracht. Dadurch kam es nicht zu den drei Lesungen der Änderungen, die verfassungsrechtlich vorgesehen sind. Der Bundesrat und die Bundesdatenschutzbeauftragte wurden umgangen und nicht beteiligt (Grunert 2017).

Dieses Vorgehen erntete einige Kritik. Der Deutsche Anwaltsverein bemängelte, dass das Gesetz über den Änderungsantrag und nicht auf ordnungsgemäßem Wege eingebracht worden sei (Schiemzik 2017). Auch die Grünen kritisierten diese Vorgehensweise. Der Ursprung des Gesetzesentwurfes sei durch den Änderungsantrag vollkommen verändert worden. Die Linke lehnte den gesamten Gesetzesentwurf ab (BT-Drs. 18/12785, S. 42).

CDU/CSU und die SPD hingegen verteidigten diesen. Laut der SPD sei die Quellen-TKÜ dringend notwendig. CDU und CSU ließen verlauten, dass sie Kritik an der Art der Einführung nicht nachvollziehen könnten. Sie verstünden aber, dass beim Inhalt des Gesetzes die Meinungen auseinandergehen (BT-Drs. 18/12785, S. 42).

2.6.2 Verstoß gegen das Fernmeldegeheimnis

Der Art. 10 Abs. 1 GG besagt, dass Brief-, Post- und Fernmeldegeheimnis unverletzlich sind. Die Quellen-TKÜ stellt zunächst einen Eingriff in dieses Grundgesetz dar (Kugelmann 2012, S. 201). Allerdings dürfen nach Art. 10 Abs. 2 GG aufgrund eines Gesetzes Beschränkungen des Art. 10 Abs. 1 GG angeordnet werden. Dies geschieht mit § 100a Abs. 1 StPO. Der Eingriff der Quellen-TKÜ in das Fernmeldegeheimnis ist somit zulässig.

2.6.3 Ausnutzen von Sicherheitslücken

Dennoch ist die Quellen-TKÜ nicht unproblematisch. Der Bundesverband IT-Sicherheit e.V. hat am 09. August 2017 eine Verfassungsbeschwerde angekündigt. Sie wird damit begründet, dass der Staat Sicherheitslücken in Endgeräten ausnutzt, um die Quellen-TKÜ-Software aufzuspielen, statt sie zum Wohl der Bürger zu schließen. Hierdurch, aber auch durch die Überwachungsmaßnahmen an sich, wird das Vertrauen der Bevölkerung in IT-Geräte verringert. Diesen Kritikpunkten lässt sich nichts entgegensetzen. Der Bundesverband IT-Sicherheit e.V. vertritt aber auch die Meinung, dass die Quellen-TKÜ wenig nutzen wird, da Kriminelle zu anderen Kommunikationswegen wechseln werden (Reimer 2017, S. 645).

Dieses Argument ist nicht treffend. Die Quellen-TKÜ ist die Antwort darauf, dass Kriminelle von Kanälen, die mit der herkömmlichen Telekommunikations-überwachung abgehört werden konnten, zu verschlüsselten Kommunikationswegen gewechselt sind. Falls sie nun erneut den Kommunikationskanal wechseln würden, wäre das kein Problem. Denn § 100a Abs. 1 StPO ist so formuliert, dass sämtliche informationstechnischen Systeme per Quellen-TKÜ überwacht werden können. Einen Weg zu finden, mit dem Kommunikation über weite Entfernungen problemlos möglich ist, und auf den die Quellen-TKÜ nicht angewendet werden kann, dürfte sich demzufolge für Kriminelle als schwierig gestalten.

Die Befürchtung des Bundesverbandes IT-Sicherheit e.V., dass Sicherheitslücken in Endgeräten zum Zweck der Quellen-TKÜ ausgenutzt werden, ist aber durchaus richtig.

Denn um die Überwachungssoftware unbemerkt zu installieren, müssen Sicherheitslücken auf dem Zielgerät bestehen. Und diese werden von den Behörden ausgenutzt. Wenn den Ermittlern eine solche Schwachstelle bekannt wird, werden sie den Hersteller des Gerätes nicht darüber aufklären. Schließlich ist es in ihrem Interesse, dass die Sicherheitslücke weiterbesteht, um auch in Zukunft den Einsatz der Quellen-TKÜ zu ermöglichen. Diese bewusst nicht geschlossenen Sicherheits-lücken können aber auch von Kriminellen genutzt werden (Handelsblatt 2017b).

So etwas ist durchaus schon vorgekommen. Der amerikanische Geheimdienst NSA hatte sich eine Sicherheitslücke im Betriebssystem Windows zunutze gemacht, statt sie Microsoft zu melden, damit der Hersteller sie hätte schließen können. Das Wissen über die Lücke gelangte an die Öffentlichkeit und wurde von Kriminellen missbraucht. Sie starteten im Mai 2017 mit dem Programm „WannaCry“ einen weltweiten Hackerangriff mit erpresserischen Absichten auf Windows-Rechner (Sokolow 2017b).

Die Kritik, dass bei der Quellen-TKÜ Sicherheitslücken von IT-Systemen ausgenutzt werden, ist folglich berechtigt und kaum zu entkräften.

2.6.4 Reichweite der Überwachungsmaßnahmen

Als ebenfalls problematisch an der Quellen-TKÜ erweist sich, dass sie wohl mehr überwacht, als sie darf. Werden in regelmäßigen Abständen Screenshots vom Bildschirm des Überwachten gemacht, bietet dies eine gute Möglichkeit, an die Kommunikationsinhalte zu gelangen, sobald er einen Messenger oder ein Mail-Programm öffnet. Das Problem hierbei ist, dass ein Großteil dieser Screenshots keine Kommunikationsinhalte zeigen dürfte, sondern andere, private Inhalte auf dem Endgerät des Benutzers (BeckOK/Graf StPO § 100a Rn. 107d).

Da auf PCs und gerade auch auf Smartphones viele persönliche Daten wie eigene Fotos und Videos, Online-Banking und individuelle Apps lagern, wäre dies ein Eingriff in den Kernbereich privater Lebensgestaltung. Nach § 100d Abs. 2 StPO sind solche Erkenntnisse, die per Quellen- oder herkömmliche TKÜ erlangt wurden, nicht zu verwerten. Sie müssen unverzüglich gelöscht werden.

Eine Quellen-TKÜ-Software erkennt im Idealfall also, wann der Verdächtige einen Messenger oder einen anderen Kommunikationskanal öffnet, wann er Nachrichten empfängt oder versendet und leitet nur dann Informationen aus. Technisch dürfte das kaum machbar sein (Stempfle 2017).

Das muss es allerdings auch nicht. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind bei der Überwachung zwar nach § 100d Abs. 2 StPO zu löschen; unzulässig macht das die Quellen-TKÜ aber nicht. Denn nur, wenn mit den Überwachungsmaßnahmen ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden können, ist die Quellen-TKÜ nach § 100d Abs. 1 StPO nicht als Ermittlungsmaßnahme zulässig.

3. ONLINE-SCHWARZMÄRKTE

3.1 DER WEG ZUM ONLINE-SCHWARZMARKT

3.1.1 Das Darknet

Um zu verstehen, wie Online-Schwarzmärkte funktionieren, ist es wichtig zu wissen, wo sie zu finden sind. Denn sie sind nicht einfach über das normale Internet zu erreichen. Sie befinden sich im Darknet.

Das gesamte Internet lässt sich grob in zwei Teile untergliedern. An erster Stelle steht das Clearnet; das sind all die Websites, die man mit herkömmlichen Suchmaschinen aufrufen kann. Wenn vom Internet gesprochen wird, ist in der Regel das Clearnet gemeint. Der andere Teil ist das sogenannte Deep Web. Es enthält Websites, die mit Suchmaschinen nicht gefunden werden können, da sie beispielsweise hinter einer Passwortschranke liegen oder den Suchmaschinen keinen Zugriff auf ihre Inhalte erlauben. Das Darknet ist ein Teil des Deep Webs (Mey 2017, S. 12f).

Es lässt sich weder über Safari noch über Firefox, sondern ausschließlich über den sogenannten Tor-Browser erreichen. Dieser ermöglicht das, was das Darknet so besonders macht: Anonymität. Da sich die Nutzer im Darknet dank Verschlüsselungstechnologien und Verschleierung der IP-Adresse weitgehend unerkannt bewegen können, ist es nicht verwunderlich, dass es sich einer gewissen Beliebtheit erfreut (Mey 2017, S. 11).

In Ländern, in denen keine Meinungsfreiheit herrscht und Kritik an der Regierung verboten ist, bieten Diskussionsplattformen im Darknet eine gute Möglichkeit, die staatliche Kontrolle zu umgehen und sich auszutauschen. Doch es finden sich auch viele illegale Inhalte im Darknet: Filesharing-Plattformen, auf denen Filme und Musik verbreitet werden, geleakte Daten, Foren für Hacker. Und Online-Schwarzmärkte (Intelliagg 2016).

3.1.2 Der Tor-Browser

Um ins Darknet zu gelangen, wird der Tor-Browser benötigt. Dieser kann ganz einfach und legal aus dem Clearnet heruntergeladen werden. Tor wird im Grunde verwendet wie Firefox und Safari, mit dem Unterschied, dass Tor es ermöglicht, anonym im Internet zu surfen.

Wenn man mit einem herkömmlichen Browser eine Website aufruft, wird die Verbindung zu der Seite von der eigenen Internetprotokoll-Adresse aus generiert. Der Internet-Provider kann nun anhand der IP-Adresse einsehen, welche Daten auf dieser Verbindung übertragen werden. Die IP-Adresse ist demnach eine Art digitale Wohnadresse, die sich sogar zum tatsächlichen Aufenthaltsort des Nutzers zurückverfolgen lässt. Wer auf Online-Schwarzmärkten einkauft, möchte das natürlich vermeiden. Deshalb fließt der Datenverkehr bei Tor nicht direkt zur Ziel-Website. Er läuft über drei sogenannte Knoten, alle mit eigenen IP-Adressen, die in verschiedenen Ländern sitzen. Eine Verbindung könnte beispielsweise von Deutschland über Russland nach China und von dort über Kanada nach Frankreich laufen. So lässt sich verschleiern, wo die Anfrage abgeschickt wurde, also in welchem Land der Internetnutzer sich befindet (Power 2014, S. 290f).

Konkret funktioniert das folgendermaßen: Die Daten fließen vom Absender zu Tor-Knoten 1, von da zu Tor-Knoten 2 und über Tor-Knoten 3 an die Zielwebsite. Die Knoten werden zufällig ausgewählt. Beim Absenden wird die Datei mit mehreren Verschlüsselungen versehen. Ein jeder Knoten entfernt die jeweils äußerste Verschlüsselung und erfährt so, welches der nächste Knoten ist (Dworschak/Winter 2015, S. 23). Jedem Knoten ist nur der vorherige und der nächste Knoten bekannt (Petrlic/Sorge 2017, S. 55). Bereits Knoten 2 kennt den Absender nicht mehr. Er weiß nur, dass die Daten von Knoten 1 kommen und an Knoten 3 weitergeleitet werden. Dieser dritte Knoten knackt die letzte Verschlüsselung und schickt die Daten an die Zielwebsite. Für diese scheint es, als käme die Anfrage von Knoten 3 (Dworschak/Winter 2015, S. 23). Die ursprüngliche Handlung, wie etwa das Aufrufen einer Website oder das Herunterladen von Content, wird demnach vom dritten und letzten Knoten ausgeführt (Mey 2017, S. 87).

Als zusätzliche Sicherheitsmaßnahme wechseln die Knoten, über die die Verbindung läuft, alle zehn Minuten (Flade et al. 2014). Dadurch wird absolute Anonymität gewährleistet.

Tor steht für „The Onion Router“, „Der Zwiebel-Router“. Der Name veranschaulicht, dass die Verschlüsselungen die Daten wie eine Schale umgeben. Die Knoten entfernen die Schale Schicht um Schicht – wie beim Schälen einer Zwiebel (Hostettler 2017, S. 31).

Passend zum Namen enden im Darknet alle Seiten statt auf .de oder .com auf .onion. Über herkömmliche Browser lassen sich diese Seiten nicht erreichen, .onion funktioniert nur über Tor (Mey 2017, S. 91). Doch Tor ist nicht ausschließlich für das Darknet nutzbar. Wer die Anonymität schätzt, kann damit auch auf ganz normalen Websites im Clearnet surfen. Durch das Umleiten der Daten über drei Knoten und die Verschlüsselungen ist Tor allerdings deutlich langsamer als gewöhnliche Browser (Flade et al. 2014).

3.2 VORTEILE VON ONLINE-SCHWARZMÄRKTEN AUS KUNDENSICHT

3.2.1 Geringes Beschaffungsrisiko

Die Gründe für die wachsende Beliebtheit von Online-Schwarzmärkten sind unter anderem die Vorteile, die sie gegenüber dem Kauf von Betäubungsmitteln auf der Straße bieten.

Anders als auf Online-Schwarzmärkten, wo dem Kaufwilligen viele Händler zur Verfügung stehen, zwischen denen er wählen kann, muss er, wenn er Betäubungsmittel „offline“ kaufen möchte, zunächst jemanden kennen, der damit handelt.

Auch wenn ein Dealer gefunden ist, wird die Übergabe nicht sehr angenehm sein. Die Angst, von der Polizei erwischt zu werden, ist ein ständiger Begleiter. Der Dealer kann den potentiellen Kunden auch überfallen oder ihn betrügen. So könnte er ihm beispielsweise statt Kokain Kreatinpulver verkaufen, ein Nahrungsergänzungsmittel mit der gleichen Optik. Reklamieren kann der Käufer das nicht (Wainwright 2016, S. 219).

Ganz anders sieht es aus, wenn im Darknet eingekauft wird. Wer illegale Ware erwerben möchte, muss nicht einmal das Haus verlassen. Ohne die Angst, überfallen oder auf dem Heimweg nach dem Kauf von der Polizei aufgegriffen zu werden, können Betäubungsmittel und andere verbotene Dinge bequem vom Computer aus bestellt werden (Wainwright 2016, S. 220).

3.2.2 Produktbewertungen

Das Problem, einen Dealer kennen zu müssen, besteht auf Online-Schwarzmärkten nicht. Hier ist es vielmehr so, dass eine riesige Auswahl an Händlern zur Verfügung steht. Dem Käufer stellt sich demnach die Frage, für wen er sich entscheiden soll, denn nicht jeder bietet Produkte von guter Qualität an. Und natürlich gibt es Betrüger. Außerdem läuft alles anonym, die Möglichkeit der Reklamation ist auch auf Online-Schwarzmärkten nicht gegeben. Die Lösung: Kundenrezensionen. Wie bei Amazon und anderen Online-Shops lassen sich Verkäufer und ihre Produkte bewerten. Das gibt den Kunden die Chance, herauszufinden, wer vertrauenswürdig ist. Und die Verkäufer können sich auf diese Weise ein gutes Ansehen verdienen. Ohne diese Produktbewertungen würden anonyme Online-Schwarzmärkte nicht funktionieren, da Anbieter und Kunden einander nicht vertrauen würden (Bartlett 2015, S. 171, 173).

Das Bewerten von Produkten wird rege genutzt. So gab es im Bereich Betäubungsmittel auf dem Online-Schwarzmarkt Silk Road im Juni 2012 über 90.000 Meinungen zu den Anbietern von Kokain. MDMA-Händler sammelten über 60.000 Bewertungen und Verkäufer von LSD 50.000 (Power 2014, S. 296).

3.2.3 Kundenservice

Die Produktbewertungen sind nicht der einzige Kundenservice, den Online-Schwarzmärkte bieten. Die Websites sind meist übersichtlich aufgebaut und klar strukturiert. Es gibt Produktfotos, anhand derer sich der potentielle Käufer ein Bild von der Ware machen kann. Neben den Kundenbewertungen bestehen sogar Community-Foren, in denen sich Kunden und Händler austauschen können, etwa um vor Betrügern zu warnen oder ganz allgemein über diverse Produkte und andere Themen zu diskutieren (Richter 2015).

Wie bei gewöhnlichen Online-Shops lässt sich nach Produktgruppen filtern, etwa nach Waffen, verschreibungspflichtigen Medikamenten oder Betäubungsmitteln. Es kann auch gezielt nach bestimmten Preisspannen gesucht werden. Des Weiteren lassen sich Händler anhand der Länder, in die sie liefern, sortieren und auflisten (Mey 2017, S. 17).

Zusätzlich zu den Bewertungen wird angezeigt, wie viele Transaktionen ein Händler bereits abgeschlossen hat. Aber auch wie viele Käufe ein Kunde bereits getätigt hat, ist ersichtlich. Sowohl Käufer als Anbieter können anhand der Anzahl einschätzen, wie vertrauenswürdig ihr Gegenüber ist. Manche Verkäufer bieten sogar Schadensersatz an, wenn eine Lieferung auf dem Weg verloren geht. Die Höhe der Erstattung richtet sich nach der Anzahl der vom Kunden getätigten Rezensionen. Je mehr es sind, desto besser (Wainwright 2016, S. 230).

Mit diesen vertrauensbildenden Maßnahmen werden Kunden geködert, Händler heben sich dadurch von der Konkurrenz ab. Es ist interessant, wie die Nutzer solcher Plattformen versuchen, seriös und anständig zu wirken, obwohl mit offensichtlich illegalen Waren gehandelt wird. Aber es funktioniert.

Online-Schwarzmärkte ermöglichen es also, dank Kundenservice und der Möglichkeit, Produkte und Anbieter zu vergleichen, Betäubungsmittel von höherer Qualität als auf der Straße zu kaufen – bei einem niedrigeren Beschaffungsrisiko (Bartlett 2015, S. 187).

3.3 WARENANGEBOT UND BETROFFENE STRAFTATBESTÄNDE

3.3.1 Betäubungsmittel § 29 BtMG

Wenn in den Medien über Online-Schwarzmärkte berichtet wird, ist vor allem von Drogen und Waffen die Rede. Tatsächlich machen aber Betäubungsmittel auf den Marktplätzen einen deutlich größeren Anteil aus als Waffen. Sie sind das wohl beliebteste Produkt im Darknet.

Wie bei gewöhnlichen Online-Shops auch, sollen sich die Kunden schnell auf den Seiten zurechtfinden. Deshalb sind die Kategorien, in die die Betäubungsmittel unterteilt werden, auf den meisten Online-Schwarzmärkten ähnlich aufgebaut (Hostettler 2017, S. 78f):

- Benzodiazepine
- Cannabis
- Dissoziativa
- Ecstasy
- Halluzinogene
- Opiate
- Steroide
- Stimulanzien
- Verschreibungspflichtige Medikamente

Betäubungsmittel sind zwar allgemein die beliebtesten Waren auf Online-Schwarzmärkten, doch es gibt einige, die besonders ins Auge fallen. Für eine Studie wurden die meistverkauften Drogen mehrerer Online-Schwarzmärkte im Januar 2016 ermittelt. Gemessen wurden sie an der Gesamtzahl aller verkauften Betäubungs-

mittel. Cannabis war mit 33% aller Transaktionen am gefragtesten. Auf dem zweiten Platz standen verschreibungspflichtige Medikamente mit 19%. Dicht darauf folgten Stimulanzien mit 18%. Ecstasy und Ecstasy-Ähnliche mit 12% lagen dicht bei Halluzinogenen, die 11% aller Betäubungsmittel-Transaktionen ausmachten (Kruithof et al. 2016, S. 57).

Es scheint kaum ein Betäubungsmittel zu geben, das nicht über Online-Marktplätze zu kaufen wäre. Geschuldet ist das unter anderem der hohen Anzahl an Drogenhändlern, die ihre illegalen Waren im Darknet anbieten. Im Januar 2016 gab es alleine in den USA 890 Verkäufer von illegalen Drogen im Darknet. Kein Land wies eine höhere Anzahl auf. In Deutschland waren es 225 Anbieter, nur in den USA und in England mit 338 Verkäufern waren es mehr (RAND Corporation 2017). Es ist zu beachten, dass es sich bei diesen Zahlen nur um die Betäubungsmittel-Händler auf Online-Schwarzmärkten handelt. Personen, die Waffen, Falschgeld und andere illegale Güter anbieten, kommen noch dazu.

Aufgrund dieser Zahlen überrascht es nicht, dass in den USA auch der höchste Umsatz mit Betäubungsmitteln erzielt wird. Im Januar 2016 wurden dort 5 Millionen US-Dollar umgesetzt. Ausgehend davon, dass der Umsatz Monat für Monat konstant bleibt, wären das 60 Millionen US-Dollar im Jahr 2016. Für Deutschland entspräche das nach dieser Rechnung einer Summe von 14,4 Millionen US-Dollar (RAND Corporation 2016). Da die Anzahl an Online-Schwarzmärkten und deren Bekanntheit aber immer weiter zunimmt, ist davon auszugehen, dass der Jahresumsatz von Betäubungsmitteln sogar über den hier errechneten Zahlen liegt.

Grundsätzlich steht auf den Handel mit Betäubungsmitteln nach § 29 Abs. 1 Nr. 1 BtMG eine Freiheitsstrafe von bis zu fünf Jahren oder eine Geldstrafe. Hiervon sind die Käufer auf Online-Schwarzmärkten betroffen. Die Anbieter erwartet eine höhere Strafe; nach § 29 Abs. 3 Nr. 1 BtMG liegt bei ihnen ein besonders schwerer Fall vor, da sie gewerbsmäßig handeln. In diesen Fällen wird eine Freiheitsstrafe von nicht unter einem Jahr verhängt.

Die gleiche Strafe haben die Betreiber von Online-Schwarzmärkten zu erwarten. Auch wenn sie selbst nichts verkaufen, verschaffen sie nach § 29 Abs. 1 Nr. 10 BtMG anderen die Gelegenheit zum unbefugten Kauf und Verkauf von Betäubungsmitteln,

indem sie die Darknet-Seite zur Verfügung stellen. Da auch das gewerbsmäßig geschieht, da sie Provisionen kassieren, ist die Strafe in diesem besonders schweren Fall nach § 29 Abs. 3 Nr. 1 BtMG eine Freiheitsstrafe von nicht unter einem Jahr.

3.3.2 Waffen §§ 51, 52 WaffG, § 22a KrWaffKontrG

Nicht alle Online-Schwarzmärkte bieten sie an, trotzdem gibt es eine Vielzahl an unterschiedlichen Waffen im Darknet. Verkauft werden Pistolen, Automatikfeuerwaffen, Schrotflinten, Sturmgewehre, Munition, Sprengstoffe und umgebaute Gas- und Schreckschusspistolen. Oftmals handelt es sich um ehemals funktionsunfähige Dekorationswaffen, die schussbereit gemacht wurden. Dekorationswaffen dürfen in Deutschland legal gekauft werden und für jemanden der sich auskennt, ist es ein leichtes, sie in scharfe Waffen zu verwandeln (Witsch 2016).

Ein anderer Teil der Waffen wird aus Waffenlieferungen abgezweigt. Da auch der Waffenhandel zwischen Ländern nicht immer legal abläuft, bleiben solche Diebstähle meist ungestraft; korrupte Personen können sich auf diese Weise im Darknet etwas dazuverdienen. Preislich unterscheiden sich die Waffen auf Online-Schwarzmärkten kaum von legal erworbenen. Die Preise für Glock-Pistolen bewegen sich zwischen 1.000 Euro und 1.300 Euro. Sturmgewehre sind deutlich teurer, sie kosten etwa 3.500 Euro (Doll 2017).

Auf den Kauf von vollautomatischen Waffen steht nach § 51 Abs. 1 WaffG eine Freiheitsstrafe von einem bis zu fünf Jahren. Die Verkäufer, die gewerbsmäßig handeln, wodurch ein besonders schwerer Fall vorliegt, erwartet laut § 51 Abs. 2 WaffG eine Freiheitsstrafe von einem bis zu zehn Jahren. Niedriger werden die Käufer von Sprengstoffen bestraft. Nach § 52 Abs. 1 Nr. 1 WaffG beträgt ihre Freiheitsstrafe mindestens sechs Monate und höchstens fünf Jahre. Auf den Handel steht hier aber laut § 52 Abs. 5 WaffG die selbe Strafe wie bei vollautomatischen Waffen: Ein Jahr bis zu zehn Jahre Freiheitsstrafe.

Bei Maschinenpistolen und vollautomatischen Gewehren greift das Kriegswaffenkontrollgesetz. Wer eine solche Kriegswaffe erwirbt oder einem anderen überlässt, in diesem Fall durch den Verkauf, wird nach § 22a Abs. 1 Nr. 2 KrWaffKontrG mit einer Freiheitsstrafe zwischen einem und fünf Jahren bestraft. Wenn, wie im Fall der Verkäufer von Kriegswaffen, durch gewerbsmäßigen Handel ein besonders schwerer Fall vorliegt, beträgt die Freiheitsstrafe laut § 22a Abs. 2 KrWaffKontrG zwischen einem und zehn Jahren. Die Kunden werden unterschiedlich

bestraft, abhängig von der gekauften Waffe. Bei den Händlern, ob sie Sprengstoffe, Maschinenpistolen oder andere vollautomatische Waffen anbieten, bewegt sich das Strafmaß im selben Rahmen.

3.3.3 Falschgeld § 146 StGB

Auch Falschgeld lässt sich leicht über Online-Schwarzmärkte beziehen. Das BKA nimmt an, dass von den 110.000 falschen Euroscheinen, die 2016 beschlagnahmt wurden, dreißig Prozent über das Internet vertrieben wurden. Am häufigsten gefälscht wurden 20-Euro-Scheine und 50-Euro-Scheine (Mey 2017, S. 34).

Auf den ersten Blick mag es verwunderlich scheinen, dass nicht vor allem höherwertige Scheine im Hunderter-Bereich gefälscht werden. Bei wertvolleren Scheinen wird aber eher darauf geachtet, ob sie echt sind, und manche Geschäfte nehmen prinzipiell keine 500-Euro-Scheine an.

Die Preise für Falschgeld hängen stark von der Qualität der Fälschung ab. Schlechte Fälschungen sind aber auf den Online-Schwarzmärkten auch als solche gekennzeichnet und dementsprechend billiger. Auf dem Marktplatz Dream Market im Darknet gibt es beispielsweise zehn 50-Euro-Scheine für 150 Euro zu kaufen. Das sind 500 falsche Euro für 150 echte. Für zwanzig 20-Euro-Scheine sind 105 Euro zu zahlen, 400 falsche für 105 echte Euro (Mey 2017, S. 33).

Laut § 146 Abs. 1 Nr. 2 StGB wird mit Freiheitsstrafe nicht unter einem Jahr bestraft, wer sich falsches Geld beschafft oder es verkauft. Auch hier machen sich sowohl Kunde als auch Verkäufer strafbar. Letztere haben allerdings nach § 146 Abs. 2 StGB mit einer Freiheitsstrafe von mindestens zwei Jahren zu rechnen, da sie gewerbsmäßig handeln.

3.3.4. Weitere Waren

Es gibt viele weitere Produkte, die auf Darknet-Märkten angeboten werden; nicht alle sind illegal. So konnte man auf Silk Road 2.0 beispielsweise auch Bücher, Alkohol und Kunst kaufen (Bartlett 2015, S. 167). Den größten Anteil nehmen dennoch strafrechtlich relevante Waren ein.

Einen guten Überblick über die Produktvielfalt geben die Kategorien auf dem mittlerweile geschlossenen Marktplatz AlphaBay (Hostettler 2017, S. 69f):

- Andere
- Betrug
- Dienstleistungen
- Digitale Produkte
- Drogen & Chemikalien
- Fälschungen
- Juwelen & Gold
- Leitfäden & Tutorials
- Mit fremden Kreditkartendaten gekaufte Gegenstände
- Sicherheit & Hosting
- Software & Malware
- Waffen

3.4 DAS BEZAHLSYSTEM

3.4.1 Die Kryptowährung Bitcoin

Bezahlt wird auf Online-Schwarzmärkten üblicherweise mit Bitcoin. Das ist eine virtuelle Währung, die aus aneinandergereihten digitalen Zeichen besteht. Bitcoin-Transaktionen werden in der Blockchain erfasst, einer Art digitalem, öffentlich einsehbarem Kassenbuch (Sixt 2017, S. 30).

Bitcoin haben einige Vorteile, gerade auch für Online-Schwarzmärkte. Sie bieten sehr schnelle Überweisungen, bei denen keine Gebühren anfallen. Sie sind für jeden zugänglich und legal zu erwerben. Es gibt sogar Banken, die selbst Bitcoin-Börsen betreiben (Hostettler 2017, S. 49).

Allerdings werden die Zahlungsströme an sich von keiner Bank oder einer anderen übergeordneten Stelle kontrolliert. Dieses Fehlen einer überwachenden Instanz macht Bitcoin so attraktiv für illegale Geschäfte auf Online-Schwarzmärkten (Richter 2015). Denn somit besteht auch keine Möglichkeit, einzelne Konten, bei Bitcoin „Wallets“ genannt, zu sperren (Mey 2017, S. 19).

Bei Bitcoin-Überweisungen bleiben die beteiligten Personen unbekannt. Es wird nur die Adresse des Empfängers benötigt. Anders als bei Banküberweisungen, bei denen die Namen der Transaktionspartner genannt werden müssen (Flade et al. 2014). Diese Anonymität ist einer der Hauptgründe, warum illegale Online-Marktplätze auf Bitcoin als Zahlungsmittel setzen.

Zusätzlich lassen sich Bitcoin waschen, etwa mit dem Online-Service „Bitcoin Fog“. Zunächst überweist der User Bitcoin auf die Wallet von „Bitcoin Fog“. Dort wird die Zahlung in mehrere kleine Beträge gestückelt und über andere Bitcoin-Wallets verschoben, bis diese schließlich auf die private Wallet des Nutzers zurückfließen. Auf diese Art lässt sich kaum nachvollziehen, woher die Bitcoin auf seinem Konto stammen (Dworschak/Winter 2015, S. 25).

Vollständige Anonymität ist durch Bitcoin allerdings nicht gewährleistet. Denn in der Blockchain sind alle jemals getätigten Transaktionen einsehbar – für jeden. Da bei den Überweisungen keine Namen genannt werden, geht daraus zwar nicht hervor, zwischen welchen Personen eine Transaktion vollzogen wurde. Aber womöglich können Ermittler anhand der erfolgten Zahlungen die beteiligten Personen ausmachen (Hostettler 2017, S. 54).

Ein Kunde von Online-Schwarzmärkten könnte nun auf die Idee kommen, sich mehrere Wallets anzulegen, um es den Behörden zu erschweren, ihn zu identifizieren. Durch die öffentlich einsehbaren Transaktionen lassen sich für Außenstehende aber Verbindungen herstellen, wenn er Bitcoin zwischen seinen Wallets überweist. Gleiches gilt, wenn er für eine Transaktion mehrere Wallets nutzt, falls das Guthaben auf den Einzelnen alleine nicht hoch genug ist. Und wer seine Bitcoin-Adresse öffentlich mit seinem eigenen Namen in Verbindung bringt, verliert jegliche Anonymität (Petrlic/Sorge 2017, S. 84).

3.4.2 Die Blockchain

Die Blockchain, die Grundlage für Bitcoin, hat keinen zentralen Speicherort. Stattdessen ist sie dezentral in Teilen auf von freiwilligen Privatpersonen zur Verfügung gestellten Rechnern gespeichert. Jede Transaktion wird automatisch vom Netzwerk geprüft, um zu verhindern, dass ein Bitcoin zweimal ausgegeben werden kann. So wird Betrug vorgebeugt (Hostettler 2017, S. 45).

Wenn jemand beispielsweise fünf Bitcoin an einen Dritten überweisen möchte, wird zunächst in der Blockchain geprüft, ob er überhaupt fünf Bitcoin besitzt. Wenn das der Fall ist, kommt es zur Überweisung. Die Informationen über Transaktionen werden als Datenblock gebündelt. Dieser Block wird dann an die Blockchain angehängt (Grassegger 2016, S. 70). Bildlich vorgestellt ist die Blockchain eine lange Kette, bestehend aus aneinandergereihten Datenblöcken voller Information.

Um diese Blöcke zu überprüfen und abzuschließen, ist Rechenleistung vonnöten. Jeder kann hierfür seinen Rechner zur Verfügung stellen. Der Vorgang nennt sich „Minen“. Neben den Blöcken entstehen auch neue Bitcoin, mit denen die Miner für ihre Rechenleistung belohnt werden. Damit es nicht zu einer Inflation kommt, ist die maximale Anzahl von Bitcoin auf 21.000.000 Stück beschränkt (Power 2014, S. 301f).

3.4.3 Die Zahlungsabwicklung

Bei Silk Road, dem ersten großen Online-Schwarzmarkt, überwiesen Käufer ihre Bitcoin auf eine Wallet auf Silk Road. Für jeden Kunden, der sich auf der Seite anmeldete, wurde eine solche Wallet erstellt. Wenn nun etwas gekauft werden sollte, überwies der Kunde die erforderliche Summe auf eine Wallet, die von Silk Road-Administratoren als Treuhandkonto verwendet wurde. Der Verkäufer wurde über den Eingang der Bitcoin informiert und verschickte seine Waren. Wenn diese beim Kunden ankamen, informierte er den Administrator, und dieser überwies die Bitcoin von der Treuhand-Wallet auf die Wallet des Verkäufers. So sollten Betrugsfälle verhindert werden (Bartlett 2015, S. 178).

Allerdings bestand die Gefahr, dass der Seitenbetreiber und seine Administratoren selbst mit dem Geld, dass sie treuhänderisch verwalteten, einfach verschwanden. Niemand hätte sich mit der Bitte um Hilfe an eine höhere Instanz wenden können. Deshalb wurde eine neue Bezahlmethode entwickelt: Die Multi-Signatur-Transaktion. Hierbei werden die Bitcoin in eigens für den Bestellvorgang erstellten Wallets gelagert. Damit sie an den Verkäufer überwiesen werden können, müssen er selbst, der Kunde und der Schwarzmarkt zustimmen. Wenigstens jedoch zwei der drei Teilnehmer. Dadurch wird verhindert, dass eine Partei mit dem Geld verschwindet. Denn alleine kann niemand eine Überweisung auslösen. Falls es zu Unstimmigkeiten kommt, etwa wenn die Ware nicht abgeschickt wird, bekommt der Kunde seine Bitcoin von der Wallet zurückerstattet (Bartlett 2015, S. 179).

Natürlich möchten die Betreiber der Online-Schwarzmärkte an den laufenden Geschäften mitverdienen. Zunächst fordern die Märkte eine Anmeldegebühr von den Verkäufern, nicht aber von den Kunden. Diese fällt unterschiedlich hoch aus, meist bewegt sie sich im niedrigen dreistelligen Euro-Bereich. Nachdem der Verkäufer angemeldet und die Gebühr bezahlt ist, kann er beginnen zu Handeln. Zusätzlich zu den Anmeldegebühren kassiert der Marktplatz für jedes verkaufte Produkt eine Provision. Diese beträgt auf den meisten Darknet-Märkten rund fünf Prozent (Hostettler 2017, S. 79).

3.5 LIEFERUNG DER WARE

3.5.1 Versenden und Empfangen

Grundsätzlich lassen sich die Waren von Online-Schwarzmärkten meist in jedes Land der Welt liefern. Hierbei besteht jedoch die Gefahr, dass der Zoll die Ware konfisziert. Damit die Pakete gar nicht erst durch den Zoll müssen, bestellen viele Kunden bei Händlern, die in ihrem Heimatland ansässig sind. Aufgrund der riesigen Anzahl von Anbietern aus verschiedenen Ländern, lässt sich das leicht bewerkstelligen (Power 2014, S. 298f).

Als Silk Road noch existierte, gab es darauf die folgenden Hinweise zum Empfang von Paketen (Power 2014, S. 285f):

- Nicht den eigenen Namen verwenden.
- Nicht an die eigene Adresse zustellen lassen.
- An ein Postfach oder die Wohnung eines Bekannten liefern lassen.
- Nicht zu einem leer stehenden Haus liefern lassen, das könnte Verdacht erregen.
- Dem Paketservice den Erhalt der Lieferung nicht bestätigen.
- Falls es auffliegt, soll der Kunde behaupten, er hätte das Paket nicht bestellt; denn man kann auch gegen den eigenen Willen etwas zugeschickt bekommen.

Als besonders gut geeignet, sowohl für das Versenden als auch das Empfangen, haben sich die Packstationen der Deutschen Post erwiesen. Ursprünglich haben sie den Zweck, dass die Nutzer ihre Pakete an anderen Orten als zu Hause empfangen können, etwa in der Nähe des Arbeitsortes. Es gibt in Deutschland bereits in 1.600 Städten solche Packstationen, insgesamt sind es 2.750 Stück. Acht Millionen

Menschen sind als Nutzer registriert. Um ein Paket zu verschicken, muss es frankiert und gescannt werden. Dann wird es einfach in eines der Schließfächer der Packstation gelegt. Wer ein Paket verschickt, wird nicht überprüft. Das Versenden läuft demzufolge vollkommen anonym ab. Wer ein Päckchen in Empfang nehmen will braucht eine Nutzerkarte und eine Transaktionsnummer, die per SMS zugeschickt wird. Damit lässt sich das Schließfach öffnen und das Paket kann entnommen werden. Auch hier ist kein Kontakt zu Postmitarbeitern nötig. Für die weitere Anonymisierung kann der Empfänger des Pakets es auch unter falschem Namen annehmen. Etwa durch gefälschte Ausweispapiere bei der Registrierung, oder durch das Kaufen eines Kundenaccounts auf einem Online-Schwarzmarkt. Zwischen zwanzig und dreißig Euro fallen hierfür an. Werden diese Verschleierungsmaßnahmen genutzt, verläuft die gesamte Lieferung, vom Versenden bis zum Empfang, absolut anonym. Deshalb sind Packstationen für Darknet-Marktplätze ein großer Gewinn (Goebel/Berke 2015).

3.5.2 Besonderheiten bei der Verpackung von Betäubungsmitteln

Um Betäubungsmittel möglichst sicher zu verschicken, greifen die Verkäufer auf diverse Methoden zurück. Zunächst verpacken sie die Betäubungsmittel geruchsdicht. So können sie von Drogenspürhunden nicht oder nur schwer entdeckt werden. Damit auch Paketboten und Postmitarbeiter keinen Verdacht schöpfen, wird das äußere Erscheinungsbild des Paketes oft bekannten Firmen nachempfunden. So wirkt die Sendung unverdächtig (Mey 2017, S. 26).

Bei einer anderen Variante werden die Betäubungsmittel zunächst ebenfalls luftdicht verpackt. Danach werden sie in eine DVD-Hülle gelegt, um schließlich in einem passenden Briefumschlag verschickt zu werden (Hostettler 2017, S. 13). Eine beiliegende Grußkarte macht die Täuschung perfekt.

3.5.3 Besonderheiten bei der Verpackung von Waffen

Bei Waffen stellt sich alleine aufgrund ihrer Größe die Frage, wie sie unauffällig per Post zum Empfänger gelangen. Meist werden sie in ihre Einzelteile zerlegt und auf mehrere Pakete aufgeteilt, die einzeln verschickt werden. Bei der Zollkontrolle kann es sein, dass das Paket einen Röntgenscanner passieren muss. Deshalb werden den Waffenteilen vor dem Versand andere Metallteile beigelegt. So sind beim Röntgen keine Umrisse mehr erkennbar, die auf eine Waffe hindeuten könnten. Munition wird ebenfalls zerlegt und in Einzelteilen verschickt. Damit niemand Verdacht schöpft, weil der Empfänger in kurzer Zeit so viele Sendungen erhält, werden diese oft als Bausätze getarnt. Hierfür werden die Pakete einfach mit einheitlichen Logos versehen und wirken auf diese Art und Weise ganz gewöhnlich (Doll 2017).

3.6 BEDEUTENDE ONLINE-SCHWARZMÄRKTE

3.6.1 Silk Road

Silk Road, die Seidenstraße, war der erste große Online-Schwarzmarkt und sicher auch der Bekannteste. Im Jahr 2011 erschien die Seite im Darknet. Sie zog große Aufmerksamkeit auf sich. Zwei Jahre später wurde der Gründer von Silk Road, Ross Ulbricht, verhaftet und die Seite geschlossen (Mey 2017, S. 234). Zu diesem Zeitpunkt waren bei Silk Road knapp eine Million Nutzerkonten registriert. Ross Ulbricht soll durch Provisionen auf der Seite 80 Millionen US-Dollar eingenommen haben (Richter 2015).

Er wurde vor Gericht unter anderem schuldig befunden für die Distribution von Drogen, Verschwörung zum Betrieb einer kriminellen Unternehmung, Verbreitung falscher Identitätsdokumente und Geldwäsche. Im Mai 2015 wurde er dafür zu einer Freiheitsstrafe von zweimal lebenslänglich und zusätzlich 30 Jahren Haft verurteilt (Sixt 2017, S. 159).

3.6.2 Silk Road 2.0

Doch den Darknet-Marktplätzen wurde dadurch kein schwerer Schlag versetzt. Denn schon einen Monat nach der Abschaltung von Silk Road ging Silk Road 2.0 online. Der technische Aufbau beruhte teilweise auf der ersten Version. Allerdings hatte Silk Road seine Vormachtstellung verloren. Konkurrierende Märkte hatten die Chance genutzt und waren gewachsen; es kam zu vielen Neugründungen von Darknet-Marktplätzen (Bartlett 2015, S. 162f).

Trotz der Konkurrenz entsprachen die Umsätze von Silk Road 2.0 bereits nach drei Monaten denen des ersten Silk Road, kurz bevor dieses geschlossen wurde. Doch Silk Road 2.0 existierte nicht lange. Am 6. November 2014, ein Jahr nachdem die Seite im Darknet online gegangen war, wurde sie aus dem Netz genommen. Im Rahmen der Operation „Onymous" gelang es mehreren zusammenarbeitenden Behörden, über 400 Online-Schwarzmärkte zu zerschlagen. Auch Silk Road 2.0 war darunter und der Betreiber der Website, Blake Benthall, wurde festgenommen (Hostettler 2017, S. 116f).

3.6.3 AlphaBay

AlphaBay war der bisher größte Darknet-Marktplatz. Er wuchs sehr schnell. Von September 2015 bis Februar 2017 vergrößerte sich die Anzahl der Angebote in der Kategorie „Drogen & Medikamente" von 16.800 auf 202.500. Zum Vergleich: Silk Road 2.0, der ehemals größte Markt, hatte im Oktober 2014, eine Woche vor seiner Schließung, 14.000 Angebote in der gleichen Kategorie (Hostettler 2017, S. 104).

Gehandelt wurden auf AlphaBay neben Betäubungsmitteln auch Waffen, Juwelen, Falschgeld, Internet-Kundenkonten und gefälschte Ausweispapiere. Es wurden täglich hunderttausende US-Dollar Umsatz gemacht. Im Juni 2017 wurde der Marktplatz geschlossen und der Betreiber verhaftet (Zeit Online 2017). Alexandre Cazes, so sein Name, verfügte über ein Gesamtvermögen von fast 21 Millionen US-Dollar (Spiegel Online 2017). Eine Woche nach seiner Verhaftung erhängte er sich in seiner Zelle (Handelsblatt 2017a).

3.7 BISHERIGE STRAFVERFOLGUNG

3.7.1 Vorgehensweise und Möglichkeiten

Die offensichtlichste Möglichkeit, um gegen Online-Schwarzmärkte vorzugehen, ist ein Verbot von Bitcoin oder Tor. Schließlich basieren die Marktplätze auf diesen Technologien. Wirklich erfolgsversprechend ist das allerdings nicht; schnell würden anderer Kryptowährungen und anonymisierte Browser an deren Stelle treten (Wainwright 2016, S. 226f). Durch den Bitcoin-Boom Ende 2017 sind bereits so viele neue digitale Währungen entstanden, dass ein Bitcoin-Ersatz schnell gefunden ist.

Vielversprechender ist es, dort anzusetzen, wo digitale und reale Welt aufeinandertreffen. Das kann an den Packstationen sein, wo illegale Waren versendet und empfangen werden (Kruithof et al. 2016, S. 90f). Entfällt die Möglichkeit, Pakete anonym zu verschicken und zu erhalten, erschwert das sowohl den Verkäufern, als auch den Kunden die illegalen Aktivitäten. Videoüberwachung an Packstationen ermöglicht es, herauszufinden, ob eine Person auffällig viele Sendungen aufgibt.

Ein anderer Ansatzpunkt zwischen digitaler und realer Welt ist die Beschaffung von Bitcoin. Bevor diese auf Online-Schwarzmärkten ausgegeben werden können, müssen sie zunächst mit echtem Geld gekauft werden. Das geschieht für gewöhnlich auf Bitcoin-Börsen, etwa auf Bitcoin.de oder Coinbase.

Dort ist für den Erwerb zumeist das normale Bankkonto des Käufers hinterlegt. Hier bietet sich für Ermittler die Möglichkeit, eine Bitcoin-Wallet mit einem realen Bankkonto zu verknüpfen und so herauszufinden, wem die Wallet gehört (Mey 2017, S. 21).

Häufig genutzt werden „verdeckte Personalermittlungen“. Hierbei melden sich Ermittler unter falschen Namen auf Darknet-Märkten an und bestellen Waren (Dittert/ Moßbrucker 2017). Durch das Aufnehmen einer Kundenbeziehung erhoffen sie sich, dass die Verkäufer unvorsichtig werden. Es wird versucht ihnen unfreiwillige Hinweise

zu entlocken, die den Ermittlungen nützen können. In Deutschland gibt es strenge Richtlinien, an die sich die Polizisten hierbei halten müssen. So ist es zulässig, dass sie Betäubungsmittel kaufen. Selbst Betäubungsmittel zu verkaufen und tatsächlich zu versenden ist der Polizei hingegen untersagt (Mey 2017, S. 147).

Wenn es den Ermittlungsbehörden gelingt, einen Kunden oder Händler festzunehmen, bietet es sich an, ihn als Kronzeugen zu nutzen. Laut § 46b Abs. 1 StGB kann das Gericht die Strafe eines Täters mildern, wenn durch das freiwillige Offenbaren seines Wissens eine Tat, die im Zusammenhang mit seiner Tat steht, aufgedeckt oder verhindert werden kann. Konkret können die Ermittler in diesem Fall den Account des Betroffenen selbst nutzen und sich als er ausgeben. Das hat den üblichen verdeckten Personalermittlungen gegenüber den Vorteil, dass es sich nicht um einen neuen, sondern um einen bekannten Kunden bzw. Händler handelt, der bereits Geschäfte getätigt hat. Dadurch ergibt sich ein Vertrauensbonus der anderen Nutzer ihm gegenüber, den die Polizei für sich nutzen kann, um weitere Verhaftungen zu ermöglichen (Mey 2017, S. 148).

3.7.2 Ermittlungserfolge

Dass es bei den Ermittlungen Erfolg verspricht, beim Postweg anzusetzen, hat die deutsche Polizei 2015 bewiesen. Beamten observierten eine Packstation in Leipzig. Dort fiel ihnen ein junger Mann auf, der verdächtig oft Pakete verschickte. Bei der Durchsuchung seiner Wohnung stießen die Polizisten auf mehrere hundert Kilogramm Kokain, Haschisch, Ecstasy und LSD. Der 20-Jährige hatte die Betäubungsmittel über Online-Schwarzmärkte vertrieben (Goebel/Berke 2015).

Da die Darknet-Marktplätze ein internationales Problem sind, ist die Zusammenarbeit von Ermittlungsbehörden unterschiedlicher Länder unerlässlich. Gut funktioniert hat das in folgendem Beispiel zwischen Österreich und Deutschland. In Wien wurden 2017 mehrere Männer verhaftet, weil sie Falschgeld auf Darknet-Marktplätzen angeboten und verkauft hatten. Bei der Festnahme gelangten die österreichischen Behörden an eine Kundenliste mit Falschgeldkäufern, die sie an ihre deutschen Kollegen weiterreichten. Mithilfe dieser Informationen wurden in Berlin acht Wohnungen durchsucht, deren Besitzer laut der Kundenliste falsche 50-Euro-Scheine erworben hatten. In einer der Wohnungen entdeckten die Polizeibeamten ein Magazin samt Munition für ein Sturmgewehr (Welt 2017).

Im Bereich Waffen ist die polizeiliche Aufklärungsquote eher niedrig, wenn sie mit der Anzahl an gehandelten Waffen auf Online-Schwarzmärkten verglichen wird. Im Jahr 2015 wurden zwischen zwanzig und dreißig Personen in Deutschland ausfindig gemacht, die im Darknet Waffendelikte begangen hatten. Große mediale Aufmerksamkeit erregte der Fall eines Mechatronik-Studenten aus Schweinfurt. Er hatte Dekorationswaffen aus der Slowakei für rund 200 Euro pro Stück legal erworben. Anschließend hatte er sie scharfgemacht und für bis zu 2.000 Euro pro Stück auf Online-Schwarzmärkten weiterverkauft. Per Post versendete er die Maschinenpistolen an Käufer aus der ganzen Welt. Im Februar 2016 erging sein Urteil: Vier Jahre und drei Monate Haft (Witsch 2016).

In Heidelberg konnte ein weiterer Waffenhändler verhaftet werden. Er hatte mindestens 65 Waffen auf Darknet-Schwarzmärkten vertrieben. Darunter waren Sturmgewehre, Maschinenpistolen und Schrotflinten. Die Polizei wurde auf ihn

aufmerksam, als der Zoll ein Paket aus den USA untersuchte. Es war an ihn adressiert und enthielt einen Musik-Receiver, in dem drei Pistolenläufe verborgen waren. Dem Angeklagten wurde unter anderem gewerbsmäßiger Handel mit Kriegswaffen und automatischen Waffen vorgeworfen (Dorner 2016). Er wurde mit einer Freiheitsstrafe von fünfeinhalb Jahren belegt (Flade/Nagel 2016).

Ein großer Erfolg gelang deutschen Ermittlungsbehörden, als sie gemeinsam mit europäischen Kollegen und dem FBI den Online-Schwarzmarkt Hansa zerschlugen. Dort wurden hauptsächlich Betäubungsmittel, Fälschungen und Juwelen verkauft. Die Betreiber von Hansa, zwei Deutsche, wurden im Zuge der Ermittlungen festgenommen (Handelsblatt 2017a).

3.7.3 Schwierigkeiten bei der Strafverfolgung

Nur einen kleinen Teil der Verbrechen auf Online-Schwarzmärkten gelingt es der Polizei aufzudecken. Denn sie hat mit einigen Schwierigkeiten zu kämpfen. Häufig liegen die Server der Seiten im Ausland; hier haben die inländischen Behörden kaum Handlungsmöglichkeiten. Die verschiedenen Verschlüsselungstechnologien wie die von Tor erschweren es, Standorte von Verkäufern oder der Server herauszufinden. Ein großes Problem ist, dass nicht genug Geld für die Bekämpfung von Online-Schwarzmärkten vorhanden ist. Das Budget eines Landeskriminalamtes für Internetkriminalität macht nur rund fünf Prozent des Gesamtbudgets aus. Um wirksam gegen die Darknet-Märkte vorzugehen und sie zu observieren, wären allerdings große und teure Serveranlagen vonnöten. Auch mangelt es an Spezialisten für IT-Sicherheit, die ebenfalls einen hohen finanziellen Aufwand bedeuten (Gauto 2016).

Ein weiteres Problem ist, dass die Online-Schwarzmärkte es den Kriminellen einfach machen. Vor den Darknet-Märkten brauchten Dealer Kontakte in die Szene. Heutzutage kann jeder, der über einen Computer mit Internetzugang verfügt, im großen Stil Betäubungsmittel an- und verkaufen (Dworschak/Winter 2015, S. 21). Bei den Tätern kann es sich um junge Menschen handeln, die nie zuvor mit dem Gesetz in Konflikt geraten sind. Und die deshalb auch kaum von ihren Mitmenschen verdächtigt werden.

Obwohl es deutlich öfter zu Verhaftungen von Händlern oder Kunden kommt, sind die Betreiber der Darknet-Märkte das Hauptziel der Ermittlungsbehörden. Wenn es gelingt, einen solchen vor Gericht zu stellen, gibt es allerdings eine Unstimmigkeit beim Urteil. Denn das Betreiben von Online-Schwarzmärkten ist in Deutschland kein eigener Straftatbestand. Stattdessen lässt sich den Betreibern nach § 129 StGB die Bildung einer kriminellen Vereinigung vorwerfen (Flade 2017b). Je nach Art der auf dem Marktplatz verkauften Waren können sich die Betreiber aber weiterer Straftaten schuldig machen, auch wenn sie selbst nichts Illegales verkauft haben. Wurden etwa Betäubungsmittel auf der Plattform gehandelt, greift § 29 Abs. 1 Nr. 10 BtMG, da die Betreiber Anderen eine Gelegenheit zum unbefugten Erwerb und zur unbefugten Abgabe von Betäubungsmitteln verschafft haben.

4. NUTZUNG DER QUELLEN-TKÜ ZUR BEKÄMPFUNG VON ONLINE-SCHWARZMÄRKTEN

4.1 MÖGLICHE ZIELPERSONEN

4.1.1 Käufer als Zielpersonen

Bei der Bekämpfung von Online-Schwarzmärkten gibt es verschiedene Zielpersonen, bei denen die Quellen-Telekommunikationsüberwachung angesetzt werden kann. Zunächst kommen die Käufer für die Überwachung in Frage. Sie sind im Vergleich zu den anderen möglichen Zielpersonen, Händlern und Betreibern, am zahlreichsten. Doch auch innerhalb dieser Zielgruppe sind unterschiedliche Arten von Käufern vorhanden.

Es gibt den Endkonsumenten. Er bestellt Betäubungsmittel in kleinen Mengen, Waffen für den Eigengebrauch und Falschgeld, um es selbst auszugeben. Vom Studenten bis zum Pensionär sind Endkonsumenten in jeder Bevölkerungsschicht und jedem Alter zu finden. Eingrenzen lässt sich diese Zielgruppe kaum. Einzig ein gewisses Technikverständnis, um sicher mit Bitcoin und Darknet umgehen zu können, und ein Internetzugang müssen gegeben sein. Heutzutage schließt das aber auch Rentner nicht mehr aus.

Der nächste Käufertypus sind Weiterverkäufer, die sich in zwei Kategorien aufteilen lassen: Weiterverkäufer im Darknet und Weiterverkäufer auf der Straße (Hostettler 2017, S. 128).

Personen, die auf Online-Schwarzmärkten bestellen und die Waren auf der Straße weiterverkaufen, sind vor allem dem Bereich Betäubungsmittel zuzuordnen. Die Drogen werden in großen Mengen bestellt, um Rabatte zu erhalten. Anschließend werden sie gestreckt und zu einem höheren Preis auf der Straße an die Konsumenten verkauft. Dass solche Straßen-Weiterverkäufer auch Schwarzmarkt-produkte wie Waffen und Falschgeld erwerben, ist unwahrscheinlich. Denn anders als bei Betäubungsmitteln gibt es hierfür keinen großen Markt auf der Straße.

Wer auf Online-Schwarzmärkten einkauft, um auf ebensolchen weiterzuverkaufen, kann theoretisch in jedem Bereich aktiv sein, seien es Juwelen, verschreibungspflichtige Medikamente oder gefälschte Produkte. Vorausgesetzt, es findet sich ein Marktplatz, auf dem dieselbe Ware zu einem höheren Preis abgesetzt werden kann. Wirklich sinnvoll ist das aber nur bei Artikeln, die in großen Mengen gekauft billiger sind. Etwa bei Betäubungsmitteln, die der Weiterverkäufer im Kilobereich bestellt, um sie in kleinere Portionen umzupacken und zu einem höheren Preis pro Gramm an Endkonsumenten weiterzuverkaufen. Auch bei Munition für Schusswaffen funktioniert diese Vorgehensweise. Die Besonderheit beim Darknet-Weiterverkäufer ist, dass er alle seine Geschäfte von zu Hause aus abwickeln kann. Er bestellt seine Waren im Internet und verkauft sie auch dort. Lediglich zum Empfangen und Versenden seiner Bestellungen muss er das Haus verlassen. Deshalb ist auch hier keine Eingrenzung auf eine bestimmte soziale Schicht oder Altersgruppe möglich. Jeder Mensch mit Internetzugang kann von Zuhause aus einen Großhandel für illegale Waren aufbauen.

4.1.2 Händler als Zielpersonen

Ein lohnenderes Ziel für die Quellen-TKÜ sind die Händler, da sie in deutlich größerem Umfang Straftaten begehen als Endkonsumenten. Neben den Weiterverkäufern, die gleichermaßen Käufer und Händler sind, gibt es Händler, die ihre Ware nicht aus dem Internet beziehen. Das können Personen sein, die verschreibungspflichtige Medikamente aus Apotheken stehlen oder abzweigen. Zugelassene Waffenhändler, die sich mit dem Darknet-Handel etwas dazuverdienen wollen. Oder ganze Gruppen, die Betäubungsmittel selbst professionell herstellen.

Die meisten Händler legen sich in ihrem Produktangebot auf eine Warengruppe fest (Mey 2017, S. 18). Dass jemand gleichzeitig etwa Schusswaffen und Opiate anbietet, ist unwahrscheinlich.

Die Festnahme eines Händlers bringt oft weitere Chancen auf Ermittlungserfolge mit sich. Anhand von Kundenlisten und Chats lässt sich nachvollziehen, wer bei ihm eingekauft und sich damit ebenfalls strafbar gemacht hat. Wenn der Festgenommene die illegalen Waren seinerseits bestellt hat, besteht die Möglichkeit, über ihn an den Verkäufer zu gelangen und damit einen weiteren Händler zu verhaften. Und wenn die Waren selbst hergestellt wurden, lassen sich Dank der Festnahme ganze Drogenlabore ausheben.

Es ist folglich sinnvoller, mit den Überwachungsmaßnahmen bei den Händlern anzusetzen als bei den Kunden. Nicht nur, weil größere Straftaten aufgedeckt werden können. Sondern auch, weil sich die Kunden oft ohnehin über die Händler identifizieren lassen.

4.1.3 Betreiber als Zielpersonen

Am besten scheint es, wenn es den Ermittlungsbehörden gelingt, einen Betreiber zu verhaften und damit seinen Online-Schwarzmarkt zu zerstören. Anders als bei Händlern ist es jedoch unwahrscheinlich, dass bei ihm Informationen gefunden werden, die zur Verhaftung von Kunden oder Verkäufern führen können. Denn der Betreiber hat für gewöhnlich keinen direkten Kontakt zu den Personen, die seinen Marktplatz nutzen. Er stellt nur die digitale Infrastruktur zur Verfügung. Dafür wird mit seiner Verhaftung ebenjene Infrastruktur zerstört und Kunden und Händlern die Möglichkeit genommen, illegale Güter zu handeln.

Das Problem hierbei ist, dass die Nutzer des Marktplatzes einfach und schnell auf andere Online-Schwarzmärkte umsteigen können. Anders als bei real existierenden Schwarzmärkten oder Umschlagplätzen für verbotene Waren ist dafür kein Ortswechsel nötig. Es muss sich nur mit ein paar Klicks auf einem anderen Darknet-Markt angemeldet werden, und der Handel kann weitergehen. Da es eine Vielzahl an Online-Schwarzmärkten gibt, werden den Kriminellen auch kaum die Alternativen ausgehen.

Die Tatsache, dass viele Betreiber im Ausland sitzen erschwert die Ermittlungen im Allgemeinen und eine erfolgreiche Quellen-Telekommunikationsüberwachung im Speziellen. Den Betreibern ist meist nur beizukommen, indem sich Behörden mehrerer Länder für gemeinsame Ermittlungen zusammenschließen und über Landesgrenzen hinweg agieren.

Die Liquidierung eines Online-Schwarzmarktes und die Verhaftung seines Betreibers sind äußerst medienwirksam und beeindrucken die Öffentlichkeit weit mehr, als wenn ein Kunde oder Verkäufer festgenommen wird. Dennoch sind Händler für die Quellen-TKÜ die geeignetsten Zielpersonen.

4.2 GELTUNGSBEREICH DER QUELLEN-TKÜ

4.2.1 Straftaten im Bereich Betäubungsmittel

Wenn eine Person verdächtig wird, auf Online-Schwarzmärkten aktiv zu sein, heißt das noch nicht zwingend, dass die Quellen-TKÜ eingesetzt werden darf. Laut §100a Abs. 1 Nr. 1 StPO müssen bestimmte Tatsachen den Verdacht begründen, dass die Zielperson eine in §100a Abs. 2 StPO bezeichnete schwere Straftat begangen hat, begehen will oder durch eine andere Straftat vorbereitet hat. Nur dann ist die Quellen-TKÜ zulässig.

Für Straftaten im Bereich Betäubungsmittel greifen §100a Abs. § 2 Nr. 7 Buchstaben a, b StPO. Im Folgenden seien nur die aus diesen Paragraphen hervorgehenden Straftaten genannt, die auf Online-Schwarzmärkten begangen werden.

Laut §100a Abs. 2 Nr. 7 Buchstabe a StPO darf die Quellen-TKÜ angewendet werden, wenn der Verdächtige nach §29 Abs. 3 Satz 2 Nr. 1 BtMG eine Straftat in besonders schwerem Fall begangen hat. Ein besonders schwerer Fall liegt vor, wenn ein Handel mit Betäubungsmitteln nach §29 Abs. 1 Nr. 1 BtMG gewerbsmäßig ausgeübt wird.

Auch das gewerbsmäßige Betreiben eines Online-Schwarzmarktes gilt als schwere Straftat, wenn nach §29 Abs. 1 Nr. 10 BtMG hierdurch eine Gelegenheit geschaffen wurde, um mit Betäubungsmitteln zu handeln.

Der §100a Abs. 2 Nr. 7 Buchstabe b StPO lässt eine Quellen-TKÜ zu, wenn die betroffene Person verdächtig wird, nach §29a Abs. 1 Nr. 2 BtMG mit einer nicht geringen Menge Betäubungsmittel Handel zu treiben, sie ohne Erlaubnis zu besitzen oder sie herzustellen. Ebenfalls zulässig ist die Quellen-TKÜ wenn ein Verdacht besteht, eine Person führe nach §30 Abs. 1 Nr. 4 BtMG Betäubungsmittel in nicht geringer Menge ins Land ein. Das trifft zu, wenn der Verkäufer der Drogen im

Ausland sitzt und nach Deutschland liefert. Wird jemand verdächtigt, nach §29a Abs. 1 Nr. 1 BtMG als Person über 21 Jahre an jemanden, der noch nicht volljährig ist, Betäubungsmittel abzugeben und dabei nach §30 Abs. 1 Nr. 1 BtMG gewerbsmäßig zu handeln, ist eine Quellen-TKÜ ebenso möglich. Dieser Verdacht kann ohne Zweifel jedem Drogenhändler auf Online-Schwarzmärkten unterstellt werden, da diese aufgrund der Anonymität besagter Schwarzmärkte nicht wissen können, wie alt ihre Kunden sind.

Zusammenfassend lässt sich festhalten, dass die Quellen-TKÜ immer angewendet werden kann, wenn jemand im Verdacht steht, auf Darknet-Märkten mit Betäubungsmitteln zu tun zu haben. Ob Kunde, Verkäufer oder Betreiber. Jeder lässt sich verdächtigen, eine Straftat begangen zu haben, durch die eine Quellen-TKÜ zulässig wird. Sei es der gewerbliche Handel, der Handel mit nicht geringen Mengen, das Einführen von Betäubungsmittel oder das zur Verfügung stellen der Gelegenheit zum Handeln für Dritte.

4.2.2 Straftaten im Bereich Waffen

Beim Verdacht auf den Kauf von vollautomatischen Waffen nach §51 Abs. 1 WaffG und den gewerblichen Handel damit nach §51 Abs. 2 WaffG ist §100a Abs. 2 Nr. 11 Buchstabe a StPO betroffen, womit die Quellen-TKÜ erlaubt ist. Wenn der Verdacht besteht, dass nach §52 Abs. 1 Nr. 1 WaffG Sprengstoffe hergestellt, erworben oder verkauft werden, ist es §100a Abs. 2 Nr. 11 Buchstabe b StPO, der die Quellen-Telekommunikationsüberwachung ermöglicht.

Auch, wenn auf einem Online-Schwarzmarkt mit Kriegswaffen gehandelt wird, lässt sich die Quellen-TKÜ einsetzen. Sie wird durch §100a Abs. 2 Nr. 9 Buchstabe b StPO legitimiert, wenn eine Person verdächtigt wird, nach §22a Abs. 1 Nr. 2 KrWaffKontrG vollautomatische Gewehre, Maschinenpistolen oder Maschinengewehre zu kaufen oder zu verkaufen.

Der Geltungsbereich der Quellen-TKÜ im Bezug auf Online-Schwarzmärkte erstreckt sich somit neben den Betäubungsmitteln auch auf Waffen und Kriegswaffen. Es finden sich zwar deutlich mehr Betäubungsmittelhändler im Darknet, da von Waffenhändlern jedoch die größere Gefahr ausgeht, ist es sehr sinnvoll, dass die Quellen-Telekommunikationsüberwachung auch in diesem Bereich zum Einsatz kommt.

4.2.3 Weitere Straftaten auf Online-Schwarzmärkten

Auch bei einigen anderen Straftaten, die auf Online-Schwarzmärkten begangen werden, kann die Quellen-Telekommunikationsüberwachung zum Einsatz kommen.

Etwa wenn jemand verdächtigt wird, sich auf einem Darknet-Marktplatz nach §146 Abs. 1 Nr. 2 StGB Falschgeld in der Absicht zu kaufen, es als echt in Verkehr zu bringen, oder welches zum Kauf anzubieten. Hier greift §100a Abs. 2 Nr. 1 Buchstabe e StPO, betroffen wären Händler und Käufer, nicht aber die Betreiber des Online-Schwarzmarktes.

Beim Verschaffen von falschen amtlichen Ausweisen nach §276 Abs. 1 Nr. 2 StGB kann die Quellen-TKÜ ebenfalls eingesetzt werden. Wenn bestimmte Tatsachen darauf hinweisen, dass der zu Überwachende einen falschen amtlichen Ausweis, der zur Täuschung im Rechtsverkehr geeignet ist, gekauft hat oder zu kaufen beabsichtigt oder solche verkauft, betrifft das §100a Abs. 2 Nr. 1 Buchstabe q StPO. Falsche amtliche Ausweise werden oft auf Online-Schwarzmärkten angeboten, etwa gefälschte Personalausweise und Führerscheine.

Auch bei Hehlerei lässt sich die Quellen-TKÜ anwenden, allerdings muss es gewerbsmäßige Hehlerei nach §260 Abs. 1 Nr. 1 StGB sein, damit §100a Abs. 2 Nr. 1 Buchstabe l StPO greift. Bei Hehlerei, die nicht gewerbsmäßig stattfindet, darf die Quellen-TKÜ nicht eingesetzt werden. Das bedeutet, dass die Quellen-TKÜ nur auf Leute angewendet werden darf, die im Verdacht stehen, mit gestohlenen Gegenständen, etwa Schmuck und Juwelen, zu handeln. Käufer solcher Hehlerware dürfen nicht überwacht werden.

Insgesamt lässt sich die Quellen-Telekommunikationsüberwachung bei nahezu allen auf Online-Schwarzmärkten begangenen Straftatbeständen nutzen. In ihrem großen Geltungsbereich muss dennoch zwischen Händlern, Käufern und Betreibern unterschieden werden. Zwar ist die Überwachung bei Straftaten aus dem Bereich Betäubungsmittel bei jeder der drei genannten Zielpersonen anwendbar. Beim Verdacht auf Falschgelddelikte sind aber nur noch Kunden und Händler als Zielpersonen für die Quellen-TKÜ möglich, während bei gewerbsmäßiger Hehlerei ausschließlich die Verkäufer überwacht werden dürfen.

4.3 IDENTIFIZIEREN VON VERDÄCHTIGEN

Damit die Quellen-TKÜ angewendet werden kann, muss eine Zielperson identifiziert werden. Doch es kann sich als schwierig erweisen, jemanden zu ermitteln, der auf Online-Schwarzmärkten im Darknet aktiv ist.

Am auffälligsten sind sicherlich Personen, die sehr häufig an Packstationen Pakete aufgeben und empfangen. Wenn diese Personen keinem Beruf nachgehen, der dieses Verhalten erklärt, dürfte das für eine Anwendung der Quellen-Telekommunikationsüberwachung ausreichend sein. Das Problem hierbei ist aber das Beobachten dieses Umstandes. Denn anders als in Post-Filialen gibt es bei Packstationen kein Personal. Es sind folglich keine Angestellten vor Ort, die ein auffälliges Verhalten beobachten und der Polizei melden könnten. Video-überwachung könnte hier Abhilfe schaffen. Allerdings ist das bei 2.750 Packstationen in Deutschland allein aus finanzieller Sicht kaum durchführbar. Die Ermittlungs-behörden können hier nur auf Hinweise aufmerksamer Anwohner hoffen, um daraufhin eine Observation der betroffenen Packstation einzuleiten.

Wenn der Zoll ein Paket entdeckt, das illegale Waren enthält, sind die bestimmten verdachtsbegründenden Tatsachen sofort gegeben. Eine Überwachung von sowohl dem Empfänger als auch dem Absender mittels Quellen-TKÜ-Software ist zulässig. Allerdings wird sie in solchen Fällen nicht notwendig sein, da etwa Falschgeld oder verbotene Substanzen in einem Paket nach §102 StPO bereits eine Wohnungsdurchsuchung bei den betroffenen Personen rechtfertigen. Eine Quellen-Telekommunikationsüberwachung durchzuführen ist hier folglich überflüssig.

Die beste Möglichkeit, Verdächtige für die Quellen-TKÜ zu identifizieren, sind Hinweise von bereits festgenommenen Händlern. Über Lieferadressen, Kundenlisten und Aussagen des Verhafteten lassen sich im besten Fall mehrere Verdächtige ausmachen. Das können Kunden, aber auch andere Händler sein.

Gerade wenn es andere Verkäufer sind, macht eine Quellen-Telekomm-unikationsüberwachung dieser Personen Sinn. Denn hier kann die Überwachung der

Kommunikation weitere Nutzer von Online-Schwarzmärkten offenbaren, die bei ihnen einkaufen. Bei einer sofortigen Wohnungsdurchsuchung besteht die Chance, die bisherigen Kunden zu identifizieren. Wird aber zunächst eine verdeckte Quellen-Telekommunikationsüberwachung durchgeführt, können noch mehr Straftäter angeklagt werden. Schließlich wird die Handelstätigkeit des Verkäufers nicht sofort unterbunden, sondern läuft zunächst unter Beobachtung der Ermittler weiter. Diese können Informationen über weitere, neue Kunden sammeln, bevor sie die Verdächtigen verhaften.

Sobald die Quellen-Telekommunikation eingesetzt ist, eignet sie sich folglich gut, um weitere Verdächtige für Überwachungsmaßnahmen zu identifizieren. Die Suche nach der ersten Person, bei der sie angewendet werden kann, gestaltet sich allerdings problematisch.

4.4 INSTALLIEREN DER ÜBERWACHUNGSSOFTWARE

Wenn nun die Zielperson ausgemacht ist, gilt es, die Quellen-TKÜ-Software unbemerkt auf deren informationstechnischem System zu installieren. Das kann der Computer oder das mobile Endgerät sein. Es ist zu vermuten, dass die meisten Nutzer von Online-Schwarzmärkten per Computer darauf zugreifen um mit anderen Kunden und Händlern zu kommunizieren. Da Tor aber auch auf mobilen Endgeräten nutzbar ist, kann man auf diesem Weg ebenfalls ins Darknet gelangen.

Beim Versuch, die Überwachungssoftware auf einem Computer zu installieren, zeigt sich ein großes Problem. Selbst wenn die Zielperson mit Namen und Wohnadresse bekannt ist, wird es kaum möglich sein, die Kommunikation auf ihrem PC mittels Quellen-TKÜ auszulesen. Denn für die Installation der Überwachungssoftware darf die Wohnung des Verdächtigen nicht betreten werden (BT-Drs. 18/12785, S. 52). Eine technische Lösung mittels Ferninstallation scheidet ebenfalls aus. Schließlich ist der Computer bei Zugriffen auf Darknet-Märkte durch Tor geschützt und anonymisiert, sodass den Ermittlern nicht einmal die IP-Adresse des Gerätes bekannt ist. Eine Installation ist nur möglich, wenn es sich beim Computer der Zielperson um einen Laptop handelt. Wenn der Verdächtige mit diesem außerhalb seiner Wohnung unterwegs ist, bietet sich den Ermittlern die Möglichkeit, die Software mithilfe kriminalistischer List aufzuspielen.

Anders stehen die Erfolgschancen, wenn ein Mobiltelefon überwacht werden soll. Ist der Verdächtige an einer Packstation ins Visier der Ermittler geraten, scheint es naheliegend, in dort abzupassen. Ein Polizeibeamter in Zivil kann die Zielperson in ein Gespräch verwickeln und dadurch ablenken, während ein zweiter Polizist dem Verdächtigen das Mobiltelefon unbemerkt abnimmt, um die Überwachungssoftware darauf zu installieren.

Allerdings wird diese Methode kaum funktionieren. Denn liegen die Behörden mit ihrem Verdacht richtig, dann ist der Betroffene gerade dabei, an der Packstation

illegale Waren zu versenden oder abzuholen. Dementsprechend nervös wird er sein und das ablenkende Gespräch, in das er verwickelt werden soll, schnell abbrechen. Es ist unwahrscheinlich, dass es einem Beamten in einer solchen Situation gelingen kann, das mobile Endgerät zu entwenden, die Software zu installieren und es dem Verdächtigen zurückzugeben, ohne dass dieser etwas davon mitbekommt.

Erfolgsversprechender ist es, einen Verdächtigen in seinem Alltag zu observieren und zu verfolgen. Sobald er sich an einem Ort befindet, der geeignet erscheint, kann die Installation stattfinden. Als solcher Ort bietet sich beispielsweise eine Bibliothek an. Hier ist der Verdächtige mit Literatur abgelenkt und denkt nicht an die von ihm begangenen Straftaten. In einer entspannten Situation ist er deutlich unvorsichtiger und gibt damit ein leichteres Ziel für die Beamten ab, die nun die Quellen-TKÜ-Software auf sein Mobiltelefon laden können.

Insgesamt stellt die Installation der Überwachungssoftware ein großes Problem dar. Zwar ist sie bei mobilen Endgeräten und Laptops durchaus möglich, wenn auch schwierig in der Umsetzung. Bei stationären PCs hingegen ist sie so gut wie gar nicht durchführbar. Umso problematischer, dass vermutlich genau über diese Geräte die meiste Kommunikation innerhalb von Online-Schwarzmärkten läuft.

4.5 ÜBERWACHEN DER KOMMUNIKATIONSKANÄLE

Sobald die Quellen-TKÜ-Software installiert ist, gilt es die Kommunikation des Verdächtigen auszulesen. Damit Kunden, Betreiber und Händler miteinander in Kontakt treten können, gibt es verschiede Kanäle im Darknet (Hostettler 2017, S. 80f):

- *Bitmessage* ist ein Messenger, mit dem sich verschlüsselte Nachrichten verschicken lassen.
- In den *Foren* auf Online-Schwarzmärkten tauschen sich vor allem Kunden untereinander aus. Auch die Betreiber der Marktplätze wenden sich über Foren manchmal an die Allgemeinheit.
- *PM* sind Nachrichten, die sich angemeldete Nutzer untereinander über ihre Profile zuschicken können. Ein eigener Kommunikationskanal der Online-Schwarzmärkte.
- Beim Chatdienst *Tor-Chat* lässt sich nur schreiben, wenn Sender und Empfänger gleichzeitig online sind.
- Unter *Tor-Mail* versteht man E-Mail-Anwendungen, auf die nur über Tor zugegriffen werden kann.

Es bieten sich somit zahlreiche Kommunikationsmöglichkeiten für die Zielpersonen. Bei den Foren ist eine Quellen-TKÜ unnötig, da Forenbeiträge öffentlich einsehbar sind. Wenn der Benutzername des Verdächtigen bekannt ist, lassen sich seine Einträge auch ohne Überwachungsmaßnahmen einsehen. Die strafrechtlich relevanteren Kommunikationsinhalte finden allerdings auf den anderen Kanälen statt.

Da Bitmessage, PMs, Tor-Chat und Tor-Mail Verschlüsselung nutzen, kann die Quellen-Telekommunikationsüberwachung hier sinnvoll zum Einsatz kommen. Für das

Überwachen des Schriftverkehrs sind die beiden bekanntesten Möglichkeiten Key-Logger und das regelmäßige Erstellen von Screenshots durch die Quellen-TKÜ-Software.

Allerdings eignen sich Key-Logger hier nur bedingt. Sie zeichnen zwar alle Tastatureinschläge auf, die an dem überwachten Gerät gemacht werden. Die Kommunikationsinhalte, die von der Partei ausgehen, mit der der Verdächtige in Kontakt steht, bleiben jedoch unbekannt.

Die Überwachungsmaßnahmen liefern lediglich ein unfertiges, halbes Gespräch, bei dem die Aussagen der anderen Partei vollkommen fehlen. Und das, obwohl laut §100a Abs. 3 StPO die Überwachungsmaßnahme auch auf Personen ausgeweitet werden darf, die vom Verdächtigen herrührende Mitteilungen entgegennehmen.

Die Kommunikationsinhalte per Screenshot-Überwachung auszulesen erweist sich als die bessere Wahl, da diese beim Eingeben und Empfangen unverschlüsselt auf dem Bildschirm zu sehen sind. Die regelmäßig von der Quellen-TKÜ-Software angefertigten Bilder liefern die komplette Kommunikation – auch wenn sie über verschlüsselte Messenger wie Bitmessage geführt wird.

Sobald die Quellen-TKÜ-Software also auf dem Endgerät des Verdächtigen installiert ist, lassen sich mit ihrer Hilfe sämtliche Online-Schwarzmärkte betreffende Kommunikationsinhalte auslesen. Egal, ob die Kommunikation über Tor oder direkt über den Darknet-Marktplatz läuft. Voraussetzung ist nur der Einsatz der richtigen technischen Überwachungsmethode.

5. AUSBLICK UND FAZIT

5.1 DAS FAZIT

5.1.1 Zusammenfassung

Zusammenfassend lässt sich sagen, dass die Händler auf Online-Schwarzmärkten die geeignetsten Zielpersonen für die Quellen-TKÜ sind. Die Betreiber sind nur sehr schwer als Verdächtige auszumachen, und die Kunden lassen sich oft ohnehin über die Händler identifizieren.

Der Geltungsbereich der Quellen-TKÜ erstreckt sich über beinahe jedes auf Darknet-Marktplätzen illegal gehandelte Gut. Bei Betäubungsmitteln sind die Überwachungsmaßnahmen immer zulässig. Allerdings muss bei anderen Waren, wie etwa bei Falschgeld und Hehlerware, zwischen Betreiber, Händler und Kunde unterschieden und einzeln geprüft werden, ob die Anwendung der Quellen-TKÜ bei dem betroffenen Verdächtigen zulässig ist.

Die größte Schwierigkeit liegt darin, konkrete Personen als Ziele für die Quellen-TKÜ zu identifizieren. Wenn solche jedoch einmal ermittelt sind, lassen sich durch die Überwachungsmaßnahmen leicht weitere Verdächtige in ihrem Umfeld ausmachen.

Ein großes Problem stellt die Installation der Überwachungssoftware dar. Das Installieren auf mobilen Endgeräten gestaltet sich schwierig, ist aber durchaus machbar. Doch es ist anzunehmen, dass der Großteil der Kommunikation auf Online-Schwarzmärkten über stationäre PCs läuft. Und hier ist die Installation der Software praktisch nicht möglich.

Sobald die Quellen-Telekommunikationsüberwachungssoftware aber auf dem betreffenden Gerät eingerichtet ist, und die richtigen technischen Überwachungsmethoden angewandt werden, lassen sich mit ihrer Hilfe sämtliche Kommunikationsinhalte auslesen. Selbst wenn diese verschlüsselt sind oder mithilfe von Tor anonymisiert werden.

5.1.2 Beantwortung der forschungsleitenden Frage

Abschließend muss gesagt werden, dass die Quellen-Telekommunikations-überwachung in Bezug auf die Bekämpfung von Online-Schwarzmärkten keine sinnvolle Maßnahme darstellt. In der Theorie scheint sie zwar gut geeignet; doch zu groß sind die praktischen Hürden bei der Identifizierung von Verdächtigen und der Installation.

Für eine sinnvolle Anwendung der Quellen-TKÜ in Bezug auf Online-Schwarzmärkte müsste folgendes Szenario gegeben sein: Eine namentlich bekannte Person müsste im Verdacht stehen, sich als Händler illegaler Waren im Darknet zu betätigen. Allerdings dürften die Behörden gegen den Verdächtigen nicht genug in der Hand haben, um eine Festnahme oder eine Hausdurchsuchung zu erwirken, da dann die Quellen-TKÜ überflüssig wäre. Des Weiteren müsste die IP-Adresse des Rechners bekannt sein, über den die Darknet-Geschäfte getätigt werden, um eine Ferninstallation zu ermöglichen; oder es müsste sich um einen Laptop handeln, den die Zielperson häufig außerhalb ihrer Wohnung mit sich trägt.

Wenn diese Voraussetzungen erfüllt sind, lassen sich mittels Quellen-TKÜ ausreichend Beweise für die Schuld des Verdächtigen sammeln; auch seine Kunden können identifiziert werden.

Doch die Wahrscheinlichkeit, dass die Bedingungen für dieses Szenario erfüllt werden, ist sehr gering. Es wird sicherlich ab und zu vorkommen, jedoch nicht oft genug, um die Quellen-Telekommunikationsüberwachung als ein sinnvolles Werkzeug im Kampf gegen Online-Schwarzmärkte bezeichnen zu können.

5.2 EIN AUSBLICK

5.2.1 Die neue Behörde ZITiS

Dennoch wird viel getan im Kampf gegen Internet-Kriminalität. So wurde eine neue Behörde gegründet, die am 6. April 2017 ihre Arbeit aufnahm. Die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“, kurz ZITiS, ist eine F&E-Behörde. Sie entwickelt technische Werkzeuge und Methoden zur Bekämpfung von Cyber-kriminalität und Terrorismus, um damit die Sicherheitsbehörden zu unterstützen und ihr zentraler Ansprechpartner in Cyber-Fragen zu sein. Aufgaben von ZITiS sind unter anderem digitale Forensik, Kryptoanalyse und Telekommunikationsüberwachung (BMI 2017).

Die Einführung der Quellen-TKÜ ist demnach nicht die einzige Maßnahme des Staates, um gegen die zunehmende Nutzung von Verschlüsselungstechnologie unter Kriminellen vorzugehen.

5.2.2 Der Online-Marktplatz OpenBazaar

Im Bereich der Online-Schwarzmärkte könnte es bald zu gravierenden Veränderungen kommen. Der Grund dafür ist OpenBazaar. Hierbei handelt es sich um einen bereits bestehenden Online-Marktplatz, an welchem aber noch gearbeitet wird. Anders als bei herkömmlichen Online-Shops und Online-Schwarzmärkten gibt es bei OpenBazaar keinen Betreiber. Jeder der teilnehmen möchte, installiert sich das Programm und kann daraufhin Produkte anderer Teilnehmer ansehen und selbst welche Anbieten. OpenBazaar ist dezentral gespeichert, verteilt auf den Rechnern der Personen, die das Programm installiert haben. Es gibt folglich keine zentralen Server, wie es bei Darknet-Märkten der Fall ist. Wer ein Produkt kaufen möchte, tritt direkt mit dem Verkäufer in Kontakt, bezahlt wird in Bitcoin. Da kein Betreiber als zwischengeschaltete Instanz beteiligt ist, fallen auch keine Gebühren an. Ähnlich wie beim Multisignatur-System von Online-Schwarzmärkten, müssen zwei von drei Personen zustimmen, damit eine Überweisung freigegeben wird. Neben Käufer und Verkäufer ist der Dritte in diesem Fall aber nicht der Betreiber, sondern ein von Kunde und Händler ausgewählter OpenBazaar-Nutzer, der als Vertrauensperson fungiert (Hostettler 2017, S. 148f).

OpenBazaar hat das Potential, zu einem Online-Schwarzmarkt zu werden, der alle anderen überschattet. Denn es gibt keinen Administrator, mit dessen Verhaftung der Marktplatz zerschlagen werden kann. Es gibt keine Server, die heruntergefahren werden können. Damit ist der Marktplatz praktisch unzerstörbar (Hostettler 2017, S. 150).

Sobald begonnen wird, auf OpenBazaar im großen Stil mit illegalen Waren zu handeln, kann der Kampf gegen Online-Schwarzmärkte demnach als verloren betrachtet werden.

LITERATURVERZEICHNIS

Abate, Constantin: Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail: Einfluss rechtlicher und technischer Entwicklungen auf verdeckte Online-Ermittlungen zur Gewährleistung der Inneren Sicherheit, in: Datenschutz und Datensicherheit, Heft 2, Februar 2011, S. 122-125.

Bartlett, Jamie: The Dark Net: Unterwegs in den dunklen Kanälen der digitalen Unterwelt, 1. Auflage, 2015, Kulmbach: Plassen Verlag.

Beukelmann, Stephan: Online-Durchsuchung und Quellen-TKÜ, in: NJW-Spezial, Heft 14, Juli 2017, S. 440.

Beuth, Patrick/Biermann, Kai: Dein trojanischer Freund und Helfer, 22.06.2017, http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss/komplettansicht, abgerufen am 01.10.2017.

Bode, Thomas A.: Verdeckte strafprozessuale Ermittlungsmaßnahmen, 1. Auflage, 2012, Heidelberg: Springer.

Buermeyer, Ulf: Technische Grundlagen und rechtliche Grenzen der Quellen-Telekommunikationsüberwachung, insbesondere: Der Begriff der "laufenden Kommunikation" im Sinne der Online-Durchsuchungs-Entscheidung - Beitrag zum 37. Strafverteidigertag, Freiburg, 2013, http://www.strafverteidigervereinigungen.org/Material/Themen/Technik%20&%20Ueberwachung/37_buermeyer.html, abgerufen am 16.09.2017.

Bundesministerium des Innern (Hrsg.): Zentrale Stelle für Informationstechnik im Sicherheitsbereich, 2017, https://www.bmi.bund.de/SharedDocs/behoerden/DE/zitis.html;jsessionid=1214E92315E2A78E2A60C84C502263B9.2_cid287, abgerufen am 13.10.2017.

Deutscher Bundestag: Drucksache 18/12785, 20.06.2017, Köln: Bundesanzeiger Verlag.

Dittert, Annette/Moßbrucker, Daniel: Reise in den digitalen Untergrund, 08.01.2017, www.tagesschau.de/inland/darknet-reise-in-die-digitale-unterwelt-101.html, abgerufen am 02.10.2017.

Doll, Nikolaus: Jeder kann sich hier eine Schusswaffe besorgen, 01.08.2017, https://www.welt.de/wirtschaft/article157438899/Jeder-kann-sich-hier-eine-Schusswaffe-besorgen.html, abgerufen am 02.10.2017.

Dorner, Christoph: Waffenhandel im Darknet unter dem Pseudonym "Dosensuppe", 26. Juli 2016, http://www.sueddeutsche.de/panorama/prozess-waffenhandel-im-darknet-unter-dem-pseudonym-dosensuppe-1.3095306, abgerufen am 02.10.2017.

Dworschak, Manfred/Winter, Steffen: Der Prinz des Darknet, in: Der Spiegel, Heft 34, August 2015, S. 20-26.

Flade, Florian: Bei WhatsApp muss der Staat selbst zum Hacker werden, 19.06.2017a, https://www.welt.de/politik/deutschland/article165688690/Bei-WhatsApp-und-Co-muss-der-Staat-selbst-zum-Hacker-werden.html, abgerufen am 02.07.2017.

Flade, Florian: Mit Steinzeitwaffen gegen die Gefahr aus dem Netz, 05.08.2017b, https://www.welt.de/wirtschaft/article167399107/Mit-Steinzeitwaffen-gegen-die-Gefahr-aus-dem-Netz.html, abgerufen am 02.10.2017.

Flade, Florian/Fuest, Benedikt/Nagel, Lars-Marten/Schlesier, Vanessa: Auf den dunklen Seiten des Netzes, 23.02.2014, https://www.welt.de/print/wams/article125110520/Auf-den-dunklen-Seiten-des-Netzes.html, abgerufen am 02.10.2017.

Flade, Florian/Nagel, Lars-M.: Die Kalaschnikow kommt mit der Post, 31.07.2016, https://www.welt.de/print/wams/politik/article157408767/Die-Kalaschnikow-kommt-mit-der-Post.html, abgerufen am 02.10.2017.

Freiling, Felix: Staatliche Spähsoftware zur Strafverfolgung, in: Informatik Spektrum, Heft 3, Juni 2016, S. 203-209.

Gauto, Anna: Auf Shoppingtour im Darknet, 26.07.2016, http://www.wiwo.de/politik/ausland/heroin-kinder-waffen-auf-shoppingtour-im-darknet/13927184.html, abgerufen am 02.10.2017.

Goebel, Jacqueline/Berke, Jürgen: Wie Kriminelle die Packstation missbrauchen, 22.12.2015, http://www.wiwo.de/unternehmen/dienstleister/deutsche-post-wie-kriminelle-die-packstation-missbrauchen/12734012-all.html, abgerufen am 13.10.2017

Graf, Jürgen-Peter (Hrsg.): Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 27. Ed., 01.01.2017, München: Verlag C.H. Beck. Zitiert als "BeckOK/Bearbeiter".

Grassegger, Hannes: Der digitale Lenin, in: Capital, Heft 1, Januar 2016, S. 62-70.

Grunert, Marlene: Durch die Hintertür zur Online-Überwachung, 22.06.2017, http://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html#void, abgerufen am 01.10.2017.

Handelsblatt (Hrsg.): Ermittlern glückt Schlag gegen Darknet-Handel, 20.07.2017a, http://www.handelsblatt.com/technik/it-internet/alphabay-ausgehoben-ermittlern-glueckt-schlag-gegen-darknet-handel/20089510.html, abgerufen am 01.10.2017.

Handelsblatt (Hrsg.): So soll der Staatstrojaner bei WhatsApp mitlesen, 22.06.2017b, http://www.handelsblatt.com/politik/deutschland/ueberwachungsgesetz-im-bundestag-so-soll-der-staatstrojaner-bei-whatsapp-mitlesen/19965814.html, abgerufen am 01.10.2017.

Hostettler, Otto: Darknet: Die Schattenwelt des Internets, 1. Auflage, 2017, Zürich: NZZ Libro.

Intelliagg: Das ist im Darknet drin, zitiert nach de.statista.com, 27.02.2016, https://de.statista.com/infografik/5349/verteilung-von-inhalten-im-tor-netzwerk/, abgerufen am 29.09.2017.

Kruithof, Kristy/Aldridge, Judith/Décary-Hétu, David/Sim, Megan/Dujso, Elma/Hoorens, Stijn: Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands, 1. Auflage, 2016, Cambridge: RAND Corporation.

Kugelmann, Dieter: Polizei- und Ordnungsrecht, 2. Auflage, 2012, Heidelberg: Springer.

Löwe, Ewald/Rosenberg, Werner: Die Strafprozessordnung und das Gerichtsverfassungsgesetz: Großkommentar, Band 3, 26. Auflage, 2014, Berlin: De Gruyter.

Mey, Stefan: Darknet: Waffen, Drogen, Whistleblower - Wie die digitale Unterwelt funktioniert, 1. Auflage, 2017, München: C.H. Beck.

Mitsch, Wolfgang: Medienstrafrecht, 1. Auflage, 2012, Heidelberg: Springer.

Moser-Knierim, Antonie: Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr, 1. Auflage, 2014, Wiesbaden: Springer Vieweg.

Petrlic, Ronald/Sorge, Christoph: Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 1. Auflage, 2017, Wiesbaden: Springer Vieweg.

Power, Mike: Dein Crack ist in der Post: Wie das Internet die Welt der Drogen revolutioniert, 1. Auflage, 2014, Köln: Eichborn Verlag.

RAND Corporation: Anzahl der Verkäufer von illegalen Drogen im Darknet in ausgewählten Ländern weltweit im Januar 2016, zitiert nach de.statista.com, 2017, https://de.statista.com/statistik/daten/studie/596128/umfrage/anza...rkaeufer-von-illegalen-drogen-im-darknet-in-ausgewaehlen-laendern/, abgerufen am 29.09.2017.

RAND Corporation: Darknet: Das verdienen Online-Drogenhändler, zitiert nach de.statista.com, 12.08.2016, https://de.statista.com/infografik/5480/darknet-das-verdienen-online-drogenhaendler/, abgerufen am 25.09.2017.

Reimer, Helmut: "Bundestrojaner": TeleTrusT - Bundesverband IT-Sicherheit e.V. kündigt Verfassungsbeschwerde an, in: Datenschutz und Datensicherheit, Heft 10, Oktober 2017, S. 645.

Richter, Konstantin: Der Pate des Internets, 08.02.2015, https://www.welt.de/137224002, abgerufen am 02.10.2017.

Schiemzik, Boris: Wie viel Überwachung braucht der Rechtsstaat?, 29.06.2017, https://www.welt.de/wirtschaft/bilanz/article166084791/Wie-viel-Ueberwachung-braucht-der-Rechtsstaat.html, abgerufen am 02.10.2017.

Sixt, Elfriede: Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie, 1. Auflage, 2017, Wiesbaden: Springer Gabler.

Sokolow, Andrej: Staatstrojaner soll für Behörden in Zeiten von WhatsApp & Co mitlesen, 23.06.2017a, https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2007043.htm&pos=3&hl words=on, abgerufen am 30.09.2017.

Sokolow, Andrej: Was die Überwachung der Messenger bedeutet, 23.06.2017b, http://www.wiwo.de/technologie/digitale-welt/whatsapp-was-die-ueberwachung-der-messenger-bedeutet/19972834.html, abgerufen am 02.10.2017.

Spiegel Online (Hrsg.): Millionenvermögen des mutmaßlichen AlphaBay Gründers beschlagnahmt, 25.07.2017, http://www.spiegel.de/netzwelt/web/darknet-behoerden-beschlagnahmen-millionenvermoegen-von-alphabay-betreiber-a-1159577.html, abgerufen am 01.10.2017.

Stempfle, Michael: Der Staat wird zum Hacker, 22.06.2017, www.tagesschau.de/inland/whatsapp-ueberwachung-101.html, abgerufen am 02.10.2017.

Stöcker, Christian: Warum Polizisten keine Smartphones hacken sollten, 18.06.2017, http://www.spiegel.de/wissenschaft/mensch/ueberwachung-warum-polizisten-keine-smartphones-hacken-sollten-kolumne-a-1152499.html, abgerufen am 01.10.2017.

Tagesschau (Hrsg.): Bundestag erlaubt WhatsApp-Überwachung, 22.06.2017, www.tagesschau.de/inland/whatsapp-ueberwachung-105.html, abgerufen 01.10.2017.

Tinnefeld, Marie-Theres/Buchner, Benedikt/ Petri, Thomas: Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, 2012, München: Oldenbourg Verlag.

Wainwright, Tom: Narconomics: Ein Drogenkartell erfolgreich führen, 1. Auflage, 2016, München: Karl Blessing Verlag.

Welt (Hrsg.): Durchsuchungen bei Bestellern von Falschgeld im Darknet, 21.09.2017, https://www.welt.de/regionales/berlin/article168897822/Durchsuchungen-bei-Bestellern-von-Falschgeld-im-Darknet.html, abgerufen am 02.10.2017.

Witsch, Kathrin: Das illegale Geschäft mit Waffen im Internet, 25.07.2016, http://www.wiwo.de/politik/deutschland/darknet-das-illegale-geschaeft-mit-waffen-im-internet/13922478-all.html, abgerufen am 02.10.2017.

Zeit Online (Hrsg.): Ermittler schließen Darknet-Portale für Drogen- und Waffenhandel, 20.07.2017, http://www.zeit.de/digital/internet/2017-07/alphabay-drogenhandel-darknet-geschlossen-usa-jeff-sessions-hansa, abgerufen am 01.10.2017.

IMPRESSUM

Covergestaltung: Leonie Schneider
Herausgeber im Selbstverlag: Lukas Schneider, Am Wengert 13, 97230 Estenfeld