Illegale Marktplätze im Darknet

Klara Scherf

Seminararbeit im Interdisziplinären Lehrangebot
des Institus für Informatik

Leitung: Prof. Hans-Gert Gräbe, Ken Pierre Kleemann

http://bis.informatik.uni-leipzig.de/de/Lehre/Graebe/Inter

Leipzig, 31. März 2021

Inhaltsverzeichnis

1 Einleitung **3**

2 Die drei Bereiche des Internets **3**

3 The Onion Routing Projekt **4**

3.1 Das Tor-Netzwerk 4

3.2 Hidden Services 7

3.3 Der Tor-Browser 7

4 Illegale Marktplätze **8**

4.1 Digitalisierung 9

4.2 Zahlungsverkehr 10

4.3 Umsätze 11

4.4 Vorteile für die Marktteilnehmer und -teilnehmerinnen 12

4.5 Exit Scams 12

4.6 Strafen 13

5 Vorgehen der Ermittlungsbehörden **14**

5.1 Vorgehen 14

5.2 Ermittlungserfolge 15

6 Fazit **16**

Abbildungsverzeichnis **18**

Literatur **19**

1 Einleitung

In unserer modernen Gesellschaft, in der fast jeder Zugang zu Technik und Internet hat, gewinnt auch der Onlinehandel immer mehr an Bedeutung. Neben legalen Geschäften manifestierte sich auch Online der Handel mit illegalen Waren und das bereits zu Beginn des Internets. Diese Arbeit beschäftigt sich mit diesem Handel, welcher zum größten Teil im sogenannten Darknet stattfindet. Das Darknet ist ein verborgener Teil des Internets, welches sich im sogenannten Tor-Netzwerk befindet. Es kann nur durch spezielle Software erreicht werden. Das Tor-Netzwerk bietet durch dessen Aufbau und Funktionen die ideale Umgebung für illegale Umschlagsplätze, auch wenn dies von den Entwicklern und Entwicklerinnen dafür nicht konzipiert worden ist.
Um dieses Thema verstehen zu können, müssen verschiedene Bereiche des Internets beleuchtet werden. Aber auch das Wissen darüber wie das Netzwerk funktioniert ist von Bedeutung. Durch das Verstehen der Anonymisierungsmechanismen lässt sich auch die Schwierigkeit für die Ermittlungsbehörden erkennen und gleichzeitig die Beliebtheit bei Kriminellen greifbar machen. Hierbei ergibt sich die Leitfrage dieser Arbeit: Lassen sich illegale Marktplätze durch Strafermittlungsbehörden aufhalten?
Bevor genauer auf das Vorgehen eingegangen wird, wie dieses Ziel verfolgt wird, werden die illegalen Marktplätze im Darknet betrachtet. Hierbei spielt die Digitalisierung eine große Rolle, da sie den weltweiten Handel mit (illegalen) Waren stark vereinfacht hat. Dabei wird kurz umrissen, wie die Bezahlung mit Kryptowährungen funktioniert und welche Umsätze auf den Marktplätzen erzielt werden konnten. Da mit einer Digitalisierung auch Vor- und Nachteile einhergehen, wird im Folgenden auf diese näher eingegangen. Durch den stark vereinfachten Zugang zu illegalen Gütern ergeben sich für Kriminelle neue Möglichkeiten. Aber auch die zu erwarteten Strafen sind von Bedeutung, weshalb diese anschließend beleuchtet werden. Nachdem die Grundlagen gelegt und die Dimension der Märkte dargestellt wurden, wird auf das Vorgehen der Ermittlungsbehörden näher eingegangen.
Zum Schluss werden alle Stränge miteinander verbunden und versucht eine Antwort auf die gestellte Frage zu finden.

2 Die drei Bereiche des Internets

Das Internet teilt sich in drei Bereiche auf. Das Surface Web, welches auch Visible Web bezeichnet wird, umfasst alle Internet-Inhalte, welche von herkömmlichen Suchmaschinen indiziert sind oder indiziert werden können. Das Deep Web ist das Gegenteil dessen und wird dementsprechend nicht von Suchmaschinen angezeigt. Das Dark Web ist ein spezieller Teil des Deep Webs und beruht auf Netzwerken, in denen ausschließlich Verbindungen

zwischen vertrauenswürdigen Partnern hergestellt werden. Der Zugang erfordert spezielle Tools. (vgl. Bundeskriminalamt, 2016c, S.1) Es wird als digitaler Ort gesehen, der sich mit technologischen Mitteln abschirmt. So wird die Anonymität bei der Nutzung sichergestellt, Verbindungsdaten und Standorte verschleiert und die Kommunikationsinhalte verschlüsselt. (vgl. Mey, 2018) Das Dark Web ist durch das The Onion Routing Projekt (Tor) realisiert.

3 The Onion Routing Projekt

Das The Onion Routing Projekt umfasst das zugehörige Tor-Netzwerk, sogenannte Hidden Services, die Internetseiten des Darknets, und den Tor-Browser. Letzteres ermöglicht den Zugang zum Netzwerk und den Hidden Services. Von weltweit ca. 4,5 Milliarden IP-Adressen nutzen 3 Millionen Tor (vgl. Simplicissimus, 2020).

3.1 Das Tor-Netzwerk

Das Tor-Netzwerk besteht aus Tor-Knoten, die den Austausch von Informationen ermöglichen, und Hidden Services, welche von den Nutzern und Nutzerinnen angeboten werden (vgl. Setz, 2013). Das namensgebende Onion-Routing geht auf Arbeiten von Goldschlag, Reed und Syverson aus dem Jahr 1999 zurück. Durch dieses Verfahren, schematisch dargestellt in Abbildung 1, wird die Anonymität der Nutzer und Nutzerinnen gewährleistet. (vgl. Hildebrandt, 2007, S. 27)

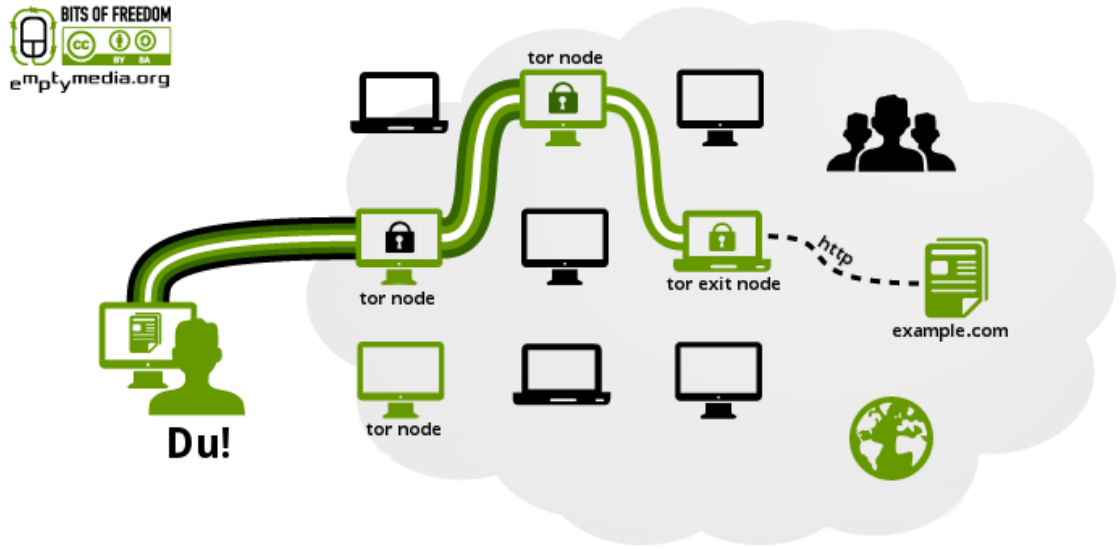

Abbildung 1: Funktionsweise des Tor-Netzwerks (emptymedia.org, 2015)

In dieser Abbildung möchte ein Nutzer eine Information an einen Server übermitteln und dabei das Tor-Netzwerk nutzen. Dabei wird die Information in mehrere Schichten ein-

gebettet, zu erkennen an den schwarzen, dunkelgrünen und hellgrünen Ummantelungen. Das Konzept lässt sich am besten am Beispiel von einem Brief mit drei Umschlägen in diesen Farben verbildlichen. Auf dem ersten, schwarzen Umschlag steht eine vorher bekannte, zufällig gewählte Adresse eines Verteilerknotens (Tor Node). Erhält dieser den Brief, entfernt er den schwarzen Umschlag und erfährt so die nächste Adresse. Der nächste Verteilerknoten öffnet nun den dunkelgrünen Umschlag und schickt den Brief an den letzten Knoten weiter, welcher nun den letzten Umschlag an den Adressaten sendet. Die Briefumschläge sind Verschlüsselungen und können nur sukzessive von den Tor Nodes entschlüsselt werden. (vgl. Schneider, 2018, S. 29f.) Die Tor Nodes von tausenden Freiwilligen weltweit betrieben (vgl. The Tor Project, Inc., 2021).
Das Verfahren sorgt dafür, dass bereits dem zweiten Knoten der Absender bzw. die Absenderin nicht mehr bekannt ist. Für den Empfänger bzw. die Empfängerin wirkt es so, als käme die Anfrage von Knoten 3. (vgl. Schneider, 2018, S. 29f.) Dies ermöglicht eine anonyme Kommunikation zwischen einem Anbieter bzw. einer Anbieterin und einem Nutzer oder einer Nutzerin eines Dienstes oder einer Austauschplattform. Dies ist auch der Grund, warum Journalisten, Journalistinnen, Blogger, Bloggerinnen und Menschen aus Ländern mit starker Internetzensur, sowie Händler und Händlerinnen illegaler Waren und Dissidenten und Dissidentinnen das Netzwerk nutzen. Es wird jedoch auch einfach von Menschen genutzt, die die Anonymität wertschätzen. (vgl. Beuth, 2014)
Und dabei ist das Tor-Netzwerk weiter verbreitet, als man zunächst annehmen würde, Pro Tag nutzen durchschnittlich etwas weniger als 250000 Personen in Deutschland das Tor-Netzwerk. In Abbildung 2 ist die Zahl der Nutzer und Nutzerinnen pro Tag seit 2015 abgebildet.
Der Ausschlag 2018 lässt sich durch einen Denial of Service (DoS)-Angriff auf das Netzwerk erklären. Nach der Veröffentlichung der neuerer Tor-Versionen, welche resistenter gegenüber diesen Attacken ist, gingen die Zugriffszahlen auf ein normales Level zurück. (vgl. The Tor Project, 2020a)
Unter einem DoS-Angriff versteht man den Versuch, einen Internetservice so zu überlasten, dass er nicht mehr verfügbar ist. Dabei werden Server oder andere Netzwerkkomponenten angegriffen. Wenn der Angriff von mehr als einem Host ausgeht, spricht man auch von einem Distributed Denial of Service (DDoS)-Angriff. (vgl. Luber & Schmitz, 2017)
Und auch weltweit nutzen mehrere Millionen Menschen das Tor-Netzwerk, wie in Abbildung 3 erkennbar ist. Auch hier ist der Ausschlag der Nutzer- und Nutzerinnenzahlen im Jahr 2018 durch den DoS-Angriff zu sehen.
Da das Netzwerk anonym ist, können die Zugriffszahlen nur abgeschätzt werden. Diese werden durch die Zählung der Anfragen der Clients an die Verzeichnisse der Tor Nodes abgeschätzt. Zudem werden diese Zahlen hochgerechnet, da nicht alle Verzeichnisse diese melden. Um herauszufinden, aus welchem Land ein Client kommt, werden die IP-Adressen

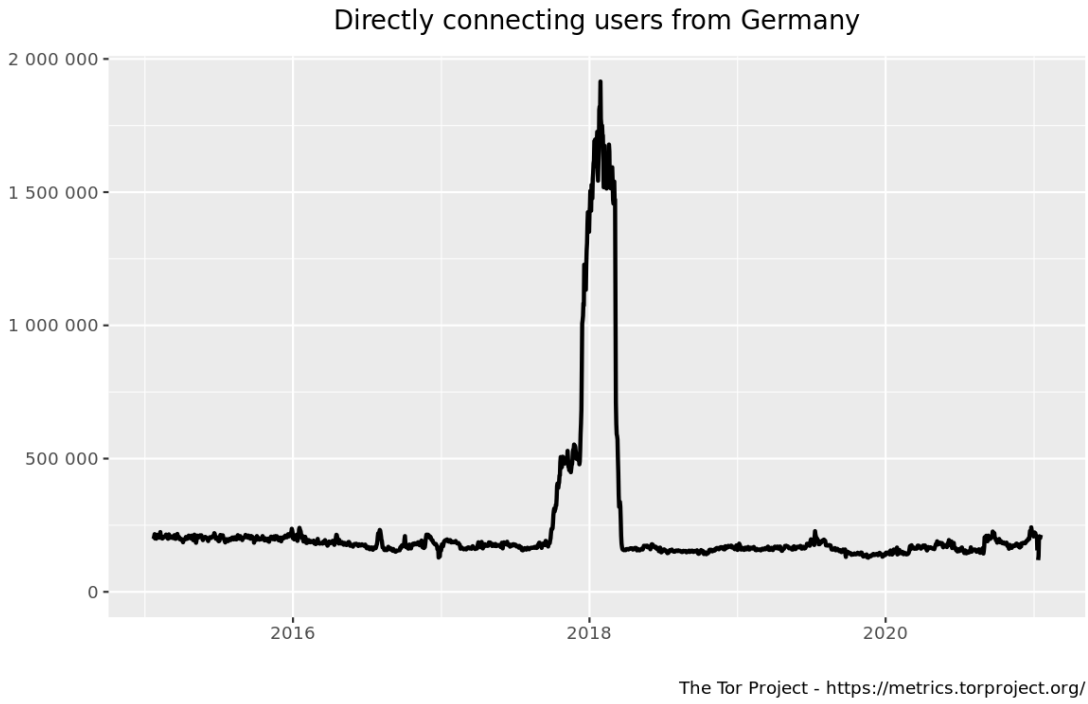

Abbildung 2: Zahl der Nutzer und Nutzerinnen des Tor-Netzwerks aus Deutschland pro Tag (The Tor Project, 2020a)

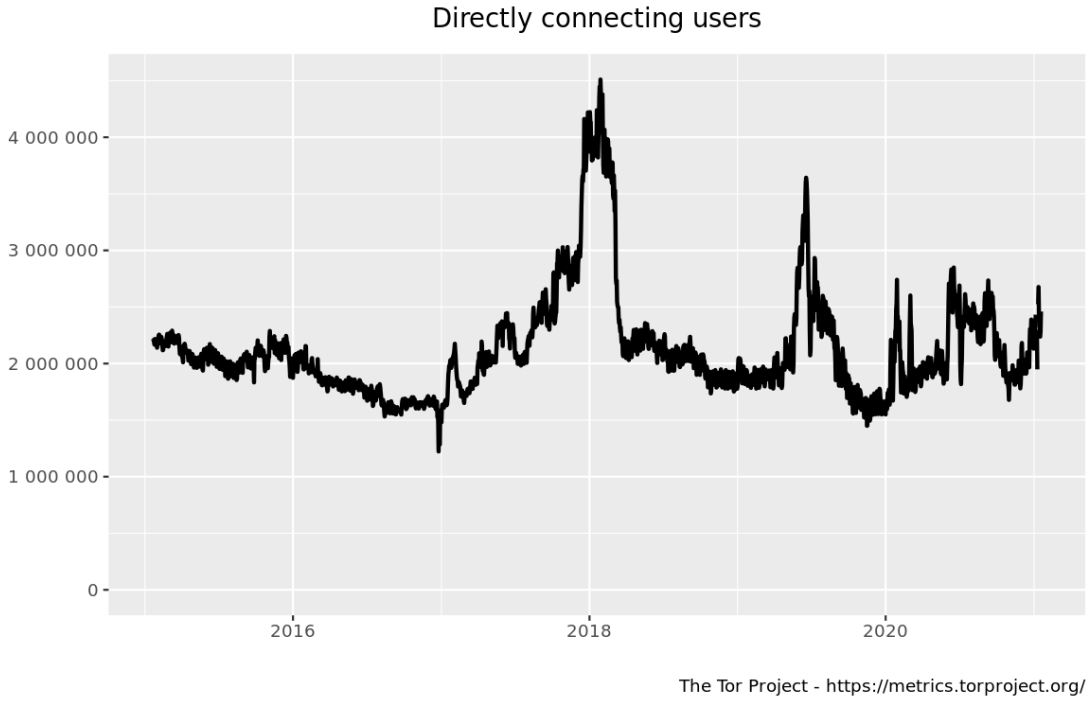

Abbildung 3: Zahl der Nutzer und Nutzerinnen des Tor-Netzwerks weltweit pro Tag (The Tor Project, 2020b)

in Ländercodes aufgelöst und in aggregierter Form gemeldet. (vgl. The Tor Project, n. d.)

3.2 Hidden Services

Hidden Services sind versteckte Dienste, die über URLs, die mit *.onion* enden, innerhalb des Tor-Netzwerks abrufbar sind. Die kryptischen Webadressen lassen sich nur schwierig merken. So ist beispielsweise die Adresse für das Hidden Wiki, das Wikipedia des Darknets: „http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page“, siehe Abbildung 4. (vgl. Beuth, 2014) Das Hidden Wiki verlinkt auf andere Hidden Services, zum Teil auch zu illegalen.

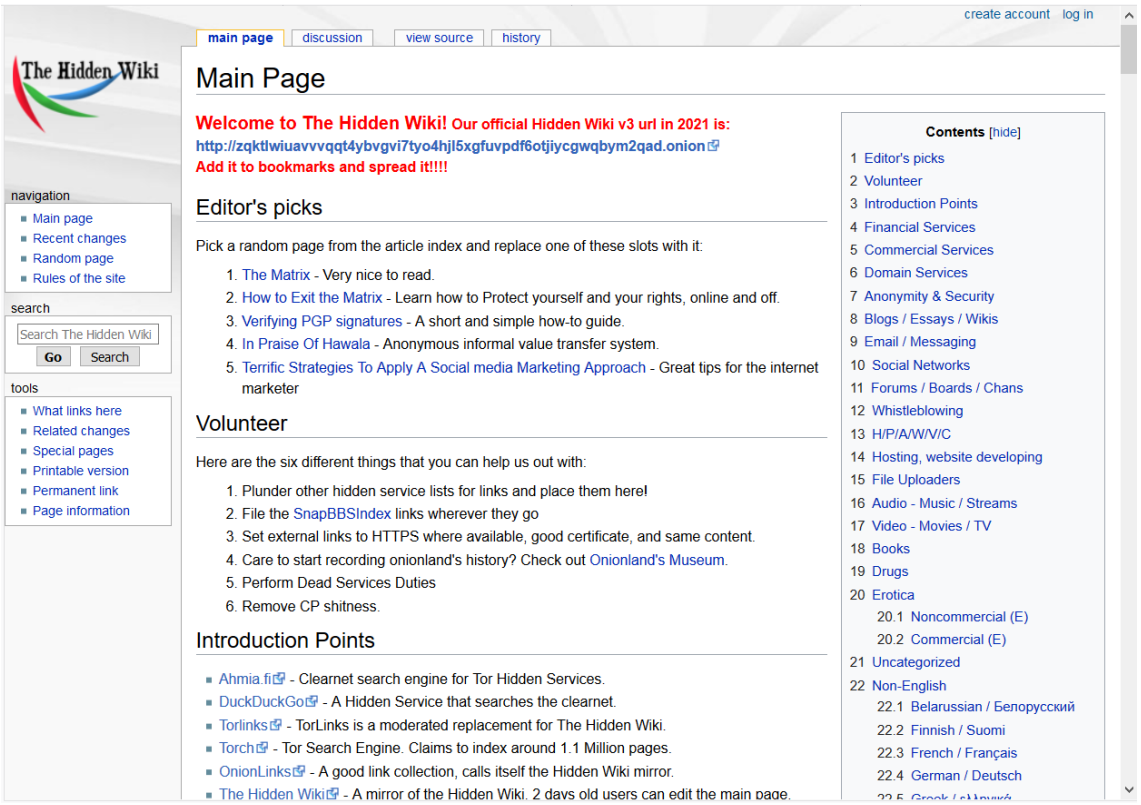

Abbildung 4: Das Hidden Wiki (Hidden Wiki, 2021)

Um die Hidden Services zu nutzen, reicht ein herkömmlicher Browser nicht aus (vgl. Schneider, 2018, S. 28). Es muss der Tor-Browser verwendet werden.
Durch das Prinzip des Onion Routing ist es zudem schwierig herauszufinden, wo sich die Server der Services befinden. Dementsprechend lassen sie sich auch nur schwierig vom Netz nehmen. (vgl. Beuth, 2014)

3.3 Der Tor-Browser

Der Tor-Browser verbindet sich mit dem Tor-Netzwerk. Er bietet amnestische Funktionen, wie ein privater Tab in einem herkömmlichen Browser. Zusätzlich wird die ursprüngliche IP, die Surfgewohnheiten und die Details eines Gerätes verborgen. Diese könnten dafür genutzt werden das Gerät innerhalb eines Netzwerks wiederzufinden. Dadurch wird eine

private Sitzung erlaubt, die vollständig Ende zu Ende verschleiert wird. (vgl. The Tor Project, Inc., n. d.) Während bei einem herkömmlichen Browser die Verbindung zu einer Seite von der eigenen IP-Adresse generiert wird, werden diese beim Tor-Browser über die Knoten geleitet, wie in Abschnitt 3.1 bereits beschrieben. Diese haben alle eigene IP-Adressen, welche aus verschiedenen Ländern kommen. Dadurch kann der Internet-Provider nicht mehr einsehen, welche Verbindungen übertragen wurden. So kann der tatsächliche Aufenthaltsort des Nutzers oder der Nutzerin nicht zurückverfolgt werden. (vgl. Schneider, 2018, S. 29) Die Knoten, über die die Verbindung läuft, werden alle zehn Minuten vom Tor-Browser geändert. (vgl. Schneider, 2018, S. 30). Durch diese Verschleierung wird die Nutzung von sonst nicht abrufbaren Internetseiten für von Internetzensur betroffenen Menschen ermöglicht (vgl. Beuth, 2014). So ist beispielsweise das sogenannte „goldene Schild“ des Ministeriums für Staatssicherheit in China, eine landesweite Firewall, nicht in der Lage, die Tor-Verbindungen komplett zu unterbinden. Durch die starke Anonymisierung Aller ist es jedoch auch für Ermittlungsbehörden enorm schwierig den Handel mit illegalen Waren zu verfolgen. (vgl. Rentrop, 2020)

4 Illegale Marktplätze

Durch die Anonymität bildeten sich schon früh Marktplätze heraus, auf denen illegale Waren, wie beispielsweise Drogen, Waffen, Falschgeld, gestohlene Kreditkarten und kriminelle Dienstleistungen angeboten werden (vgl. Bundeskriminalamt, 2016a). 2011 entstand der erste Marktplatz seiner Art. Die Silk Road kombinierte das Anonymisierungsverfahren, welches Tor bietet, und digitale Kryptowährungen und ermöglichte so einen globalen Handel mit illegalen Drogen. Die Technologien ermöglichen die Verschleierung der Identität und den Standort der Nutzer und Nutzerinnen, weshalb die Arbeit der Strafverfolgungsbehörden erschwert wird. Zudem wird die Reichweite der Händler und Händlerinnen erhöht, ohne das Risiko einer Strafverfolgung zu erhöhen. Es gibt keine Altersbeschränkung oder andere Regulierungen, um auf dem Marktplatz einzukaufen, sofern der Zugang zum Tor-Netzwerk hergestellt wurde. (vgl. Tzanetakis, 2019b, S. 113)
Nach einer Darknet Statistik waren 2018 ein bis zwei Dutzend Kryptomärkte, wie die illegalen Marktplätze im Darknet ebenfalls genannt werden, online (vgl. Tzanetakis, 2019a, S. 113). Die Marktplätze sind ähnlich zu den herkömmlichen Online-Shops, wie beispielsweise Amazon, aufgebaut (vgl. Schneider, 2018, S. 33).
Im Folgenden wird auf die Digitalisierung und deren Effekte auf den illegalen Handel im Internet eingegangen. Anschließend wird erklärt wie das Bezahlsystem der Marktplätze hinsichtlich der Bezahlung mit Kryptowährungen funktioniert. Um die Dimension der Marktplätze zu verdeutlichen, handelt der nächste Abschnitt über die Umsätze der Märkte. Da es auch im Darknet Vor- und Nachteile gibt, wird anschließend auf die Vortei-

le für Händler, Händlerinnen, Kunden und Kundinnen, sowie den größten Nachteil, den Exit Scams, eingegangen. Zum Schluss werden die zu erwartenden Strafen für Verkäufer, Verkäuferinnen, Käufer, Käuferinnen, Betreiber und Betreiberinnen genannt.

4.1 Digitalisierung

Der Handel im Darknet ist digitalisiert. „Unter Digitalisierung ist ein sozio-ökonomischer Wandel zu verstehen, der durch die Verbreitung digitaler Technologien sowie deren Nutzung und die dadurch bedingte Vernetzung in die Wege geleitet wurde.“ (Tzanetakis, 2019a, S. 482) Durch diese Digitalisierung ist es für Handelnde wesentlich unwahrscheinlicher strafrechtlich verfolgt zu werden, im Vergleich zum herkömmlichen Handel mit illegalen Waren auf dem materiellen Markt. Gleichzeitig können sie ihr Angebot weltweit anbieten. Dies ist vor allem durch die Anonymisierungsverfahren möglich, welche das Tor-Netzwerk bietet. Neben den bereits vorher erwähnten Aspekten muss kein sozialer Beziehungsaufbau stattfinden. Dadurch werden sie als semi-öffentliche Märkte beschrieben. Diese zeichnen sich durch den Verkauf in einem nicht-öffentlichen Raum aus. Der herkömmliche Handel findet in offenen Märkten, also an öffentlichen Orten, oder in geschlossenen Märkten statt. Bei Letzterem findet der Verkauf an relativ sicheren Orten, wie Parks oder privaten Wohnraum, statt und Verkäufer bzw. Verkäuferinnen und Käufer bzw. Käuferinnen sind einander bereits bekannt. Somit bewirkt die Digitalisierung hier das Entfallen der geographischen Beschränkung. (vgl. Tzanetakis, 2019a, S.483f.) Weiterhin wirken sich das Wachstum an Technologien, der Zugang und die Entwicklung der Infrastruktur sowie politische und kulturelle Veränderungen auf die Nachfrage nach illegalen Produkten und Dienstleistungen aus (vgl. Thomaz, 2020). Den Anstieg der Nachfrage an illegalen Waren im Darknet, sieht man beispielhaft für Drogen in den GDS2019 Key Findings Report der Global Drug Survey. In Abbildung 5 sieht man den Anteil der beschafften Drogen in Prozent in den Jahren 2014 bis 2019 für die Länder Österreich, Deutschland, Italien, Niederlande und Schweiz, die über die Marktplätze erworben wurden. Hier lässt sich ein klarer Anstieg erkennen. (vgl. Global Drug Survey, 2019, S. 161)
Käufer und Käuferinnen von Drogen im Darknet sind zu etwa 80% männlich und in den Mitt- bis Endzwanzigern. Sie sind sozio-ökonomisch gut situiert. Es handelt sich meist um Gelegenheits-, Party- und Freizeitkonsumenten und -konsumentinnen. (vgl. Mey, 2018, S. 27)
Durch die Existenz der Märkte wurde der physische Fußabdruck des Handels mit illegalen Gütern über Grenzen erweitert und vereinfacht. Zudem wurde der Informationsfluss erleichtert. (vgl. Thomaz, 2020)
Durch die Digitalisierung hat sich außerdem eine institutionelle Selbstregulierung etabliert. Unter einer Selbstregulierung nach wirtschaftstheoretischem Verständnis versteht man den Tausch von Waren auf der Basis von Preisen, sodass der Nutzen aller betei-

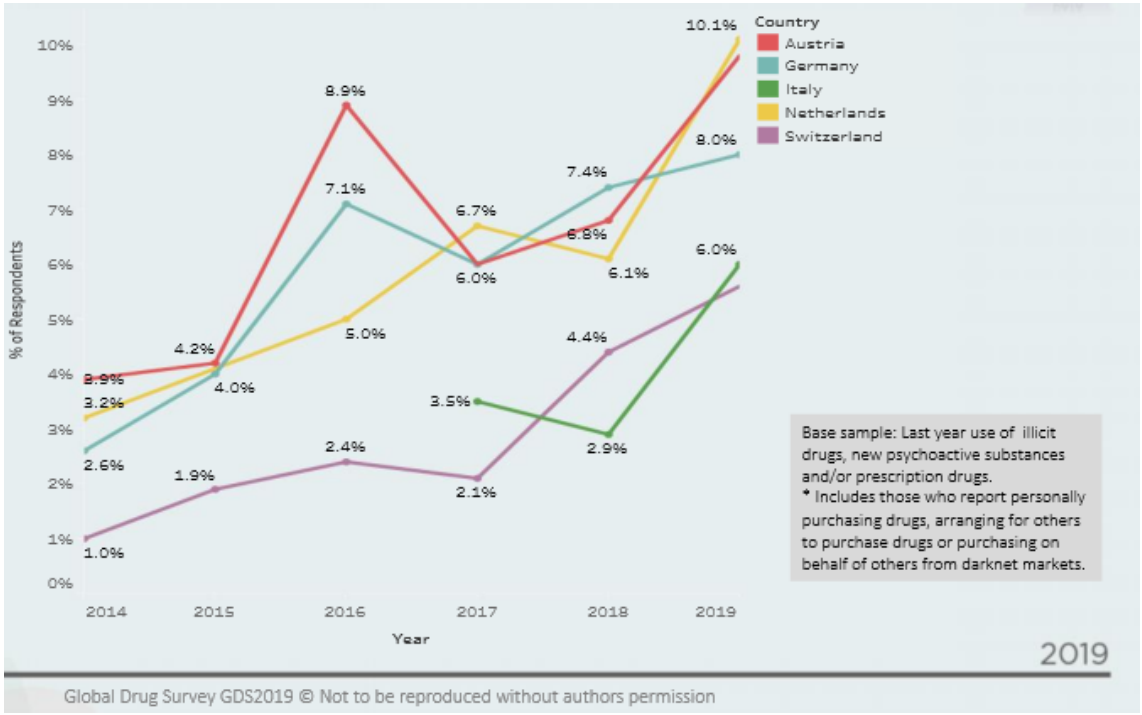

Abbildung 5: 6 Jahrestrend der beschafften Drogen im Darknet (Global Drug Survey, 2019)

ligten Akteure und Akteurinnen maximiert wird. Es wird auf den Kryptomärkten die Ausweitung von Marktbeziehungen auf der Basis von effizienten Strukturen ermöglicht. Dadurch werden sie zu dynamischen Wachstumsmärkten. Durch die Überschneidung des materiellen und virtuellen Marktes ist diese Selbstregulierung jedoch nicht in vollem Umfang gegeben. Circa ein Viertel der drogenbezogenen Transaktionen sind beispielsweise aufgrund ihrer Größe nicht für den Eigenkonsum bestimmt und werden wahrscheinlich profitorientiert weiterverkauft. Die weltweite Drogenprohibition hat dabei keinen Einfluss auf die Selbstregulierung. (vgl. Tzanetakis, 2019a, S. 488)
Nach den Daten des UNODC werden 187 Länder als Teilnehmer im Tor-Netzwerk beobachtet. 99% des Handelsvolumen beschränkt sich auf 40 von diesen und wird nur über 5,66% aller verfügbaren Verbindungen bewegt. Dies weist auf ein effizientes und organisiertes System hin. (vgl. Thomaz, 2020)

4.2 Zahlungsverkehr

Mit der Digitalisierung ebenfalls einhergehend ist die Möglichkeit der digitalen Zahlung. Im illegalen Umfeld ist außerdem die Nutzung einer Kryptowährung vorteilhaft, da diese unregulierten globalen Austausch von Geld ermöglicht. (vgl. Tzanetakis, 2019b, S. 489) Die wohl bekannteste Währung ist der Bitcoin. Die massenhafte Nutzung brachte diesen jedoch an die Grenzen seiner technischen Infrastruktur, weshalb sich auch Alternativen

wie beispielsweise Monero durchsetzten. Diese funktionieren ähnlich. Die folgenden Ausführungen begrenzen sich auf den Bitcoin.
Ein einzelner Bitcoin lässt sich in bis zu 100 Millionen Einzelteile zerlegen, welche als Satoshis bezeichnet werden. Um mit der Währung zu handeln, wird eine Software benötigt. Durch diese wird dem Nutzer bzw. der Nutzerin eine Adresse zugewiesen, welche ein aus zufälligen Zeichen bestehendes Nummernkonto ist. Zwischen diesen Konten lassen sich dann Überweisungen abwickeln. Wie andere Währungen auch, lassen sich diese überwachen. Hierbei gibt es jedoch keine zentrale Kontrollstelle, sondern eine Datenbank, in der aufgezeichnet wird, wem welcher Bitcoin gerade gehört. Jeder der die bereits erwähnte Software heruntergeladen hat, lädt auch eine Kopie der Datenbank runter. (vgl. Mey, 2018, S. 19f.) Die Transaktionen sind jedoch von außen nicht verfolgbar, da die Identität hinter dem Konto nicht in Erfahrung gebracht werden kann (vgl. Setz, 2013, S. 3). Trotzdem ist es möglich, durch den Kauf von Bitcoins auf Bitcoin-Börsen durch Zahlung mit einer Fiatwährung, diese preiszugeben. In den Datenbanken dieser Börsen sind somit potentiell die Informationen gespeichert, welches realweltliche Konto mit dem Bitcoin-Konto verknüpft ist. (vgl. Mey, 2018, S. 21)
Um das mehrfach Ausgeben der Währung zu verhindern, gibt es die sogenannte Blockchain. Dabei prüft ein Teil der Bitcoin-„Crowd“, ob der Bitcoin, welcher überwiesen werden soll, noch dem Nummernkonto gehört oder schon ausgegeben wurde. Falls eine Überweisung möglich ist, wird die Transaktion zusammen mit anderen in einem digitalen Block zusammengefasst, welcher aus Einzelinformationen besteht. Die Kette aller Transaktionsblöcke wird als Blockchain bezeichnet. (vgl. Mey, 2018, S. 21f.)
Ein weiterer Schutzmechanismus zu Kryptowährungen ist die Verwendung von Treuhandkonten. Beim Einkauf von Waren auf den illegalen Marktplätzen kann das Geld so zusätzlich geschützt werden. Hierbei behält der Marktplatz die Zahlung des Käufers bzw. der Käuferin ein, bis dieser bzw. diese bestätigt, dass die Bestellung erhalten wurde. Erst dann erhält der Händler bzw. die Händlerin sein Geld. (vgl. Christian, 2015) Dies ermöglicht jedoch auch Exit Scams, auf welche später in Abschnitt 4.5 eingegangen wird.

4.3 Umsätze

Bevor es im Oktober 2013 dem US-amerikanischen FBI gelang die Handelsplattform Silk Road zu schließen, wurde der Umsatz 2012 auf 15 Millionen US-Dollar geschätzt und 2013 auf über 100 Millionen. Kurz nach diesem Erfolg der Strafermittlungsbehörden entstanden jedoch neue Märkte. Deren Umsätze bleiben seit 2013 relativ stabil. (vgl. Tzanetakis, 2019b, S. 479) Der Umsatz wird auf 300000 bis 600000 Dollar pro Tag auf den größten Marktplätzen und auf wenige Tausende bei kleineren Plattformen geschätzt. Die 9000 einzelnen Händler und Händlerinnen verkaufen ihre Waren auf durchschnittlich 3 verschiedenen Marktplätzen. In einer Studie von Metropi Tzanetakis und Tanja Bukac von

2015/16 wurden während dieses Zeitraums auf 56% der Händler und Händlerinnen weniger als 10000 Dollar umgesetzt. Nur 5% kamen auf mehr als 200000 Dollar. Daraus lässt sich schließen, dass viele von ihnen wenig professionell und erwerbstätig mit Waren handeln. (vgl. Mey, 2018, S. 17f.)
Die bedeutendste Warengruppe, mit dreiviertel des Umsatzes, sind Drogen. Die fünf häufigsten Herkunftsländer dieser sind die Vereinigten Staaten, Großbritannien, Australien, die Niederlande und Deutschland. (vgl. Tzanetakis, 2019a, S. 481) Im Januar 2016 gab es in den USA 890 Verkäufer und Verkäuferinnen illegaler Drogen, in Deutschland 225 und in Großbritannien 338 (vgl. Schneider, 2018, S. 36). Dies hat eine Relevanz für die westlichen Industrienationen, da sie keine bedeutende Distributionsrolle auf den Märkten spielen. Zu den Anbau- und Produktionsstaaten gehören beispielsweise Afghanistan, Bolivien, Kolumbien, der Libanon und Marokko. (vgl. Tzanetakis, 2019a, S. 481) An dieser Stelle zeigt sich zudem, dass das Netzwerk ein reales Verständnis der Welt repräsentiert, da diese Länder, welche normalerweise ebenfalls einen florierenden Drogenhandel haben, auch hier präsent sind (vgl. Thomaz, 2020).

4.4 Vorteile für die Marktteilnehmer und -teilnehmerinnen

Wie bereits erwähnt, lassen sich durch den zu herkömmlichen Online Shops ähnlichen Aufbau, Produktgruppen filtern und Kunden- und Kundinnenbewertungen verfassen. So können sich Kunden und Kundinnen versichern, ob es sich um einen vertrauenswürdigen Händler oder eine Händlerin handelt. Zudem gibt es Produktfotos und Foren für den Austausch über die Qualität der Ware oder deren Anwendung. Auch ist es möglich, Anbieter bzw. Anbieterinnen und Produkte zu vergleichen. So ist es beispielsweise für Drogen möglich, eine höhere Qualität bei einem geringeren Beschaffungsrisiko zu erwerben, als bei dem herkömmlichen Vertrieb auf dem materiellen Markt. (vgl. Schneider, 2018, S. 33) Auch entfällt die Gefahr der Gewaltanwendung beim Einkauf (vgl. Mey, 2018, S. 26).
Aus Kunden- und Kundinnensicht ist zudem der Wettbewerb zwischen den Händlern und Händlerinnen von Vorteil. Bei Lieferproblemen kann dann auf einen anderen Anbieter bzw. Anbieterin zurückgegriffen werden. (vgl. Tzanetakis, 2019a, S. 484)

4.5 Exit Scams

Das System des Treuhandkontos, welches in Abschnitt 4.2 umrissen wurde, kann verschieden ausgestaltet sein. So ist es zum Teil möglich, dass der ursprüngliche Treuhänder bzw. Treuhänderin, also die Betreiber bzw. Betreiberinnen des Marktplatzes, als Kriminelle agieren und das Geld aus den laufenden Transaktionen unterschlagen und dann untertauchen (vgl. Bundeskriminalamt, 2016b, S. 11f.). Das Untertauchen der Betreiber und Betreiberinnen und das daraus resultierende Schließen des Marktes wird als Exit Scam

bezeichnet. Um dies zu verhindern wird zum Teil die Maßnahme des „Multisignature“ angewandt. Dabei müssen zwei der drei beteiligten Parteien einer Überweisung zustimmen. Dadurch wird verhindert, dass die Marktplatzbesitzer bzw. Marktplatzbesitzerinnen nicht allein auf das Geld zugreifen können. (vgl. Mey, 2018, S. 23f.)
Grund für einen Exit Scam ist vor allem das ständige Wachstum der Märkte. Durch ihre Größe werden sie öfter Opfer von DoS-Angriffen bzw. -Erpressern und -Erpresserinnen. Zudem werden Strafermittler und Strafermittlerinnen auf den Marktplatz aufmerksam. Weiterhin steigt die Gefahr einer Haftstrafe genauso wie die Beute an Kryptowährungen, die in den Treuhandkonten hinterlegt ist. (vgl. Bergmann, 2019) Somit werden die Besitzer und Besitzerinnen eher dazu verleitet. Durch diese Scams wird das Vertrauen in die Wirtschaft des Darknets mehr unterminiert, als die Erfolge der Ermittlungsbehörden (vgl. Mey, 2018, S. 23). Nur selten wird das Geld vor der Schließung des Marktes ausgezahlt, wie es bei den zwei Märkten Blackmarket Reloaded oder Dream Market der Fall war. Eine weitere Möglichkeit der Schließung ist der Erfolg der Strafermittlungsbehörden. Hier waren es beispielsweise die Märkte Silk Road und Hansa. (vgl. Bergmann, 2020)

4.6 Strafen

Den Händlern, Händlerinnen, Käufern, Käuferinnen und auch den Marktplatzbetreibern und Marktplatzbetreiberinnen drohen hohe Haftstrafen, falls die Strafermittlungsbehörden Erfolg haben. Auszugsweise gehe ich dabei nur auf den Drogen-, Waffen- und Falschgeldhandel ein.
Bei dem Handel mit Betäubungsmitteln droht den Käufern und Käuferinnen nach §29 Abs. 1 Nr. 1 BtMG eine Freiheitsstrafe zwischen ein und fünf Jahren oder eine Geldstrafe. (vgl. Schneider, 2018, S. 35) Da Verkäufer und Verkäuferinnen gewerbsmäßig handeln liegt ein besonders schwerer Strafbestand vor, weshalb ihnen nach §29 Abs. 3 Nr. 1 BtMG eine Freiheitsstrafe von mindestens einem Jahr droht. (vgl. Schneider, 2018, S. 35)
Den Betreibern und Betreiberinnen von den Marktplätzen droht die gleiche Strafe nach §29 Abs. 3 Nr. 1 BtMG, da sie eine Provision erhalten. Nach §29 Abs. 1 Nr. 10 BtMG verschaffen sie anderen die Möglichkeit zum Kauf und Verkauf von Betäubungsmitteln. (vgl. Schneider, 2018, S. 35f.) Eine tatsächlich verhängte Strafe war die Inhaftierung von Ross Ulbrich, dem Betreiber der Silk Road. Er wurde zu zweimal lebenslänglich und 40 Jahren Haft ohne die Möglichkeit einer vorzeitigen Entlassung verurteilt (vgl. Horch, 2019). Um die Nutzer der Plattformen zu belangen, benötigen die Ermittler und Ermittlerinnen Kontaktdaten der Händler und Händlerinnen (vgl. Muth, 2019).
Bei dem Kauf von Waffen kann man laut §51 Abs. 1 WaffG eine Freiheitsstrafe zwischen ein und fünf Jahren erwarten. Verkäufern und Verkäuferinnen droht nach §51 Abs. 2 WaffG eine Freiheitsstrafe zwischen ein und zehn Jahren. Bei Maschinenpistolen und vollautomatischen Gewehren werden die Käufer, Käuferinnen, Verkäufer und Verkäuferinnen

nach dem Kriegswaffenkontrollgesetz verurteilt. Der Kauf wird nach §22a Abs. 1 Nr. 2 KrWaffKontrG mit einer Freiheitsstrafe von ein bis fünf Jahren belangt. Da beim Verkauf ein besonders schwerer Fall vorliegt, sind laut §22a Abs. 2 KrWaffKontrG zwischen ein und zehn Jahre Haft zu erwarten. (vgl. Schneider, 2018, S. 37)
Für den Kauf von Sprengstoff droht nach §52 Abs. 1 Nr. 1 WaffG eine Freiheitsstrafe von mindestens sechs Monaten und maximal fünf Jahren. Gemäß §52 Abs. 5 WaffG müssen Verkäufer und Verkäuferinnen mit einer Strafe von ein bis zu zehn Jahre rechnen. (vgl. Schneider, 2018, S. 37)
Für den Handel mit Falschgeld gibt es eine Freiheitsstrafe für Käufer und Käuferinnen nach §146 Abs. 1 Nr. 2 StGB von mindestens einem Jahr und für Verkäufer und Verkäuferinnen nach §146 Abs. 2 StGB von mindestens zwei Jahren (vgl. Schneider, 2018, S. 39).

5 Vorgehen der Ermittlungsbehörden

Im Folgenden wird auf das Vorgehen eingegangen, welches Ermittlungsbehörden anwenden, um die Kriminalität im Darknet einzudämmen. Anschließend werden Beispiele für Ermittlungen und die daraus resultierenden Erfolge vorgestellt.

5.1 Vorgehen

Um Erfolge erzielen zu können, arbeiten nationale und internationale Sicherheitsbehörden zusammen (vgl. LKA NRW, n. d.). Eine direkte Überwachung der Transaktionen sowie eine Auswertung der Kommunikationen ist, wie bereits deutlich gemacht, nicht ohne Weiteres möglich. Allerdings kann eine Auswertung der Nicknames und der Shopnamen erfolgen. (vgl. Moßburger, 2017) Es wird meist auf die klassische Polizeiarbeit zurückgegriffen. Dazu zählen beispielsweise das Beobachten von Paketstationen und der Einsatz von verdeckten Ermittlern und Ermittlerinnen, die sich als Kunden und Kundinnen oder Händler und Händlerinnen ausgeben und so auch in Foren unterwegs sind. Sie sammeln dabei Puzzlestücke, aus denen sich die Identität mit öffentlich zugänglichen Quellen zusammensetzen lässt. Eine weitere Möglichkeit ist die Bestellung von illegalen Waren. Insgesamt gibt es viele angreifbare Punkte, wie zum Beispiel ein Forum oder der Versand. (vgl. Knoke, 2017)
Denkbar ist auch die Möglichkeit einer breiten Serverüberwachung. Dabei beobachtet die Strafermittlungsbehörde einige Server auf der Welt und drosselt zufällig die Bandbreite einzelner. Scheint ein illegaler Marktplatz dadurch beeinträchtigt, kann herausgefunden werden in welcher Region sich der Server des Marktplatzes befindet. Der Radius kann so immer weiter minimiert werden. Dadurch können auch andere Verbindungen weiter

verfolgt werden. (vgl. Simplicissimus, 2020)
Einige Methoden der Strafermittlungsbehörden werden jedoch nicht direkt veröffentlicht (vgl. Moßburger, 2017). Fakt ist jedoch, dass ein einziger Fehler eines Kriminellen oder einer Kriminellen im Darknet zum Erfolg der Behörden führen kann (vgl. Knoke, 2017). Insgesamt ist die Strafermittlung sehr schwierig und aufwendig, wie auch die Beispiele im folgenden Abschnitt verdeutlichen.

5.2 Ermittlungserfolge

Ein bekannter Ermittlungserfolg war die „Operation Onymous“. Es konnten dabei 410 Onion-Domains, Bitcoins im Wert von einer Millionen US-Dollar und 180000 Euro in Bar beschlagnahmt werden. Auch Drogen, Waffen und Edelmetalle wurden sichergestellt. (vgl. Kannenberg, 2017) Zudem wurden die Marktplätze Pandora, Silk Road 2.0, Black Market, Blue Sky, Tor Bazaar, Topix, Hydra, Cloud 9 and Alpaca geschlossen (vgl. European Monitoring Centre for Drugs and Drug Addiction & Europol, 2017). Kurz nach der Schließung der Silk Road 2.0 war offenbar schon Silk Road 3.0 online (vgl. Kannenberg, 2017). Dabei arbeiteten das FBI, Europol und die Zollbehörde des US-Heimatschutzministeriums DHS zusammen (vgl. Beuth, 2014). Bis heute ist nicht bekannt, wie sie Erfolg haben konnten. Die Betreiber und Betreiberinnen von Tor konnten keine Schwachstellen feststellen, weshalb sie klassische Polizeiarbeit vermuten. (vgl. Kannenberg, 2017) Allerdings wurde bekannt, dass es im Sommer 2014 Unbekannten gelungen ist, mehrere Hidden Services zu deanonymisieren, indem sie vergleichsweise große Teile des Netzwerks monatelang kontrollierten (vgl. Beuth, 2014).
Ein weiterer Erfolg gelang der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) in Gießen im Juni 2017. Die Website Elysium, die bislang größte deutsche Plattform für den Tausch kinderpornografischen Materials, konnte vom Netz genommen werden. (vgl. LKA NRW, n. d.) Zwei der vier Betreiber sollen vorher auf einer anderen Kinderporno-Plattform aktiv gewesen sein, auf der sie sich kennengelernt haben. Da diese aufflog, kam im November 2016 Elysium online. Weltweit konnte die Plattform in dieser kurzen Zeit mehr als 111000 Nutzer erreichen. (vgl. o.A., 2018) Auch wenn auf diesen Plattformen nicht zwingend gewerbsmäßig gehandelt wird, zeigt sich auch hier das Phänomen, dass sich neue Seiten öffnen, wenn es den Ermittlungsbehörden gelingt, eine zu schließen.
Ein vor kurzem erreichter Erfolg konnte die Zentrale Kriminalinspektion Oldenburg (ZKI) und die Landeszentralstelle Cybercrime (LZC) der Generalstaatsanwaltschaft Koblenz erreichen. Dabei waren auch ausländische Behörden beteiligt, wie das FBI, die Polizeistellen in der Schweiz, der Ukraine, Australien, Dänemark und Moldawien. So konnte am 11. Januar 2021 der bis dahin weltweit größte Marktplatz Darkmarket geschlossen werden. Es wurden vor allem Drogen gehandelt. Aber auch Falschgeld, gestohlene und gefälschte

Kreditkarten, Sim-Karten und Schadsoftware wurden angeboten. Über den Marktplatz wurden mehr als 320000 Geschäfte abgewickelt und über 4650 Bitcoins sowie 12800 Moneros bewegt. Das entsprach zu diesem Zeitpunkt einer Summe von mehr als 140 Millionen Euro. Neben den 20 Servern in Moldawien und der Ukraine, welche beschlagnahmt werden konnten, war auch der Bunker im rheinland-pfälzischen Traben-Trarbach zeitweise ein Host des Darkmarket. (vgl. o.A., 2021)
Dieser Bunker wurde durch einen Fall in den Jahren 2015 bis 2019 bekannt (vgl. SWR, 2020). Auf den rund 400 Servern wurden mindestens 249000 Straftaten ermöglicht (vgl. Muth, 2020). Im Visier ist der Geschäftsmann, welcher Herman X. genannt wird, bereits seit 2015. Er soll schon in den Niederlanden ein verdächtiges Rechenzentrum betrieben haben. Zu Beginn der Ermittlungen observierte die Landeszentralstelle Cybercrime (LZC) der Generalstaatsanwaltschaft Koblenz und das LKA Mitarbeiter und Mitarbeiterinnen über Monate. Auch Gespräche über Telefone wurden überwacht. Da sie über zwei Jahre lang keine Erfolge erreichen konnten, bekamen sie von der Staatsanwaltschaft die Erlaubnis, den Bunker anzuzapfen und einen Polizist einzuschleusen. Ziel war es, Beweise zu finden, dass sich die Beteiligten bewusst waren, dass ihr Dienst für kriminelle Plattformen genutzt wird. (vgl. SWR, 2020) Denn ein Provider muss erst aktiv werden, wenn er von den kriminellen Geschäften Kenntnis hat. Nach dem Providerprivileg muss dieser aber nicht prüfen, was auf seiner Plattform passiert. (vgl. Muth, 2020) Es konnten sieben Beteiligte, darunter auch Herman X., festgenommen werden (vgl. SWR, 2020).

6 Fazit

Die Frage nach der nachhaltigen Bekämpfung der illegalen Marktplätze im Darknet durch die Ermittlungsbehörden lässt sich abschließend nicht klar beantworten. Fakt ist jedoch, dass sich die Märkte auch durch Betrugsmaschen, wie Exit Scams selbst schaden, da dadurch das Vertrauen zwischen den Akteuren und Akteurinnen geschädigt wird. Fälle, wie der des Marktplatzes Evolution, bei welchem die Betreiber im Frühjahr 2015 mit Bitcoins im Wert von mehreren Millionen Euro verschwanden, unterminieren das Vertrauen meist mehr als das Einschreiten der Ermittlungsbehörden (vgl. Mey, 2018, S.23).
Zudem entstehen für einen geschlossenen Marktplatz, sei es durch einen Exit Scam oder durch den Erfolg von Ermittlungsbehörden, drei neue. Dies kann auch als „Immunsystem des Darknets“ (Bergmann, 2020) bezeichnet werden. (vgl. Bergmann, 2020) Ein Grund hierfür ist wahrscheinlich der Fakt, dass wo es eine Nachfrage gibt, auch ein Angebot vorhanden ist. Hier muss auch angemerkt werden, dass die Vorteile des Kaufes im Darknet präsent sind. Wenn beispielsweise erreicht wird, dass die Qualität der verkauften Drogen steigt, kommt es zu weniger Todesfällen wegen verunreinigten Substanzen. Nach der Forscherin Meropi Tzanetakis führt die Verfügbarkeit nicht dazu, dass es immer mehr

Menschen gibt, die gefährliche Drogen konsumieren (vgl. Mey, 2018, S.27). So muss in der Sicht der Strafverfolgung weiter gegen die Händler, Händlerinnen, Marktplatzbetreiber und Marktplatzbetreiberinnen vorgegangen werden, der positive Effekt des Onlinehandels im Darknet ist jedoch nicht zu vergessen.
Ein weiterer Punkt ist die Kriminalität, die in der nicht digitalen Welt stattfindet. Diese wird stetig verfolgt und bekämpft, lässt sich aber trotzdem nicht aufhalten. Dies lässt sich ebenso auf das Darknet übertragen. Aufgrund der ständigen Eröffnung von neuen Marktplätzen und dem internationalen Interesse der Händler und Händlerinnen ihre Reichweite zu erhöhen, zeigt sich, dass sich das System nur schwer bis gar nicht aufhalten lässt. Hier möchte ich noch die Vermutung anbringen, dass der Wertanstieg der Kryptowährungen diesem Effekt der immer neu entstehenden Marktplätze nicht entgegengewirkt, sondern diesen weiter fördert.
Weiterhin sollte über die Drogenpolitik weiter nachgedacht werden. Wenn Drogen reguliert und entkriminalisiert werden, wird der Nährboden für dieses Phänomen entzogen. Auch über eine entsprechende Altersbeschränkung sollte nachgedacht werden. Durch Drogenarbeit, wie Beratung und Drug Checking-Angebote, wobei die Qualität im Labor geprüft wird, würde der Konsum sicherer werden, da Gefahren durch Verunreinigungen vermindert werden. (vgl. Tzanetakis, 2019a, S. 489) An dieser Stelle zeigt sich, dass Drogen sowohl auf dem materiellen als auch virtuellen Markt ein großer Punkt sind, für die eine Lösung gefunden werden muss. Drug Checking ist hierbei ein guter Anfang, es müssen aber auch weitere und vor allem für alle zugängliche Lösungen gefunden werden.
Neben dem Drogenhandel und -konsum, müssen jedoch auch die anderen illegalen Vorgänge im Darknet Antworten gefunden werden. Dazu zählt auch der Bereich des kinderpornografischen Dateienaustausch, da hierbei auch Menschenleben zu schaden kommen, die unfreiwillig beteiligt sind. Da diese Medien meist über Foren und nicht über Marktplätze gehandelt werden sollte überlegt werden die Kapazitäten der Ermittlungen umzudisponieren, um sich stärker auf diese zu konzentrieren.
Trotz der vielen negativen Aspekte des Darknets, darf die Bedeutung für politisch Verfolgte oder Unterdrückte nicht außer Acht gelassen werden. Das Tor-Netzwerk ist durch die Dezentralisierung fast unmöglich zu regulieren. Beeindruckend finde ich, dass sich der hier frei geschaffene Markt selbst reguliert, indem zum Beispiel Treuhänder, Bewertungen, freier Informationsaustausch und Wettbewerb stattfinden. Dies sorgt für bessere und günstigere Angebote, welche jedoch illegal sind.

Abbildungsverzeichnis

1 Funktionsweise des Tor-Netzwerks (emptymedia.org, 2015) 4
2 Zahl der Nutzer und Nutzerinnen des Tor-Netzwerks aus Deutschland pro Tag (The Tor Project, 2020a) 6
3 Zahl der Nutzer und Nutzerinnen des Tor-Netzwerks weltweit pro Tag (The Tor Project, 2020b) 6
4 Das Hidden Wiki (Hidden Wiki, 2021) 7
5 6 Jahrestrend der beschafften Drogen im Darknet (Global Drug Survey, 2019) 10

Literatur

Bergmann, C. (2019, 25. April). *Darknetmarket Wall Street Market macht offenbar den Exit Scam*. Verfügbar 28. März 2021 unter https://bitcoinblog.de/2019/04/25/darknetmarket-wall-street-market-macht-offenbar-den-exit-scam/

Bergmann, C. (2020, 1. September). *Empire, der größter Darknet-Marktplatz, geht mit Exit-Scam offline*. Verfügbar 28. März 2021 unter https://bitcoinblog.de/2020/09/01/empire-der-groesster-darknet-marktplatz-geht-mit-exit-scam-offline/

Beuth, P. (2014). *Operation Onymous: Selbst die Tor-Entwickler rätseln*. https://www.zeit.de/digital/datenschutz/2014-11/operation-onymous-faq?utm_referrer=https%3A%2F%2Fduckduckgo.com%2F

Bundeskriminalamt. (2016a). *BKA stellt Bundeslagebild Cybercrime 2015 vor*. Verfügbar 30. Dezember 2020 unter https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2016/Presse2016/160727_VeroeffentlichungLagebildCybercrime.html;jsessionid=3256C976AC6CC0394CF3B73A318E1A44.live0612?nn=29874

Bundeskriminalamt. (2016b). *Cybercrime Bundeslagebild*. Verfügbar 30. Dezember 2020 unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.pdf?__blob=publicationFile&v=8

Bundeskriminalamt. (2016c). *Informationen zum Darknet*. Verfügbar 30. Dezember 2020 unter https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2016/pi160727_Darknet.pdf?__blob=publicationFile&v=2

Christian, J. (2015). *The 'Exit Scam' Is the Darknet's Perfect Crime*. Verfügbar 27. März 2021 unter https://www.vice.com/en/article/xyw7xn/darknet-slang-watch-exit-scam

emptymedia.org. (2015, 6. Januar). *Wie das Tor-Netzwerk funktioniert*. Verfügbar 19. Januar 2021 unter https://mtmedia.org/manuals/wie-funktioniert-tor/

European Monitoring Centre for Drugs and Drug Addiction & Europol. (2017). *Drugs and the darknet: perspectives for enforcement, research and policy*. Verfügbar 20. Januar 2021 unter https://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet

Global Drug Survey. (2019). *GDS Key Finding 2019*. Verfügbar 18. Januar 2021 unter https://www.globaldrugsurvey.com/gds-2019/

Hidden Wiki. (2021). *Hidden Wiki*. Verfügbar 29. März 2021 unter http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

Hildebrandt, K. (2007). *Konzeption von Authentifizierungsmechanismen für anonyme Dienste und Realisierung eines ausgewählten Verfahrens im Anonymisierungsnetzwerk Tor* (Diplomarbeit).

Horch, P. (2019, 5. Juni). *Silk-Road-Betreiber Ross Ulbricht: „In meiner Situation ist Schmerz unvermeidbar“*. Verfügbar 28. März 2021 unter https://www.btc-echo.de/ross-ulbricht-aus-dem-gefaengnis-in-meiner-situation-ist-schmerz-unvermeidbar-bitcoin-schwarzmarkt/

Kannenberg, A. (2017). *Operation Onymous: 17 Verhaftungen bei Schlag gegen Darknet-Drogenplattformen*. Verfügbar 18. Januar 2021 unter https://www.heise.de/newsticker/meldung/Operation-Onymous-17-Verhaftungen-bei-Schlag-gegen-Darknet-Drogenplattformen-2444615.html

Knoke, F. (2017). *Fahndung im Darknet: So funktioniert die Verbrecherjagd im anonymen Netz*. Verfügbar 31. Dezember 2020 unter https://www.chip.de/news/Fahndung-im-Darknet-So-funktioniert-die-Verbrecherjagd-im-anonymen-Netz_128664221.html

LKA NRW. (n. d.). *Erfolge im Kampf gegen Darknet-Plattformen*. Verfügbar 20. Januar 2021 unter https://polizei.nrw/artikel/erfolge-im-kampf-gegen-darknet-plattformen

Luber, D.-I. S. & Schmitz, P. (2017, 22. Dezember). *Definition Distributed Denial of Service (DDoS) Was ist ein DDoS-Angriff?* Verfügbar 28. März 2021 unter https://www.security-insider.de/was-ist-ein-ddos-angriff-a-672826/

Mey, S. (2018). *Darknet: Waffen, Drogen, Whistleblower*.

Moßburger, T. (2017). *Wie Ermittler Verbrechen im anonymen Netz bekämpfen*. Verfügbar 2. Januar 2021 unter https://www.focus.de/digital/multimedia/internet-staatsanwalt-erklaert-gibt-es-das-perfekte-verbrechen-wie-die-ermittler-kriminalitaet-im-darknet-bekaempfen_id_6808837.html

Muth, M. (2019, 3. Mai). *Ermittler heben einen der größten illegalen Online-Marktplätze aus*. Verfügbar 29. Dezember 2020 unter https://www.sueddeutsche.de/digital/darknet-handel-drogen-daten-bka-europol-1.4430785

Muth, M. (2020, 19. Oktober). *Sie nannten ihn Cyberbunker*. Verfügbar 30. März 2021 unter https://www.sueddeutsche.de/digital/cyberbunker-traben-trarbach-darknet-prozess-1.5076338

o.A. (2018, 2. August). *Prozess wegen Kinderporno-Plattform im Darknet „Elysium“ – das Paradies der Pädophilen*. Verfügbar 30. März 2021 unter https://www.stuttgarter-nachrichten.de/inhalt.prozess-wegen-kinderporno-plattform-im-darknet-elysium-das-paradies-der-paedophilen.d96339f4-7f0a-49cf-b852-aecd51ae0e4a.html

o.A. (2021, 12. Januar). *Erfolg für Koblenzer Ermittler Polizei stoppt größten Darknet-Marktplatz*. Verfügbar 30. März 2021 unter https://www.n-tv.de/panorama/Polizei-stoppt-groessten-Darknet-Marktplatz-article22286015.html

Rentrop, C. (2020). *Der Tor-Browser: Unzensiert im Darknet surfen*. https://www.heise.de/tipps-tricks/Der-Tor-Browser-Unzensiert-im-Darknet-surfen-3853797.html

Schneider, L. (2018). *Bekämpfung von Online-Schwarzmärkten mittels Quellen-Telekommunikationsüberwachung*.

Setz, C. (2013). *Die Tiefe*. Verfügbar 18. Januar 2021 unter https://documents.epfl.ch/users/l/le/lenstra/public/papers/Die_Zeit_internet-deep-net-tor-onionland.pdf

Simplicissimus. (2020). *Wie 3 Deutsche im Darknet reich wurden*. Verfügbar 30. Dezember 2020 unter https://www.youtube.com/watch?v=Kw5w5dk4BSQ

SWR. (2020, 16. Oktober). *Der Cyberbunker in Traben-Trarbach Als das Darknet an die Mittelmosel kam*. Verfügbar 30. März 2021 unter https://www.swr.de/swraktuell/rheinland-pfalz/trier/cyberbunker-auf-mont-royal-100.html

The Tor Project. (n. d.). *Questions and answers about user statistics*. Verfügbar 19. Januar 2021 unter https://gitweb.torproject.org/metrics-web.git/tree/src/main/resources/doc/users-q-and-a.txt

The Tor Project. (2020a, 1. September). *Directly connecting users*. Verfügbar 19. Januar 2021 unter https://metrics.torproject.org/userstats-relay-country.html?start=2015-01-21&end=2021-01-19&country=de&events=off

The Tor Project. (2020b, 1. September). *Directly connecting users*. Verfügbar 19. Januar 2021 unter https://metrics.torproject.org/userstats-relay-country.html?start=2015-01-21&end=2021-01-19&country=all&events=off

The Tor Project, Inc. (n. d.). *Was ist der Unterschied zwischen Tor Browser und "Inkognitomodus", oder privaten Tabs?* https://support.torproject.org/de/tbb/tbb-and-incognito-mode/

The Tor Project, Inc. (2021). *Tor Browser (10.0.8)* (Software).

Thomaz, F. (2020). The Digital and Physical Footprint of Dark Net Markets. *Journal of International Marketing*, *28*(1), 66–80. https://doi.org/10.1177/1069031X19898678

Tzanetakis, M. (2019a). Digitalisierung von illegalen Märkten. *Drogen, Darknet und Organisierte Kriminalität*.

Tzanetakis, M. (2019b). Zu den Strukturen des Drogenhandels im Darknet. *Handbuch Drogen in sozial- und kulturwissenschaftlicher Perspektive*.