Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2019

geleitet durch Prof. Dr. Paul Molitor

Das Darknet - Im Licht der Öffentlichkeit

Mohamed Najjar & Hannah Schwaß

Inhaltsverzeichnis

Überarbeitung durch den Dozenten: Der vorliegende Text entspricht im Wesentlichen dem ursprünglichen durch die oben genannten Autor*inn*en erstellten Bericht. Der Dozent hat lediglich Schreib- und Kommatafehler entfernt sowie Formatierung angepasst.

1 Einleitung

Diese Ereignisse lesen sich wie eine Chronik der Kriminalität: **Oktober 2013**: Der Drogenmarktplatz *The Silk Road* im Darknet wird vom FBI hochgenommen und der Betreiber verhaftet. [1]; **Juni 2015**: Hacker veröffentlichen im Darknet Nutzerdaten von 32 Millionen Kund*innen der Webseite *Ashley Madison* – eine Webseite auf der verheiratete Menschen eine Affäre suchen. [2] **Juli 2016**: Der Monat, in dem bekannt wurde, dass der Attentäter auf das Münchener Olympia-Zentrum die Tatwaffe im Darknet gekauft hatte. [4] **März 2017**: Ein neunjähriges Kind wird in Herne ermordet, der Täter soll ein Video davon im Darknet hochgeladen haben – was sich später als falsch herausstellt. [3] Diese Ereignisse korrelieren ebenfalls mit den Ausschlägen der Skala in Abbildung 1. Dort werden die Google-Suchanfragen für den Begriff „Darknet“ in Deutschland dargestellt. Anscheinend wird genau dann nach dem Darknet gesucht, wenn Kriminelle es für Straftaten nutzen und damit auffliegen.

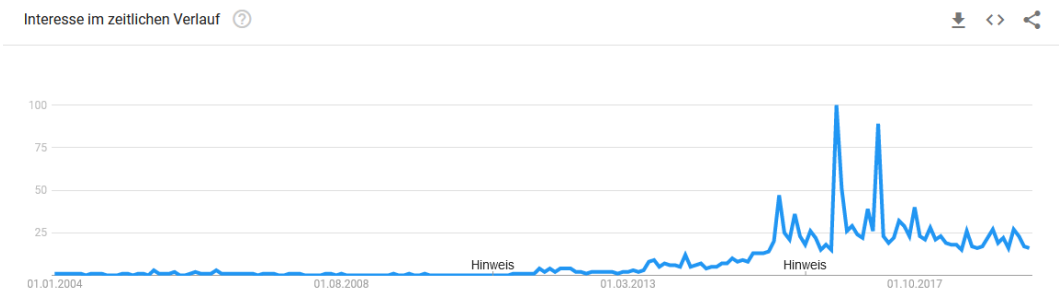

Abbildung 1: Suchanfragen für den Begriff „darknet“ in Deutschland 2004-2019 [5]

Die vorliegende Arbeit analysiert den öffentlichen Diskurs über das Darknet. Es wird geklärt, was das Darknet überhaupt ist und wie es sich von dem *normalen* Internet abgrenzt. Am Beispiel des Tor-Netzwerks wird die Funktionsweise eines Darknets vorgestellt und geklärt, wofür es momentan genutzt wird und zukünftig genutzt werden könnte. Danach wird die öffentliche Debatte über das Darknet in den Blick genommen: Wie wird es dargestellt? Wie berichten Journalist*innen darüber? Abschließend soll geklärt werden, was am Darknet überhaupt illegal ist und ob es seinem kriminellen Ruf gerecht wird.

2 Was ist das Darknet?

2.1 Surface Web, Deep Web, Darknet

In der Regel wird das Internet in drei verschiedene Bereiche aufgeteilt: Das Surface Web, das Deep Web und das Darknet.
Der offen zugängliche Teil wird **Surface Web** (dt. Oberflächen-Web), Clearnet (dt. klares Netz) oder Visible Web (dt. sichtbares Web) genannt, meint aber immer das gleiche Konzept: Internetseiten im Surface Web können von Suchmaschinen erfasst werden. Das wird auch *indiziert werden* genannt. Man erreicht Zugang zu diesen Seiten über gängige Browser wie Chrome, Mozilla Firefox oder Safari. Man erkennt sie daran, dass ihre Domain (Internetadresse) mit typischen Top-Level-Domains wie .de, .com oder .org endet. [6, S.11]
Das **Deep Web** (dt. tiefes Web) liegt eine Schicht unter der Oberfläche, ist allerdings auch Teil des alltäglich genutzten Internets. Es wird ebenfalls Hidden Web (dt. verstecktes Web) oder Invisible Web (dt. unsichtbares Web) genannt. Es beschreibt den Teil des Internets, der nicht durch Suchmaschinen gefunden werden kann oder soll – also nicht indiziert ist. Dies kann sein, wenn Teile einer Website durch Bezahlschranken oder Passwörter geschützt sind, bei dynamischen Inhalten oder wenn Suchmaschinen – mittels robots.txt. [7]– bewusst ausgeschlossen werden. [6, S.12]
Das **Darknet** ist an sich Teil des Deep Webs, grenzt sich aber dennoch davon ab. Praktisch gesehen gibt es *das Darknet* gar nicht, da es eher ein Konzept ist, das durch verschiedene Umsetzungen realisiert wird. Das Konzept lässt sich wie folgt umschreiben: „Ein Darknet ist ein digitales Netz, das sich vom sonstigen Internet abschirmt und mit technologischen Mitteln die Anonymität seiner Nutzer herstellt. Wer Inhalte anbietet, wer mit wem kommuniziert und worüber, das alles wird mithilfe von Verschlüsselungstechnologien verschleiert.“ [8]
Wenn wir also vom *dem Darknet* reden, beziehen wir uns auf das Konzept eines anonymen und verschlüsselten Internets, das nur durch bestimmte technische Umsetzungen zu erreichen ist. Die bekanntesten technischen Realisierungen sind Tor (The Onion Routing Network), I2P (The Invisible Internet Project) und Freenet.

2.2 Funktionsweise des Darknets – am Beispiel Tor

Will man Tor benutzen, muss man nur den Tor-Browser herunterladen. Um in das Darknet zu gelangen, ruft man eine Internetadresse auf, die mit .onion endet. Diese sind in den meisten Fällen eine zufällige Folge von Buchstaben und Ziffern – um sich also orientieren zu können, gibt es sogenannte Wikis oder Linklisten. Diese sind eine Sammlung von Seiten und ihren aktuellen .onion-Adressen.
Mit dem Tor-Browser kann man allerdings auch im gewohnten Internet surfen. In beiden Fällen sind die User anonym. Wie funktioniert das?

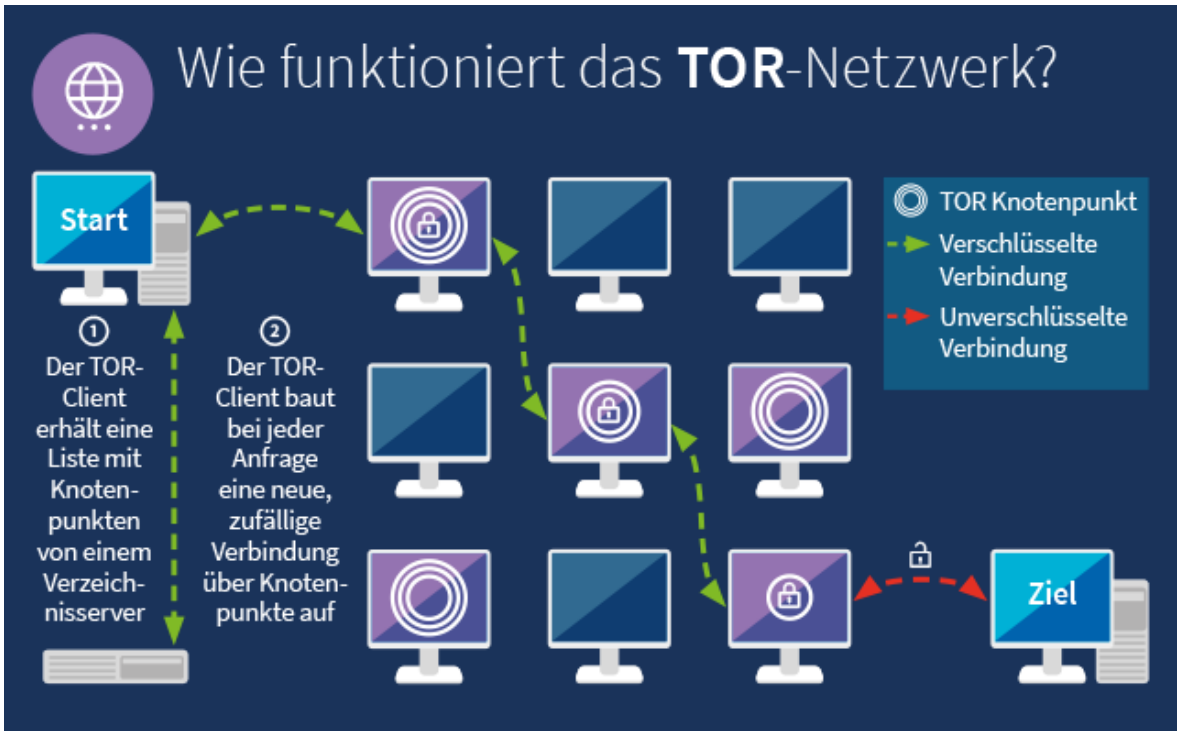

Abbildung 2: Funktionsweise des Tor-Netzwerks [9]

Im herkömmlichen Internet wird stets eine direkte Verbindung vom User zum Zielserver aufgebaut, um eine schnelle Kommunikation zu ermöglichen. Die anfragenden Netzwerke, also zum Beispiel der heimische Router, können durch die IP-Adresse eindeutig zugeordnet werden. Nicht immer sind die gesendeten Daten dabei verschlüsselt. In Abbildung 2 ist dargestellt, wie die IP-Adresse im Tor-Netzwerk verschleiert wird. Das geschieht dadurch, dass die Anfrage an den Zielserver mehrmals umgeleitet wird. Die Daten werden verschlüsselt an die erste Umleitung, Knoten genannt, weitergegeben. An diesem Eingangspunkt kann der Einstiegsknoten die IP-Adresse des Senders

sehen. Allerdings wird das Datenpaket über einen weiteren Knoten geschickt, der nur die IP-Adresse des vorherigen Knotens und des kommenden Knotens kennt. Der dritte und meistens letzte Knoten gibt das Datenpaket an den Zielserver weiter. An diesem Punkt kann man die IP-Adresse des Senders nicht mehr nachvollziehen, er ist anonym. Allerdings tritt das Datenpaket hier aus dem Tor-Netzwerk aus, ab dem Punkt ist nicht mehr garantiert, dass die Verbindung zum Zielserver verschlüsselt ist.
Der Pfad der Verbindung wird also über mindestens drei Knoten umgelenkt. Bei jeder neuen Anfrage oder nach zehn Minuten wird ein neuer Pfad zufällig gewählt. Jeder Knotenpunkt weiß zwar, woher das Datenpaket kam und wohin es geht, aber nie den ganzen Pfad. Da sich die Verschleierung wie Schichten um das Datenpaket legt, wird es Onion-Routing genannt. [10]

2.3 Hintergründe des Tor-Netzwerks

Der Begriff des Darknets fiel zum ersten Mal in den späten 1960ern. Damals gab es das *ARPANET* als erste Version des heutigen Internets. Daneben tauchten andere isolierte, geheime Netze auf, die als Darknets bekannt wurden. [11] Die Entwicklung von Tor begann erst wesentlich später in den 1990ern. Forscher*innen des US-amerikanischen Naval Research Lab (NRL) entwickelten den ersten Prototyp des Onion-Routings. [12] Mittlerweile ist Tor eine Nonprofit-Organisation und der Code unter einer freien und offenen Softwarelizenz veröffentlicht. An der Entwicklung arbeiten Festangestellte, eine Kerngruppe aus Entwickler*innen und ehrenamtliche Freiwillige. Vermutlich konnte sich Tor gegen andere Umsetzungen wie Freenet und I2P gerade deshalb durchsetzen, weil sie ein sehr großes Budget – und damit auch das Geld für festangestellte Entwickler*innen – haben.
Gerade dieses Budget wird immer wieder kritisch betrachtet. Das Tor Projekt veröffentlicht selbst regelmäßig einen Finanzbericht. Aus dem Bericht des Jahres 2015 geht hervor, dass 85% bis 90% der Finanzen aus Forschungstöpfen der US-Regierung kamen. [8] Da der Code sowieso frei einsehbar ist, sollte das eigentlich kein Problem sein, doch so einfach ist es nicht. Durch die Förderanträge, die Tor stellen muss, bekommt die US-Regierung einen Einblick, wie der Code weiterentwickelt werden soll und kann dementsprechend darauf reagieren. Für ein Projekt, das sich bewusst gegen die Überwachung der US-Regierung wehren will, ist das durchaus problematisch.

2.4 Nutzung des Darknets

Das Darknet grenzt sich vom Surface Web dadurch ab, dass es nicht durch Suchmaschinen indiziert werden kann, so steht es in Kapitel *Surface Web, Deep Web, Darknet*. Doch wie kann man dann erforschen, was im Darknet passiert und wozu es genutzt wird? Es gibt viele Gerüchte, die dem Darknet den Ruf des „Abgrunds des Internets“ [13] eingebracht haben, doch oft ohne ausreichende Belege.
Anders als meist angenommen, ist nicht alles, was im Darknet passiert, unsichtbar. Es gibt Seiten, die im Tor-Netzwerk feste .onion-Adressen haben, wie z.B. Facebook und die New York Times. Illegale Angebote wie Drogenmarktplätze ändern zwar ihre Adressen, sind aber darauf angewiesen gefunden zu werden. [14, S.18] Dies passiert meist durch Linklisten, wie im Kapitel *Funktionsweise des Darknets – am Beispiel Tor* beschrieben wurde.
So gibt es auch Forschung, die Programme schreibt und nutzt, die wie Suchmaschinen funktionieren, sogenannte Crawler. Mithilfe der Crawler werden .onion-Seiten gefunden, analysiert und kategorisiert. Exemplarisch wollen wir hier die Ergebnisse von Avarikioti u.a. in Abbildung 3 darstellen. Dabei wurden aus technischen Gründen lediglich die englischsprachigen Seiten analysiert, was rund 66% der Seiten einschließt. Die 4,5% deutschsprachige Seiten haben keinen Einfluss auf die Klassifikation. [14, S.12f.] Die Ergebnisse werden in zwei Bereiche aufgeteilt: In offen zugängliche .onion-Seiten und in versteckte .onion-Seiten (hidden services), quasi das Deep Web des Darknet, die oft nur nach einem Login besucht werden können.
Blogs haben in beiden Bereichen eine hohe Präsenz – darunter fallen alle Seiten, die ein festes Team an Autor*innen haben. Diese posten Inhalte auf den Blog, die nicht auf Interaktivität ausgelegt sind – im Gegensatz zu einem Forum. Darunter fallen hier auch Nachrichten – oder Marketingseiten, die nicht in ein spezifischeres Label eingeordnet werden können. Ein solches wäre **Activism**, unter das zum Beispiel Menschenrechtsaktivismus fällt. Oder aber **Whistleblowing**, das vor allem durch Wikileaks bekannt worden ist, aber auch sogenannte SecureDrops einbezieht, durch die Personen anonym Journalist*innen Daten zuspielen können. **Software** umschließt alle Seiten, die sich mit Softwareentwicklung oder -vermarktung beschäftigen – ausgenommen von **Hacking**, das eine eigene Kategorie hat, die allerdings nur einen minimalen Anteil hat. Der Unterpunkt **Hub** beschreibt Seiten, die wiederum auf andere Seiten verweisen, wie Wikis und Linklisten. Da man diese Seiten als Suchmaschinen-Ersatz nutzt, ist es logisch, dass sie in offenen Seiten einen wesentlich größeren Teil ausmachen. **Fraud** bezieht in

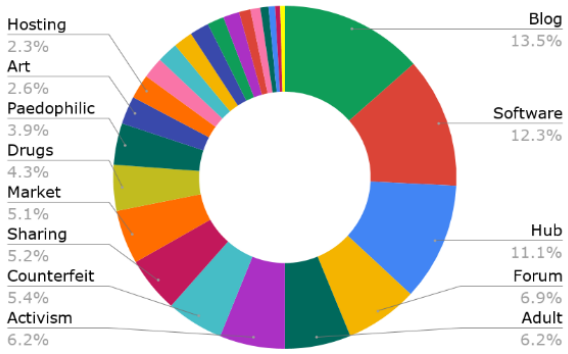

Fig. 10. Label of darknet pages

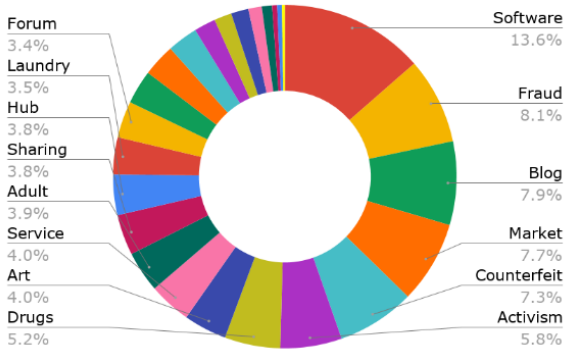

Fig. 11. Label of darknet hidden services

Abbildung 3: Grafische Darstellung der Nutzung [14, S.17]

den versteckten Seiten einen großen Anteil. Dies sind Betrugsseiten, die meist für einen Einsatz an Bitcoin (meistgenutzte Cryptowährung im Tor-Netzwerk) einen höheren Rücklauf an Bitcoin versprechen, diesen aber nicht einhalten. Ähnlich dazu ist **Laundry**, das Angebote der Geldwäsche verspricht, oft durch sogenanntes Bitcoin Mining. Oft wird das Darknet mit Marktplätzen in Verbindung gebracht, wie im Kapitel *Mediendarstellung des Darknets* später genauer beschrieben wird. Hier gibt es ebenfalls den Punkt **Market**, der solche Marktplätze beschreibt. Ebenfalls fallen **Drugs** und **Counterfeit** teilweise darunter, die Seiten beschreiben, in denen entweder Drogen und gestohlene Waren angeboten oder über diese geschrieben bzw. diskutiert wird. Ist das Hauptziel einer Seite, Gespräche zwischen Usern zu ermöglichen, so fällt sie unter das Label **Forum**. Ausgenommen sind Foren oder Chats, die sich spezifischen Themen verschrieben haben – diese könnten dann unter bereits erwähnte Label wie Aktivismus oder Drogen fallen. Es gibt ebenfalls das Label **Sharing**, das sich auf Seiten zum

Austausch von Dateien bezieht. Dies ist allerdings im Tor-Netzwerk nicht gewünscht und wird größtenteils von Ausgangsknoten blockiert, da ein so hoher Datenverkehr das Netz zu stark verlangsamt. [15] Unter **Adult** fallen pornografische Inhalte. Unter **Paedophilic** fallen davon abgegrenzt Inhalte wie Kinderpornografie und andere Themen rund um Pädophilie, wie zum Beispiel Selbsthilfegruppen. [14, S.15f.]
Das ist nur eine Auswahl der Label, die in der Studie genutzt wurden – und auch diese Seite sind nur eine Abstraktion, da für das Einordnen in eine Kategorie Abstriche in der Komplexität gemacht werden müssen. Dennoch zeigt die Studie sehr gut, dass es durchaus eine vielfältige Nutzung des Tor-Netzwerks gibt. Diese Unterscheiden sich von Darknet zu Darknet. So gibt es beispielsweise in Freenet und I2P mehr Filesharing-Plattformen, besser kuratierte Linklisten und eine große Vielfalt an Blogs mit gesellschaftlichen Themen. [8] Diese Forschung zeigt eine Momentaufnahme davon, wie das Darknet heutzutage genutzt wird. Ein Netz, das vor Überwachung und Zensur geschützt ist, in dem man anonym surfen kann. Dies lockt vor allem User an, die diese Anonymität brauchen. Das kann vielfältige Gründe haben, vielleicht für illegale Geschäfte oder aber den anonymen Austausch über kriminelle Erfahrungen. Genauso nutzen es Journalist*innen, die ihre Quellen schützen wollen. Menschen aus Staaten, in denen das Surface Web stark zensiert, wenn nicht gar gesperrt wird, oder aber solche, die vielen ihren politischen Aktivismus verfolgt werden, sind auf das Darknet angewiesen.
Abbildung 4 zeigt eine Weltkarte der Tor User in Relation zu den Gesamtzahlen der Internet User. Hier zeigt sich einerseits, dass Tor auf der gesamten Welt verbreitet ist, aber auch, dass es sich stark auf Europa und Nordamerika konzentriert. Dabei trennt Tor in seinen Erhebungen nicht, ob User auf .onion-Seiten surfen oder das *normale* Internet anonym nutzen.
Gerade wenn man sich das Surface Web genauer anschaut, zeigt sich das Potential des Darknets. Von der Überwachung des Internets sind nicht nur Kriminelle und Whistleblower betroffen, sondern alle, die das Internet nutzen. „Nahezu jeder Seitenaufruf wird von Werbedienstleistern mitgeschnitten und weiter verarbeitet. Aus diesen Informationen können individuelle Profile erstellt werden, die es ermöglichen, Nutzerinnen und Nutzern auf sie zugeschnittene Werbeangebote zu zeigen“, so Rechtsanwalt Jan Schallaböck. [17] Google durchsucht Emails nach Stichwörtern, um die passende Werbung daneben einzublenden [17], Marketing-Firmen schreiben ausführliche Anleitungen, wie man die Nutzer*innen am besten ausspäht. Dabei geht es um technische Daten wie beispielsweise Betriebssystem, Browser, Browser-Sprache und installierte

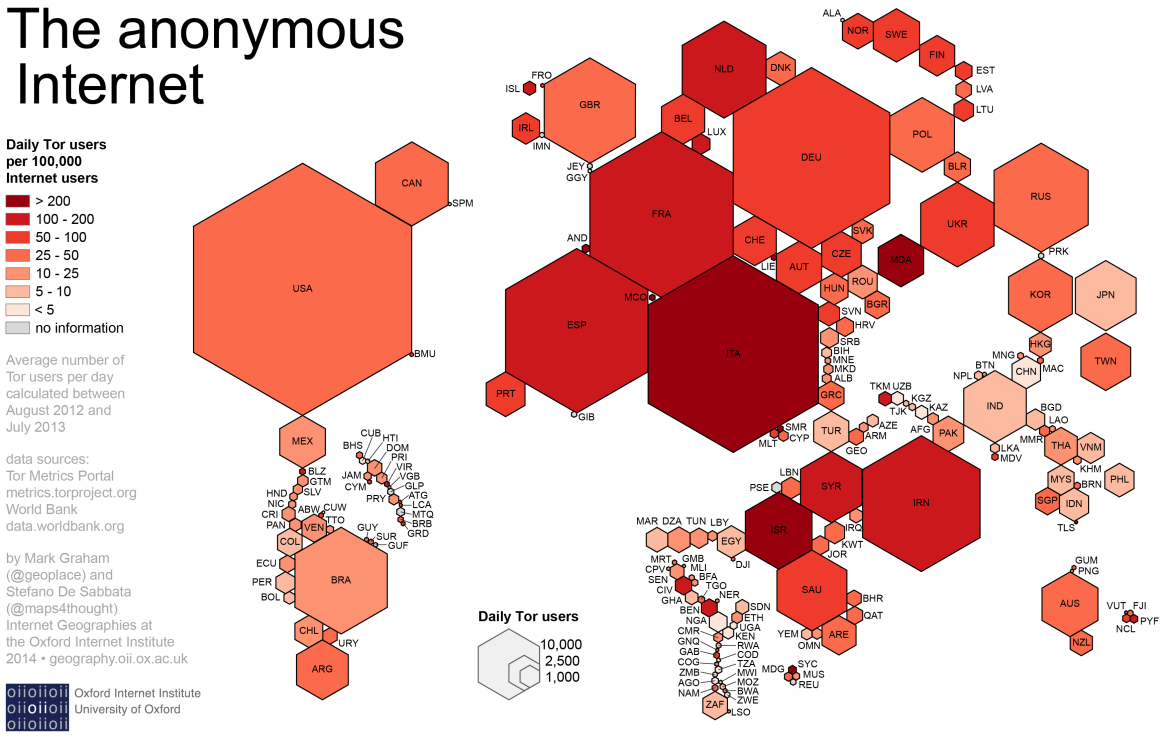

Abbildung 4: Weltkarte der Tor User [18]

Plugins. Aber auch das Verhalten der Nutzer*innen wird analysiert: [19] Seitenaufrufe pro Besucher*in, Verweildauer pro Besucher*in, Häufigkeit der Besuche, durchschnittlicher Umsatz pro Besucher*in, Clickmap/Heatmap. [19] Aus diesen Daten werden sogenannte Profile erstellt und diese werden genutzt um User zu manipulieren – sei es zum Kauf von bestimmten Produkten, aber auch demokratische Wahlen können so beeinflusst werden. [20] „Auch wenn diese in vielen Fällen nicht direkt auf einzelne Individuen zurückgeführt werden können, entsteht damit ein Wissenspotenzial, dass das Vertrauen in die Manipulationsresistenz von ganzen Gesellschaften beeinträchtigen kann. Das klassische Datenschutzrecht greift in dieser Hinsicht zu kurz, weil es den Schutz der Demokratie nicht hinreichend im Blick hat“, befürchtet Schallaböck. [17]

3 Mediendarstellung des Darknets

3.1 Bildsprache

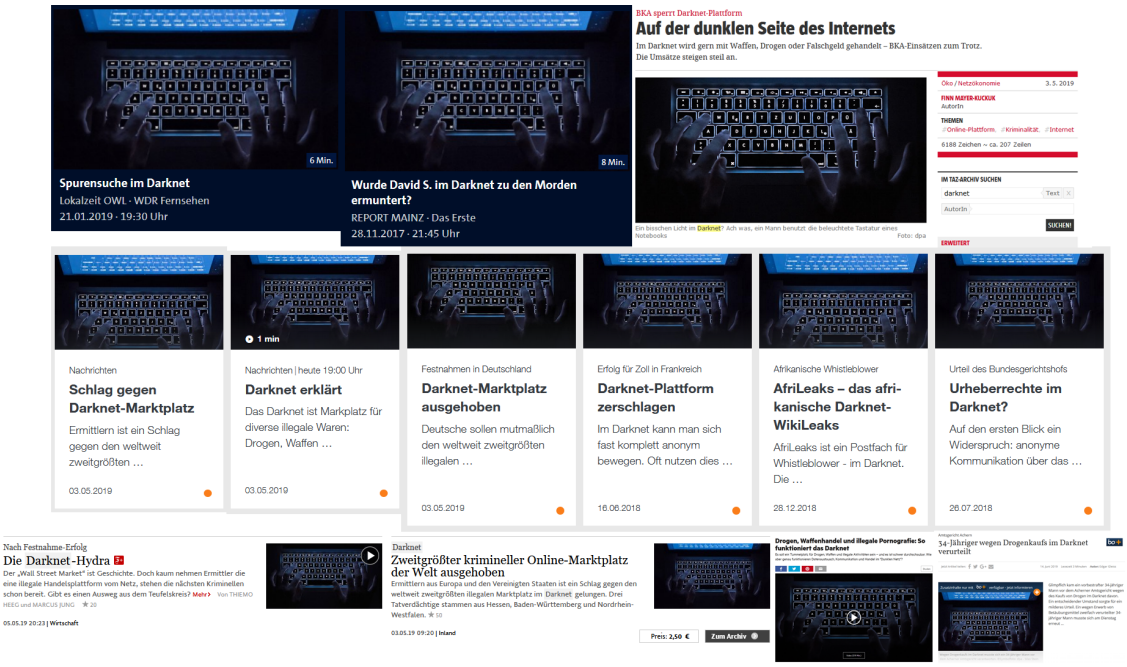

Abbildung 5: Vielfältige Bildauswahl verschiedener Nachrichtenportale

Egal mit wem man sich über das Darknet unterhält, weckt es doch meist ein sehr spezifisches Bild. Manche denken vielleicht an den Film *Matrix*, andere an die Serie *How to sell drugs online (fast)*. Oft wird es mit der gleichen Ästhetik verbunden, mit der auch Hacker dargestellt werden. Dunkel, geheim, mysteriös, gefährlich, illegal.
Wie Abbildung 5 zeigt, sind sich verschiedene Nachrichtenportale darüber einig, welches Bild das Darknet am besten repräsentiert. Sie alle wählen die gleiche Illustration: Ein Laptop im Dunkeln, nur die Tastatur leuchtet, spiegelt sich im Bildschirm wider und eine Person tippt etwas ein. Auch Abbildung 6 zeigt, dass die Bildsprache sehr eindeutig ist. Die Farben sind meist schwarz, weiß und blau. Die Motive sind leuchtende Tastaturen, spiegelnde Bildschirme, tippende Hände, Menschen, die sich mit einer Kapuze verhüllen. Auch Netzwerkkabel und ein Hologramm-Globus sind zu sehen. Doch warum ähneln sich alle Bilder so sehr? Wie im Kapitel *Nutzung des Darknets* diskutiert, hat das Darknet durchaus auch einen sozial erwünschte Nutzen, der nicht unbedingt in einem dunklen Hinterzimmer ausgeführt werden muss.

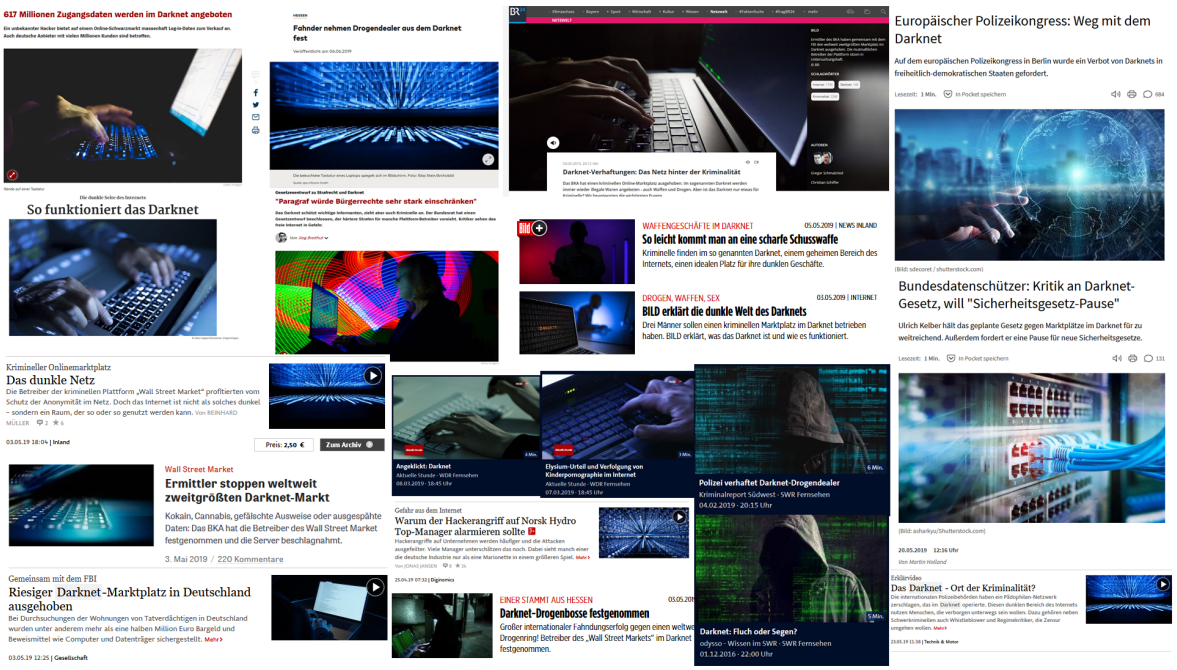

Abbildung 6: Eindeutige Bildsprache bei Artikeln über das Darknet

Wenn man sich überlegt, welche Adjektive das Konzept eines Darknets am besten beschreiben, so kommt man zum Beispiel auf: anonym, digital, modern, global, vernetzt. Und man könnte auch den ausgewählten Bildern diese Eigenschaften zuschreiben. Die Menschen auf den Bildern sind nicht zu erkennen, sie scheinen irgendwas an Tastaturen einzutippen, die durchaus modern wirken – was man von ihnen sehen kann zumindest. Globus, Netzwerkkabel – die Menschen sind wohl auch untereinander vernetzt.
Doch warum sind alle Bilder so dunkel, geheimnisvoll? Nun, das könnte vielleicht am Namen *Darknet* selbst liegen. Die Assoziation der *dunklen Seite des Internets* scheint darin ja schon festgeschrieben. Diese Frage scheinen sich auch Darknet-User immer wieder selbst zu stellen, wie eine sieben Jahre alte Reddit-Konversation beispielhaft zeigt: „‚darknet' sounds to many like a platform for a bunch of people who want to pirate movies or share child porn. Why not name it something that doesn't sound evil and computer-hacker-ish?" [21] Angeblich wurde der Name *Darknet* bei der Schaffung durch *ARPANET* (vgl Kapitel *Hintergründe des Tor-Netzwerks*) vergeben, doch fehlen dazu ausreichende Belege. [22]
Es stellt sich die Frage, ob vordergründig der Name *Darknet* die Darstellungen oder die Wahrnehmung in der Gesellschaft prägt – oder ob auch die Mediendarstellung Einfluss auf das Bild der *dunklen Seite des Internets* hat. Und sind die einseitigen bildlichen

Darstellungen überhaupt einschlägig in der Meinungsbildung, repräsentieren sie doch gut die Eigenschaften des Darknets? Schaut man auf die Überschriften, die mit den Bildern einhergehen, so scheinen sie sich größtenteils auf die illegale Seite des Darknets zu beziehen: „Darknet-Drogenbosse festgenommen“ [23], „Das Darknet – Ort der Kriminalität?“ [24] oder „Drogen, Waffenhandel und illegale Pornografie: So funktioniert das Darknet“ [25].
Um zu erfahren, ob das Darknet medial so einseitig dargestellt wird, wie es die Bildsprache vermuten lässt, lohnt sich ein Blick in den Text.

3.2 Inhaltsanalyse

Wie im vorherigen Kapitel *Bildsprache* schon angesprochen, scheint die öffentliche Meinung und die mediale Darstellung vom Darknet sehr einseitig geprägt: Sie bezieht sich immer wieder auf die Illegalität. Doch auch im Kapitel *Nutzung des Darknets* wurde dargestellt, dass Darknets viele verschiedene Nutzen haben, sogar teilweise erwünscht und unabdingbar für eine demokratische Gesellschaft. Woher kommt diese schlechte Meinung? Ist die mediale Darstellung tatsächlich so negativ geprägt? Was wird genau über das Darknet gesagt?

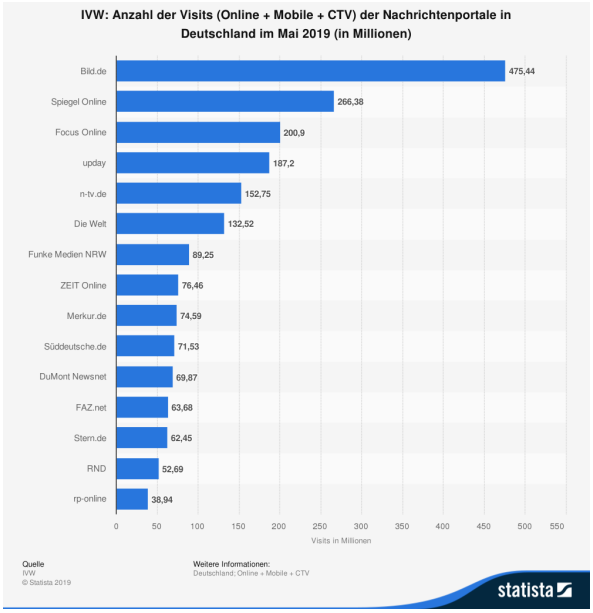

Abbildung 7: Meistbesuchte Online-Nachrichtenportale im Mai 2019 [26]

Um dies herauszufinden, haben wir die aktuellen Texte untersucht, die über das Darknet berichten. Wir haben die fünf meistbesuchten Nachrichtenportale Deutschlands (im Mai 2019) herausgesucht. Wie in Abbildung 7 zu sehen, sind diese: *Bild.de*, *Spiegel Online*, *Focus Online*, *n-tv.de* und *Die Welt*. [1] Auf diesen Plattformen haben wir Artikel analysiert, die folgende Kriterien erfüllen: Das Wort „Darknet“ ist im Titel oder Untertitel enthalten und sie sind aus dem Jahr 2019 (vor dem 26. Juni 2019). Zusätzlich begrenzten wir es auf die 10 neuesten Artikel pro Plattform, damit nicht eine Plattform die gesamte Analyse dominiert. So wurden insgesamt 35 Artikel ausgewertet.

Abbildung 8: Wortwolke der häufigsten Wörter

[1] Da *upday* nur über eine App zugänglich ist und daher mit unserem Analyseprogramm *MAXQDA 2018* inkompatibel war, musste es ausgelassen werden.

Rang	Wort	Dokumente %	Häufigkeit
1	darknet	100,00	195
2	tor	34,29	67
3	market	51,43	64
4	drogen	71,43	60
5	daten	60,00	59
5	ermittler	54,29	59
5	street	45,71	59
5	waren	65,71	59
9	online	60,00	57
10	plattform	54,29	56
11	betreiber	48,57	50
11	wall	37,14	50
13	internet	60,00	45
14	netzwerk	34,29	35
15	jahren	54,29	34
16	marktplatz	40,00	33
17	web	14,29	31
18	weltweit	48,57	30
19	euro	57,14	29
20	illegale	42,86	28
21	deutschland	45,71	27
21	illegalen	48,57	27
21	millionen	42,86	27
24	ermittlungen	48,57	26
24	nutzer	40,00	26
26	bka	34,29	25
26	kriminelle	40,00	25
26	server	51,43	25
26	waffen	28,57	25
30	welt	42,86	24

Abbildung 9: Tabellarische Übersicht der häufigsten Wörter

Die vorkommenden Worte in den Artikeln wurden nach Häufigkeit sortiert, dabei wurden Stoppworte, d. h. Worte, die keine eigenständige Bedeutung beitragen (z.B. *und*, *man*, *hatten*), ausgeschlossen. Die Ergebnisse sieht man als Wortwolke in Abbildung 8 und tabellarisch in Abbildung 9. In der Wortwolke sind die Wörter größer, je öfter sie absolut in den Texten vorkommen. In der Tabelle sieht man in der Spalte *Häufigkeit* die absolute Häufigkeit (Wie oft wird das Wort genannt?), auf die sich auch die Wortwolke bezieht. In der Spalte *Dokumente %* sieht man den Anteil in wie vielen Artikeln (von allen 35 Artikeln) das Wort vorkommt. Das Wort „Darknet“ kommt in allen Dokumenten vor (das war auch die Voraussetzung) und wird insgesamt 195 mal genannt.

Was sagen diese Ergebnisse nun aus? Auf Platz zwei der Häufigkeit ist „Tor“, was darauf schließen lässt, dass zumindest das spezifische Darknet erwähnt wird, auf das man sich bezieht. Andere Darknets wie z.B. FreeNet finden sich gar nicht unter den häufigsten Wörtern. Auch wird „Tor“ nur in einem Drittel (34,29 %) der Artikel überhaupt erwähnt. Das könnte darauf schließen lassen, dass die restlichen zwei Drittel nicht erklären, wie Darknets überhaupt funktionieren. Andere technisch konnotierte Begriffe wie „Daten“, „Internet“, „Netzwerk“ und „Server“ lassen sich ebenfalls finden. Jedoch sind diese noch auf einem recht oberflächlichen fachsprachlichen Ebene, was die These bestärkt, dass der Großteil der Texte die Funktionsweise von Darknets nicht erklären. In 71,43 % der Artikel (und der damit höchsten Prozentzahl) findet sich das Wort „Drogen“. Das lässt vermuten, dass sich der Großteil der Artikel auf Drogenhandel beziehen. Und tatsächlich finden sich häufig Worte, die sich auf Online-Marktplätze beziehen: „wall street market“ (einer der Marktplätze, die Anfang 2019 polizeilich gesperrt wurden), „Waren“, „Plattform“, „Marktplatz“, „Waffen“, „Millionen“ und „Euro“.
Der dritte inhaltliche Schwerpunkt sind Begriffe, die sich auf Illegalität und polizeiliche Maßnahmen beziehen. Dort findet man „illegale“, „illegalen“, „Ermittler“, „Ermittlungen“, „BKA“ und „Kriminelle“.
Zusammen lässt dies darauf schließen, dass die meisten dieser Artikel über Verfahren gegen Marktplätze im Darknet berichten. Damit spezialisieren sie sich auf illegale Handlungen wie Drogen- und Waffenhandel. Auffällig ist, dass keine Begriffe vorkommen, die den sozial erwünschten Nutzen des Darknets betonen. Solche wären zum Beispiel Anonymität, Zensur/unzensiert, Sicherheit, Whistleblower, Journalismus, Aktivismus. So bestätigt sich also die Vermutung, dass in der Berichterstattung über das Darknet oft die negativen Aspekte betont werden und sie ähnlich einseitig ist, wie ihre Bildwahl vermuten lässt.
Nicht beantworten lässt sich die Frage, was wovon beeinflusst wird. Ist die allgemeine Meinung durch die Berichterstattung geprägt oder gibt die Berichterstattung nur wieder, was die Allgemeinheit sowieso denkt? Und ist es denn überhaupt so erstaunlich, dass in den Medien größtenteils über Straftaten berichtet wird? Vielleicht ist ja das Darknet auch einfach nur voller Krimineller? Im folgenden Kapitel soll etwas *Licht ins Dunkel* gebracht werden, wie illegal das Darknet wirklich ist. Daran klärt sich zumindest die Frage, ob die Berichterstattung über das Darknet den Aktivitäten im selben angemessen ist.

4 Gesetzeslage

4.1 Ist-Zustand

Im Kapitel *Mediendarstellung des Darknets* wurde gezeigt, dass die Mehrheit der Gesellschaft oft nur von kriminellen Machenschaften im Darknet mitbekommt. Neben die Annahme, dass sie kein Darknet benötigen, weil sie nichts Illegales tun möchten, mischt sich die Vermutung, dass *alles* im Darknet illegal sei. Vielleicht schon das Nutzen des Tor-Browsers? Oder der Aufruf einer .onion-Adresse? Macht man sich damit schon strafbar? Die kurze Antwort ist: Nein. Das Nutzen des Tor-Browsers, sowie das Surfen auf .onion-Adressen ist legal. „Wer allerdings nicht auf einschlägigen Seiten unterwegs ist, hat nicht zu befürchten. Im Darknet zu surfen ist per se nicht illegal“, schreibt eine online Anwaltsberatung. [27] „Einschlägige Seiten“ meint hier alles, was auch außerhalb des Darknets rechtswidrig ist. So ist es natürlich illegal, wenn man Drogen, Waffen und Ähnliches kauft. Vorsichtig sollte man dennoch sein, wenn man eigentlich legale Dinge kauft, denn auch diese können aus Diebstählen kommen und damit würde man sich der Hehlerei schuldig machen. Genauso wie im Darknet keine Steuer- oder Zollabgaben gezahlt werden müssen, was je nach Fall auch Konsequenzen haben kann. [28]
Das Darknet ist kein rechtsfreier Raum – bei einem Rechtsbruch ist nur schwieriger festzustellen, wer ihn begangen hat. Dennoch ist es nicht unmöglich. Viele Online-Marktplätze, die u. a. Drogen verkauften, wurden schon hochgenommen, ihre Betreiber teilweise bereits verurteilt – z.B. *the Silk Road* oder *Wall Street Market*.
Die Ermittler*innen haben dabei verschiedene Herangehensweisen: „Verdeckte Ermittlungen, Hacking, Open Source Informationen, Massenüberwachung, Durchkämmen beschlagnahmter Daten, den Geldfluss nachverfolgen, das Postsystem.“ [29] Dabei scheinen gerade Daten wie „IP-Adressen, Domain-Namen, Klarpersonalien, Anschriften, PGP-Keys und Bitcoin-Adressen“ [30] den Ermittler*innen zu helfen, die Verdächtigen ausfindig zu machen. Jedoch veröffentlichen das Bundeskriminalamt und die Bundespolizei keine Informationen oder Statistiken, die zeigen, wie sie genau ermitteln und wie erfolgreich diese Ermittlungen sind. Bereits 2016 stellte Martina Renner der Linken eine Kleine Anfrage im Bundestag, die mehr Transparenz über die Ermittlungen forderte. Die Antworten blieben vage, oft wurde betont: „Hierüber wird im BKA keine Statistik geführt.“ [30] Gleichzeitig versuchen BKA und Bundespolizei immer wieder ihre Befugnisse für die Ermittlung auszuweiten, ohne zu evaluieren, wie erfolgreich die bisherigen Befugnisse sind.

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Abbildung 10: Tabellarische Übersicht der analysierten Darknet-Webseiten und ihrer Kategorien [16, S.21]

Daher stellt sich die Frage: Ist das nötig? Wird das Darknet tatsächlich nur für Straftaten genutzt? In der Beschaffenheit des Darknets liegt es, dass die Webseiten nicht indexiert, das heißt für Suchmaschinen zugreifbar, sind. Wie soll man da herausfinden, wie es tatsächlich genutzt wird? Mehrere Studien haben sich bereits der Erforschung des Darknets gewidmet und mit sogenannten Crawlern die Webseiten durchsucht. Diese beginnen auf Seiten mit Linklisten, wie Wikis, und testen alle angegebenen Links, speichern ihre Daten und arbeiten sich so immer tiefer vor.
Die Abbildungen 10 und 11 zeigen die Ergebnisse dieser Studien. In der Studie zu Abbildung 10 wurden 2.723 aktive Darknet-Webseiten gefunden und in verschiedene Kategorien eingeteilt, z.B. Drogen, Finanzen, Hacking und Soziales. Davon fallen 1.547 Seiten in eine illegale Kategorie. Damit sind 58,8 % als illegal einzuordnen. Die Studie zu Abbildung 11 unterteilt in Webseiten ohne Zugangsbeschränkung (z.B. Login), davon sind 37,4 % illegal, und Webseiten mit Zugangsbeschränkung, davon sind 56,4 % illegal. Natürlich ist die Definition, was illegal ist, immer abhängig von dem Land, in dem die Studie veröffentlicht wird. So gibt es weitreichende Unterschiede, wie verschie-

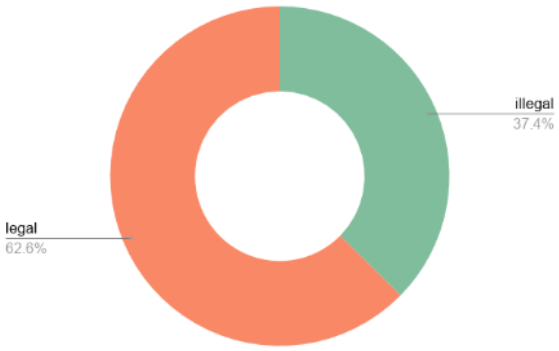

Fig. 12. Approximately 60% of all pages are legal in the visible part of the darknet.

Fig. 13. When accumulating the pages by hidden service, we find that above 50% of all hidden services contain illegal content.

Abbildung 11: Verhältnis der legalen zu illegalen Darknet-Webseiten [14, S.19]

dene Drogen und Medikamente eingeschätzt werden. Auch die gesetzlichen Regelungen zu Whistleblowing unterscheiden sich mitunter stark.
Egal ob einem diese Prozentzahlen im ersten Moment viel oder wenig vorkommen, so ist eindeutig, dass das Darknet nicht ausschließlich für Illegales genutzt wird. Zusammenfassend lässt sich sagen, dass es durchaus Kriminalität im Darknet gibt – allerdings nicht so exklusiv, wie es in der Öffentlichkeit den Anschein hat. Dazu kommt, dass es den Behörden momentan durchaus möglich ist, im Darknet erfolgreich zu ermitteln.

4.2 §126a

Die in Kapitel *Ist-Zustand* beschriebene rechtliche Situation, scheint dennoch nicht ausreichend zu sein. So legt der Ministerpräsident Nordrhein-Westfalens dem Bundesrat im Januar 2019 einen Gesetzesänderungsantrag vor, der §126 des Strafgesetzbuchs erweitern soll. Der bestehende Paragraph hier in gekürzter Fassung:

„§126 STGB Störung des öffentlichen Friedens durch Androhung von Straftaten:

(1) Wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören,

1. *einen der [..] Fälle des Landfriedensbruchs,*
2. *einen Mord (§ 211), Totschlag (§ 212) oder Völkermord [...] oder ein Verbrechen gegen die Menschlichkeit [...] oder ein Kriegsverbrechen [...]*
3. *eine schwere Körperverletzung (§ 226),*
4. *eine Straftat gegen die persönliche Freiheit [...]*
5. *einen Raub oder eine räuberische Erpressung [...]*
6. *ein gemeingefährliches Verbrechen [...] oder*
7. *ein gemeingefährliches Vergehen [...]*

androht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, wider besseres Wissen vortäuscht, die Verwirklichung einer der in Absatz 1 genannten rechtswidrigen Taten stehe bevor.“ [31]

Dieser Paragraph stellt nicht nur den unter Strafe, der Straftaten durchführt, sondern auch den, der sie androht oder vortäuscht. Wie bereits erwähnt, gelten alle diese Gesetze natürlich ebenfalls im Darknet und können dort strafrechtlich verfolgt werden. Dennoch soll der Paragraph um §126a erweitert werden. Dieser ebenfalls in gekürzter Fassung:

„§126a Änderung Anbieten von Leistungen zur Ermöglichung von Straftaten

(1) Wer eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten im Sinne von Satz 2 zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. [...]

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 Satz 2 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig begeht.“ [32]

In der Begründung des Änderungsvorschlages wird klar, dass diese Gesetzesänderung darauf abzielt, auch die Betreibenden von Darknet-Marktplätzen besser strafrechtlich verfolgen zu können, nicht nur diejenigen, die selbst illegale Waren anbieten. „Diese Angebote stellen eine erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass die geltende Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung bietet.“ [32], heißt es in der Begründung. Obwohl kurz vorher steht: „Die Zentralstellen der Staatsanwaltschaften für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren jedoch bereits zahlreiche Ermittlungsverfahren gegen die Verantwortlichen einschlägiger Foren oder Plattformen und deren Nutzer geführt, z. B. ‚Deutschland im Deep Web‘ oder ‚crimenetwork.biz‘.“ [32] Anscheinend war in diesen Fällen die strafrechtliche Verfolgung doch möglich, so wurde der Betreiber des Forums ‚Deutschland im Deep Web‘ zu sechs Jahren Haft verurteilt. [33]
Die Formulierung des §126a hat einige Kritik geerntet. Denn auch wenn die Zielobjekte Darknet-Marktplätze illegaler Waren sind, so ist die Formulierung „internetbasierte Leistung [...], deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten [...] zu ermöglichen“ sehr vage. Es könnte genauso nicht auf einzelne Marktplätze, sondern auf den Tor-Browser angewendet werden. Damit wären nicht nur kriminelle Handlungen im Darknet illegal, sondern auch die andere Hälfte an legalen Handlungen wäre unmöglich.
Der Bundesdatenschutzbeauftragte Ulrich Kelber kritisiert diese vage Formulierung: „Wann ist der Dienst darauf ausgerichtet, die Begehung rechtswidriger Taten ‚zu ermöglichen oder zu fördern‘? Und wie konkret muss dies geklärt sein? [...] Wenn man nach einer Kneipenschlägerei nicht beweisen kann, wer sich daran mutwillig beteiligt hat, kommt man doch auch nicht auf die Idee, alle zu bestrafen, die in der Nähe herumstanden“ [34] Er kritisiert ebenfalls, dass durch diese offene Formulierung ein Anfangsverdacht viel zu leicht gefunden wäre und dass dadurch die Bürgerrechte stark eingeschränkt würden. Zudem forderte er eine Pause für Sicherheitsgesetze, bevor die alten nicht evaluiert seien. [34] Wie im Kapitel *Ist-Zustand* bereits gesagt, findet diese Evaluation nicht statt. [30]

5 Fazit

Die im Kapitel *§126a* angeschnittene Debatte über die Strafbarkeit im Darknet ist nur eine von vielen aktuellen Entwicklungen zum Thema Darknet und Internetsicherheit. So veröffentlicht Bundesinnenminister Horst Seehofer das umstrittene IT-Sicherheitsgesetz 2.0, durch das das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Recht bekommen soll, Bürger*innen zu hacken und ihre Systeme auszuspähen. [35] Und der parlamentarische Staatssekretär Günther Krings eröffnet den Europäischen Polizeikongress 2019 wie folgt:

„Ich verstehe, warum das Darknet einen Nutzen in autokratischen Systemen haben kann. Aber in einer freien, offenen Demokratie gibt es meiner Meinung nach keinen legitimen Nutzen. Wer das Darknet nutzt, führt in der Regel nichts Gutes im Schilde. Diese einfache Erkenntnis sollte sich auch in unserer Rechtsordnung widerspiegeln.“ [36]

Diese Arbeit sollte zeigen, dass das Darknet sehr viel mehr ist, als ein Tummelplatz für kriminelle Machenschaften. Es kommt also zu kurz zu behaupten, dass User eines Darknets „nichts Gutes im Schilde [führen]“. Damit werden die User diffamiert und das eigentliche Problem verschoben. Denn die im Darknet praktizierten Straftaten sollten der Fokus bleiben, der Handel von Drogen und Waffen zum Beispiel – Straftaten, die durchaus erfolgreich vom BKA verfolgt werden.
Darüber hinaus sollte diese Arbeit zeigen, dass die Öffentlichkeit es sich zu einfach macht, das Darknet als die Ursache für Straftaten darzustellen. Denn wer eingesteht, dass man in einem autokratischen Staat das Darknet braucht, der sollte auch erkennen, dass es ein demokratisches Werkzeug ist. Verbietet man dieses Werkzeug nun in einer Demokratie, ist sie dann noch demokratisch?
Während das *normale* Internet immer massiver überwacht wird, sowohl durch Staaten als auch Unternehmen, wird die überwachungssichere Alternative kriminalisiert. Mit der aktuellen Offensive gegen das Darknet scheint nicht illegaler Warenhandel im Fokus zu stehen, sondern ein Konzept: Anonymität.

Literatur

[1] Andy Greenberg. (2013, 2. Oktober). End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market. Abgerufen 15. August 2019, von https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

[2] Virginia Kirst. (2015, 19. August). Ashley-Madison-Hack: Wie komme ich ins Darknet? Abgerufen 15. August 2019, von https://www.welt.de/wirtschaft/webwelt/article145402685/Wie-komme-ich-eigentlich-ins-Darknet.html

[3] Markus Böhm. (2017, 13. März). Bluttaten von Herne: Darknet-Killer ohne Darknet. Abgerufen 15. August 2019, von https://www.spiegel.de/netzwelt/netzpolitik/herne-die-geschichte-vom-darknet-killer-ohne-darknet-a-1138492.html

[4] Süddeutsche.de. (2018, 19. Dezember). OEZ-Anschlag - Sechs Jahre Haft für Darknet-Betreiber. Abgerufen 15. August 2019, von https://www.sueddeutsche.de/muenchen/oez-anschlag-urteil-darknet-1.4259420

[5] Google Trends. (2019, 15. August). Suchbegriff darknet. Abgerufen 15. August, 2019, von https://trends.google.de/trends/explore?date=all&geo=DE&q=darknet

[6] Julia Görmer. (2018). Anonymität im Darknet. Nutzer und Usability im Vergleich der drei Hauptvertreter. Abgerufen von https://opendata.uni-halle.de/bitstream/1981185920/12783/1/Bachelorarbeit%20Julia%20G%c3%b6rmer.pdf

[7] The Web Robot Pages. (o.D.). About /robots.txt. Abgerufen 14. August, 2019, von https://www.robotstxt.org/robotstxt.html

[8] Stefan Mey. (2017, 10. November). „Tor " in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets. Aus Politik und zeitgeschichte - Darknet, APUZ (46-47/2017). Abgerufen von https://www.bpb.de/apuz/259135/tor-in-eine-andere-welt?p=all

[9] Ines Maria Eckermann. (2019, 7. Juni). Was ist das Darknet? Plattform für illegale Geschäfte | G DATA. Abgerufen 15. August 2019, von https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet

[10] The Tor Project, Inc. (o.D.-b). Tor Project: Overview. Abgerufen 15. Augus, 2019, von https://2019.www.torproject.org/about/overview.html.en

[11] Ty McCormick. (2013, 9. Dezember). The Darknet: A Short History. Abgerufen 15. August 2019, von https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/

[12] Das Tor Project. (o.D.). Privatsphäre und Freiheit Online - Verlauf. Abgerufen 15. August, 2019, von https://www.torproject.org/de/about/history/

[13] Tobias Bug. (2017, 6. Dezember). Das Darknet: Abgründe des Internets. Abgerufen 14. August 2019, von https://www.faz.net/aktuell/wirtschaft/das-darknet-abgruende-des-internets-15326787.html?printPagedArticle=true

[14] Georgia Avarikioti, Roman Brunner, Aggelos Kiayias, Roger Wattenhofer, Dionysis Zindros. (2018). Structure and Content of the Visible Darknet. Abgerufen von https://arxiv.org/pdf/1811.01348.pdf

[15] The Tor Project, Inc. (o.D.-b). Tor Project: FAQ - How can I share files anonymously through Tor? Abgerufen 15. August 2019, von https://2019.www.torproject.org/docs/faq.html.en#FileSharing

[16] Daniel Moore, Thomas Rid. (2016). Cryptopolitik and the Darknet. Abgerufen von https://doi.org/10.1080/00396338.2016.1142085

[17] Jan Schallaböck. (2019, 23. Juli). Was ist und wie funktioniert Webtracking? Abgerufen 15. August 2019, von https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386

[18] Oxford Internet Institute Web Team. (2014, 9. Juni). The anonymous Internet. Abgerufen 15. August 2019, von http://geography.oii.ox.ac.uk/the-anonymous-internet/

[19] E-Commerce-Leitfaden. (2009). Kapitel 3: Lasst Zahlen sprechen - kontinuierliche Verbesserung durch Web-Controlling. Abgerufen 15. August 2019,

von https://www.ecommerce-leitfaden.de/ecl-v2/140-kapitel-3-lasst-zahlen-sprechen-kontinuierliche-verbesserung-durch-web-controlling

[20] Karolin Schwarz. (2019, 3. Mai). Wahlmanipulation: Diese Schutzmaßnahmen treffen Internetkonzerne - bpb. Abgerufen 15. August 2019, von https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/290577/schutzmassnahmen-der-internetkonzerne

[21] Reddit. (2011, 19. November). r/darknetplan - Just a thought: the name "DarkNetïs not going to appeal to the mainstream.. Abgerufen 12. August, 2019, von https://www.reddit.com/r/darknetplan/comments/mid03/just_a_thought_the_name_darknet_is_not_going_to/

[22] Wikipedia. (2019, 13. August). Darknet. Abgerufen 13. August 2019, von https://en.wikipedia.org/w/index.php?title=Darknet&oldid=910615835

[23] Bild.de. (2019, 3. Mai). „Wall Street Market“: Darknet-Drogenbosse festgenommen. Abgerufen 13. August 2019, von https://www.bild.de/regional/frankfurt/frankfurt-aktuell/wall-street-market-darknet-drogen-bosse-festgenommen-61640728.bild.html

[24] Frankfurter Allgemeine Zeitung GmbH. (2019, 23. Mai). Erklärvideo: Das Darknet - Ort der Kriminalität? Abgerufen 13. August 2019, von https://www.faz.net/aktuell/technik-motor/erklaervideo-das-darknet-ort-der-kriminalitaet-16202393.html

[25] STERN.de. (2019, 3. Mai). Drogen, Waffenhandel und illegale Pornografie: So funktioniert das Darknet. Abgerufen 13. Augus, 2019, von https://www.stern.de/digital/darknet--was-ist-das-und-wie-funktioniert-es--8694104.html

[26] IVW. (n.d.). IVW: Anzahl der Visits (Online + Mobile + CTV) der Nachrichtenportale in Deutschland im Mai 2019 (in Millionen). In Statista - Das Statistik-Portal. Abgerufen 26. Juni 2019, von https://de.statista.com/statistik/daten/studie/154154/umfrage/anzahl-der-visits-von-nachrichtenportalen/

[27] Anwalt.org. (o.D.). Im Darknet surfen. Abgerufen 13. August 2019, von https://www.anwalt.org/im-darknet-surfen/

[28] Motherboard Staff. (2017, 24. Juli). 9 Darknet-Fragen, die sich jeder stellt, aber niemand zu fragen traut - VICE. Abgerufen 12. August 2019, von https://www.vice.com/de/article/wj8a9q/9-darknet-fragen-die-sich-jeder-stellt-aber-niemand-traut-zu-fragen

[29] Joseph Cox. (2016, 20. Juli). Sieben Wege, wie die Polizei Darknet-Nutzern auf die Schliche kommt - VICE. Abgerufen 12. August, 2019, von https://www.vice.com/de/article/aek5y4/7-wege-wie-die-polizei-dir-im-darknet-auf-die-spur-kommt

[30] Anna Biselli. (2016, 26. August). Bundesregierung: Keine Ahnung, wie derzeit im Netz ermittelt wird - aber trotzdem neue Befugnisse fordern. Abgerufen 12. August 2019, von https://netzpolitik.org/2016/bundesregierung-keine-ahnung-wie-derzeit-im-netz-ermittelt-wird-aber-trotzdem-neue-befugnisse-fordern/

[31] Dejure.org Rechtsinformationssysteme GmbH. (o.D.). § 126 StGB Störung des öffentlichen Friedens durch Androhung... - dejure.org. Abgerufen 26. Juni 2019, von https://dejure.org/gesetze/StGB/126.html

[32] Bundesrat. (2019). Entwurf eines Strafrechtsänderungsgesetzes. Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen (Drucksache 33/19). Abgerufen von https://www.bundesrat.de/SharedDocs/drucksachen/2019/0001-0100/33-19.pdf?__blob=publicationFile&v=1

[33] Christoph Lemmer. (2018, 19. Dezember). Prozess um Darkweb-Forum DiDW: Sechs Jahre Haft fÃ¼r Administrator. Abgerufen 15. August 2019, von https://www.heise.de/newsticker/meldung/Prozess-um-Darkweb-Forum-DiDW-Sechs-Jahre-Haft-fuer-Administrator-4256723.html

[34] Max Muth. (2019, 20. Mai). Oberster Datenschützer kritisiert Darknet-Gesetzentwurf. Abgerufen 26. Juni 2019, von https://www.sueddeutsche.de/digital/darknet-kelber-datenschutz-polizei-1.4453166

[35] Andre Meister. (2019, 18. April). IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. Abgerufen 13. August 2019, von https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-

wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/

[36] Detlef Borchers. (2019, 20. Februar). Europäischer Polizeikongress: Weg mit dem Darknet. Abgerufen 26. Juni 2019, von https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Weg-mit-dem-Darknet-4313276.html