HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Herr
Oscar Trepte

Erstellung einer aktuellen Übersicht von Tor-Hidden-Webservices und deren Inhalten

Mittweida, Dezember 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Erstellung einer aktuellen Übersicht von Tor-Hidden-Webservices und deren Inhalten

Autor:
Oscar Trepte

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w6-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Felix Fischer, M.Sc.

Einreichung:
Mittweida, 24.12.2023

Verteidigung/Bewertung:
Mittweida, 2024

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Creation of an up-to-date overview of Tor hidden web services and their content

Author:
Oscar Trepte

Course of Study:
General and digital forensics

Seminar Group:
FO20w6-B

First Examiner:
Prof. Dr. rer. nat. Dirk Labudde

Second Examiner:
Felix Fischer, M.Sc.

Submission:
Mittweida, 24.12.2023

Defense/Evaluation:
Mittweida, 2024

Bibliografische Beschreibung

Trepte, Oscar:
Erstellung einer aktuellen Übersicht von Tor-Hidden-Webservices und deren Inhalten. – 2023. – 67 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2024.

Referat

In dieser Arbeit wurde ein aktueller Überblick über die im Dark Web verfügbaren Hidden Services erstellt. Dazu wurden Onion-Adressen mit Hilfe von Suchmaschinen und Verzeichnissen gewonnen.

Über diese Onion-Adressen wurden Hidden Services aufgerufen und untersucht. Die gefundenen Hidden Services wurden in Kategorien eingeteilt und anschließend näher betrachtet. Dabei wurde vor allem auf die Inhalte eingegangen. Diese wurden untereinander und mit Webseiten aus dem Clear Web verglichen.

Es konnten zahlreiche verschiedene angebotene Inhalte festgestellt werden. Sowohl legale als auch illegale Inhalte. Die Anzahl der Hidden Services mit illegalen Inhalten überwiegt. Die größte Kategorie stellen digitale Marktplätze dar. Auf diesen werden verschiedene, hauptsächlich illegale Produkte und Dienstleistungen verkauft.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AES ..... Advanced Encryption Standard

BBC ..... British Broadcasting Corporation

BKA ..... Bundeskriminalamt

CD ..... Compact Disc

CIA ..... Central Intelligence Agency

CSAM ..... Child Sexual Abuse Material

DMT ..... Dimethyltryptamin

FAQ ..... Frequently Asked Questions

FBI ..... Federal Bureau of Investigation

HSDir ..... Hidden Service Directory

HTML ..... Hypertext Markup Language

HTTP ..... Hypertext Transfer Protocol

IP ..... Internet Protocol

LSD ..... Lysergsäurediethylamid

MDMA ..... Methylendioxymethylamphetamin

PGP ..... Pretty Good Privacy

PRISM ..... Planning tool for Resource Integration, Synchronization, and Management

Tails ..... The Amnesic Incognito Live System

URL ..... Uniform Resource Locator

USB ..... Universal Serial Bus

1 Einleitung

1.1 Motivation

Cybercrime spielt eine immer größere Rolle. Sowohl bei der Strafverfolgung als auch im Alltag von Privatpersonen. Es wird vor Phishing E-Mails und Hackerangriffen gewarnt. Rentner müssen inzwischen ebenso auf die Gefahren des Internets vorbereitet werden wie Schüler.

Doch neben all diesen Sachverhalten, die immer mehr an die Öffentlichkeit heran getragen werden verbirgt sich noch ein weiterer Schauplatz. Das sogenannte Dark Web. Dieser Name für das Tor-Netzwerk, suggeriert eine dunkle Version des Internets zu sein und tatsächlich sieht man immer wieder Schlagzeilen, die eben dies anscheinend bestätigen.

“Student aus Landshut wegen Drogenhandel im Darknet verurteilt“, “Gestohlene Daten und Zugänge von jedem dritten Unternehmen im Darknet“ oder “Drogenhandel: Europol schließt Dark-Web-Portal Monopoly Market - fast 300 Festnahmen“ sind nur einige Beispiele von vielen. [1–3]

So rückt das Dark Web immer mehr in den Fokus der Öffentlichkeit. Doch der Forschung ist es schon länger bekannt. Das Tor-Netzwerk ist ein Netzwerk aus mehreren Servern und Computern, das seinen Nutzern Anonymität im Internet ermöglicht. Zugriff wird mit Hilfe des Tor-Browsers erhalten und nur mit diesem können auch die sogenannten Hidden Services erreicht werden.

Es existieren bereits zahlreiche wissenschaftliche Arbeiten die sich mit dem Tor-Netzwerk, dessen Funktion sowie dessen Sicherheitslücken beschäftigen. Aber auch das Erlangen von möglichst vielen Onion-Adressen, die den Zugang zu Hidden Services ermöglichen wurde bereits auf mehrere Arten durchgeführt.

Ebenso wurden Hidden Services bereits nach ihren Inhalten klassifiziert und nach legal und illegal unterschieden. So werden Rückschlüsse auf den Anteil der Kriminalität im Dark Web geschlossen.

1.2 Zielstellung

Ziel dieser Arbeit ist es, die im Dark Web verfügbaren Hidden Services genauer zu untersuchen und so eine Übersicht über diese zu erstellen. Der Fokus liegt dabei auf der Analyse der Inhalte.

Es soll die Vielfalt der angebotenen Dienste eingefangen werden. Diese werden außerdem untereinander und mit Alternativen aus dem Clear Web verglichen.

Es wird auf die Benutzeroberfläche und das Webdesign eingegangen, auf die angebotenen Produkte und deren Preise. Außerdem auf das Verhalten und die Kommunikation der Nutzer, sowie den generellen sozialen Umgang. Die Legalität der Hidden Services wird ebenfalls betrachtet, ist aber nicht in allen Fällen eindeutig einschätzbar. Ebenso verhält es sich mit dem Aufdecken von Betrug. Hidden Services werden danach beurteilt, wie glaubwürdig sie auf den Nutzer wirken und gegebenenfalls auch nach vorhandenen Erfahrungsberichten.

1.3 Abgrenzung

Andere Arbeiten haben sich bereits mit dem Generieren und Sammeln von einer größtmöglichen Anzahl an Onion-Adressen beschäftigt. In dieser Arbeit werden stattdessen bereits existierende Ressourcen verwendet und eine kleinere Anzahl an Hidden Services analysiert. Dies geschieht um mehr Aufmerksamkeit für die detaillierte Untersuchung der einzelnen Services aufbringen zu können.

Aufgrund der Komplexität der Aufgabe ist es nicht möglich jeden Hidden Service eindeutig bezüglich seiner Legalität einzuordnen. Es wird nur eine generelle Einschätzung in die Kategorien legal, illegal und rechtliche Grauzone vorgenommen. Diese erhebt keinen Anspruch auf vollständige Richtigkeit.

Dass auch kinderpornografische Inhalte im Dark Web auftauchen, wird anerkannt. Aufgrund der deutschen Gesetzeslage wird jedoch darauf verzichtet Hidden Services, die solche Inhalte verbreiten, explizit aufzusuchen.

“Wer es unternimmt, einen kinderpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, abzurufen oder sich den Besitz an einem solchen Inhalt zu verschaffen oder wer einen solchen Inhalt besitzt, wird mit Freiheitsstrafe von einem Jahr bis zu fünf Jahren bestraft.” (§ 184b Absatz 3 StGB).

1.4 Dokumentaufbau

Nach dieser Einleitung werden im Kapitel 2 zunächst die für die Arbeit relevanten Grundlagen beschrieben. Dabei werden die wichtigsten Begriffe sowie die Funktionsweise des Tor-Netzwerkes und der Hidden Services erklärt.

Anschließend wird im Kapitel 3 die Vorgehensweise anhand der verwendeten Methoden erläutert. Die so erlangten Ergebnisse, die untersuchten Hidden Services, werden im darauffolgenden Kapitel 4 ausführlich beschrieben und ausgewertet.

Das Kapitel 5 bietet ein zusammenfassendes Fazit über die gesammelten Beobachtungen. Die Erkenntnisse, die aus den betrachteten Hidden Service erlangt wurden werden zusammengefasst.

Ein Ausblick auf mögliche zukünftige Forschungsfelder, die sich aus der Arbeit ergeben, ist im Kapitel 6 zu finden. Außerdem wurde im Rahmen dieser Arbeit eine Sammlung von Onion-Adressen erstellt.

2 Grundlagen

In diesem Kapitel werden grundlegende Begriffe erklärt, die im Verlauf der Arbeit verwendet werden. Ein gewisses informatisches Grundwissen wird vorausgesetzt. Die Funktionsweise des Tor-Netzwerkes und auch die der sogenannten Hidden Services wird jedoch nachfolgend erklärt. Zuerst erfolgt nun eine Abgrenzung von Bezeichnungen für verschiedene Bereiche des Internets.

2.1 Clear Web, Deep Web und Dark Web

Das World Wide Web ist ein globales, über das Internet erreichbares Informationssystem. Es verbindet Hypertext-Dokumente über Hyperlinks miteinander, damit Nutzer schnell und einfach zwischen Dokumenten navigieren können. Große Suchmaschinen wie Google, Bing oder DuckDuckGo indexieren diese Dokumente mit Hilfe ihrer Links und ermöglichen es ihren Nutzern damit die entsprechenden Webseiten zu finden. [4]

Webseiten, die von diesen bekannten Suchmaschinen indexiert werden, bilden das sogenannte Clear Web, auch Clearnet oder Surface Web genannt. Sie sind für die allgemeine Öffentlichkeit über eine Suchanfrage bei diesen Suchmaschinen einfach zu erreichen. Im Clear Web befinden sich beispielsweise gängige Internetshops wie Amazon, soziale Medien wie Reddit oder Instagram, Online-Enzyklopädien wie Wikipedia und viele weitere Webseiten unterschiedlichster Art. [4]

Webseiten, die nicht von der allgemeinen Öffentlichkeit über populäre Suchmaschinen erreichbar sind, gehören zum Deep Web. Um sie zu erreichen, muss die entsprechende URL direkt in einen Browser eingegeben werden. Zum Deep Web gehören auch Seiten, die verschlüsselt oder mit einem Passwort geschützt sind. Ein Beispiel hierfür sind interne Firmennetzwerke, Onlinebanking Angebote oder nur eingeschränkt erreichbare Datenbanken von Universitäten. [4]

Ein kleiner Teil des Deep Webs ist das Dark Web, auch Darknet genannt. Um Webseiten im Dark Web zu erreichen sind spezielle Technologien wie zum Beispiel ein bestimmter Browser notwendig. Hierfür wird meist der sogenannte TOR Browser verwendet. TOR steht für The Onion Routing oder The Onion Router, wird aber mittlerweile vom Tor-Projekt nicht mehr als Akronym verwendet. Das Dark Web stellt also die Menge aller Webseiten und Services dar, die nur über das Tor-Netzwerk erreichbar sind. [4]

2.2 Das Tor Netzwerk

Wie bereits erwähnt können Webseiten, die Teil des Dark Webs sind nur über das Tor-Netzwerk erreicht werden. Dieses Netzwerk ist eine Gruppe aus Servern und will bei seinen Nutzern für erhöhte Sicherheit und Privatsphäre im Internet sorgen. [5]

2.2.1 Gründung

Im Jahr 2006 wurde das The Tor Project, Inc als Nonprofit-Organisation gegründet. Die Idee zum sogenannten Onion Routing existierte jedoch bereits Mitte der 1990er Jahre. Entwickelt wurde sie von David Goldschlag, Mike Reed und Paul Syverson des U.S. Naval Research Lab. In den frühen 2000ern wurde die Idee von Roger Dingledine gemeinsam mit Paul Syverson und später auch Nick Mathewson weiterverfolgt. Im Oktober 2002 wurde der Code des Tor-Netzwerks zum ersten Mal veröffentlicht - frei zugänglich als Open Software Lizenz. [6]

Zunächst finanziell unterstützt durch die Electronic Frontier Foundation, wird das Tor Project heute immer noch durch Spenden finanziert. 2020 bis 2021 stammten 38% der Einnahmen von der U.S. Regierung und 36% aus Spenden von Einzelpersonen. Danach folgen private Organisationen und nicht US-amerikanische Regierungen, sowie Spenden von Firmen. Insgesamt erhielt das Tor Project einen Spendenbetrag in der Höhe von über 7,4 Millionen US-Dollar. [7]

Wie an der Spendenhöhe bereits zu erahnen ist, handelt es sich bei Tor um das meistgenutzte Netzwerk für anonyme Kommunikation im Internet. Gegründet, um gesicherten Zugang zum unzensierten Internet zu ermöglichen, besteht das Netzwerk heute aus ungefähr 8000 Knoten, die auch Onion Router oder Relays genannt werden (siehe Abbildung 2.1). Die namensgebende Zwiebel-Bezeichnung (engl. onion) beschreibt die grundlegende Funktionsweise des Netzwerkaufbaus.

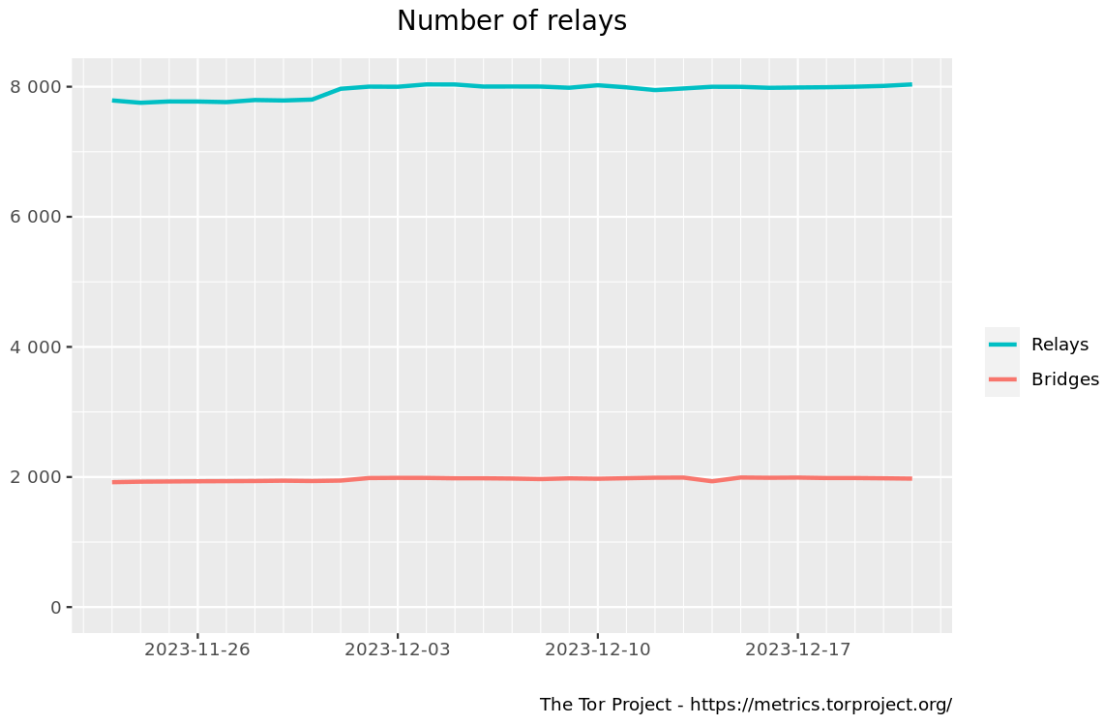

Abbildung 2.1: Statistik Anzahl der Relays im Tor-Netzwerk [8]

2.2.2 Funktionsweise

Die Grundidee des Tor-Netzwerk und des Onion Routings ist es den Datenverkehr der Nutzer über mehrere Server zu leiten. Um die Internet Protocol (IP)-Adresse der Rechner und damit die Identität der Nutzer zu verschleiern, wird der Datenverkehr außerdem bei jedem Schritt verschlüsselt. [9]

Wenn ein Nutzer auf einen Webservice zugreifen will, erfolgt der Aufbau der Verbindung wie in Abbildung 2.2 dargestellt :

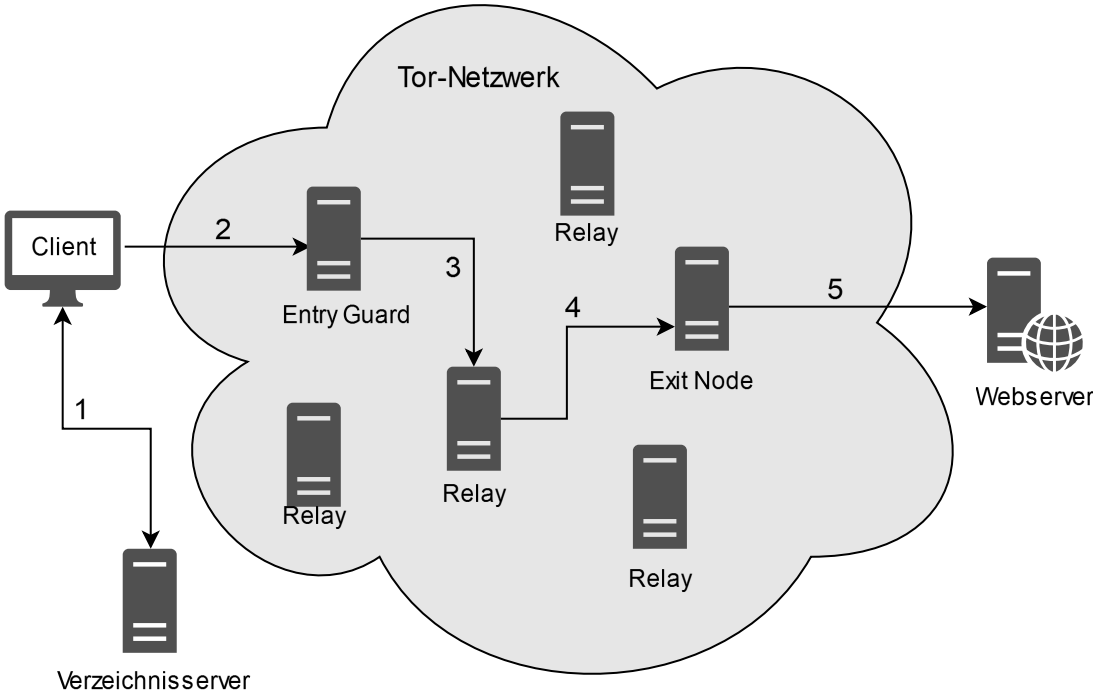

Abbildung 2.2: Funktionsweise Tor-Netzwerk basierend auf [10, 11]

Im ersten Schritt fragt der Client einen sogenannten Verzeichnisserver (engl. Directory) an (1). Dieser enthält eine Liste aller verfügbaren Tor-Knoten, die auch als Nodes oder Relays bezeichnet werden. Aus der Liste, die er vom Verzeichnisserver erhält, wählt der Client mindestens drei Knoten aus.

Der erste Knoten, der den Einstiegspunkt in das Tor-Netzwerk bildet, wird Entry Guard genannt. Danach folgen ein oder mehrere Relays und zum Schluss ein Ausgangsknoten, genannt Exit Node.

Über diese Knoten wird nun eine Verbindung zum Webserver aufgebaut. Zuerst verbindet sich der Client mit dem Entry Guard (2). Dieser sendet das Datenpaket des Clients weiter an einen Relay (3). Der Relay sendet das Datenpaket erneut weiter, an den Exit Node (4). Der Exit Node sendet als letzter Knoten der Reihe das Datenpaket an den gewünschten Webservice (5).

Um die Anonymität der Nutzer zu bewahren, verfügt jeder Knoten, der Teil der Verbindung ist, nur über die Informationen, die er selbst benötigt. Dafür wird das zu sendende Datenpaket nach dem Zwiebelprinzip in mehreren Schichten verschlüsselt. Dieser Vorgang wird nun anhand von Abbildung 2.3 erklärt.

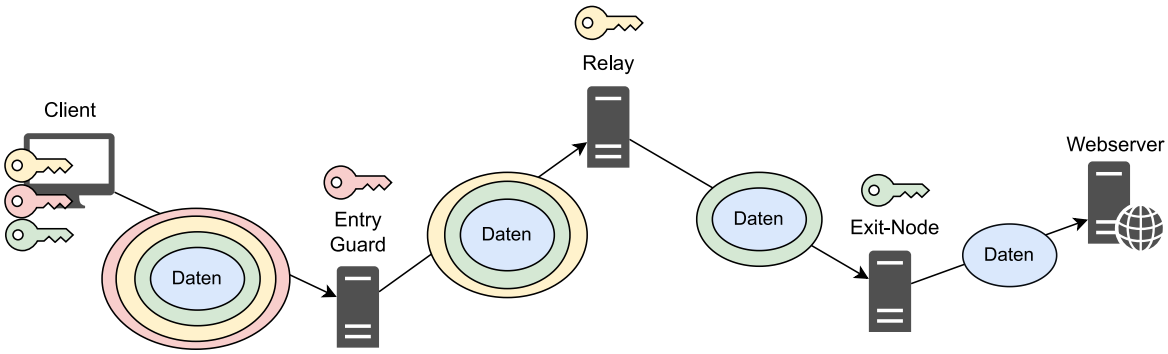

Abbildung 2.3: Verschlüsselung Datenpaket

1. Während des Verbindungsaufbaus vereinbart der Client nacheinander mit jedem Knoten in der Route einen eigenen Schlüssel. Der jeweilige Schlüssel wird mit dem Diffie-Hellman-Schlüsselaustausch vereinbart. [10–14]

2. Anschließend verschlüsselt der Client sein Datenpaket schichtweise mit dem symmetrischen Verschlüsselungsverfahren Advanced Encryption Standard (AES). [10–14]

2.1 Zuerst werden die Daten und die Informationen über die IP-Adresse des Empfängers mit dem Schlüssel des Exit-Nodes verschlüsselt. [10–14]

2.2 Danach wird die Adresse des Exit-Nodes hinzugefügt und das Paket mit dem Schlüssel des mittleren Relays verschlüsselt. [10–14]

2.3 Zum Schluss wird die Adresse des mittleren Relays hinzugefügt und das Paket mit dem Schlüssel des Entry Guards verschlüsselt. [10–14]

3. Nun wird das Datenpaket durch das Tor-Netzwerk geschickt. [10–14]

4. Zu Beginn sendet der Client das Paket an den Entry Guard. Dieser entfernt mit Hilfe des vereinbarten Schlüssels die erste Schicht der Verschlüsselung. Er erhält nun die Adresse des nächsten Relays und kann das Paket weiterschicken. [10–14]

5. Der Relay erhält das Paket vom Entry Guard und entfernt die zweite Verschlüsselungsschicht mit seinem Schlüssel. So gelangt er an die Adresse des Exit-Nodes und schickt das Paket weiter an diesen Knoten. [10–14]

6. Der Exit-Node erhält das Paket und entfernt mit seinem Schlüssel die letzte Schicht der Verschlüsselung. Somit erhält er die Adresse des Servers und die Daten, die an den Server geschickt werden sollen. [10–14]

7. Im letzten Schritt sendet der Exit-Node das nun unverschlüsselte Paket an den Server und es verlässt somit das Tor-Netzwerk. [10–14]

Die Antwort des Servers bewegt sich auf dem umgekehrten Weg durch das Tor-Netzwerk. Also vom Exit-Node zum Relay, danach zum Entry-Guard und anschließend zum Client. Auf diesem Weg legt jeder Knoten mit seinem eigenen Schlüssel wieder eine Verschlüsselungsschicht um das Paket. So kommt es vollständig verschlüsselt beim Client an. Dieser kann die Antwort des Servers dann mit Hilfe der Schlüssel entschlüsseln. [10–14]

Durch diese Funktionsweise kennt keiner der Knoten in der Verbindung sowohl den Absender als auch den Empfänger. Der Exit Guard kennt nur den Absender, der mittlere Relay kennt weder den Client noch den Internetservice und der Exit-Node kennt nur den Internetservice, an den er das Datenpaket schickt. So wird Anonymität für die Nutzer sichergestellt. Nur wenn ein Angreifer sowohl den Entry-Guard als auch den Exit-Node kontrolliert, kann der Datenverkehr eines Nutzers mitgelesen werden.

Anstelle des Entry Guards kann auch ein Bridge Node verwendet werden. Dabei handelt es sich um einen Proxy, der nicht öffentlich von den Verzeichnisservern aufgelistet ist. So kann der Tor-Browser auch von Menschen in Ländern verwendet werden, in denen die Verwendung des Tor-Browsers durch die Regierung eingeschränkt wird. Der Zugang zum Tor-Netzwerk kann eingeschränkt werden, wenn Regierungsorganisationen den Datenverkehr zu allen, von den Verzeichnissservern aufgelisteten, Knoten blockieren. Mit einem Bridge Node, dessen Adresse zum Beispiel per E-Mail erhalten wird, kann dies umgangen werden. [15]

Die meisten Nutzer, die das Tor-Netzwerk über Bridge Nodes erreichen befinden sich aktuell in Russland und dem Iran. Zusammen ergeben sie über 50% des täglichen Zugriffs per Bridge Nodes. [8]

2.2.3 Der Tor Browser

Um Zugriff auf das Tor-Netzwerk zu erhalten kann der Tor Browser genutzt werden. Dieser enthält eine modifizierte Version von Mozilla Firefox und ermöglicht die Verbindung zum Tor-Netzwerk. Der Browserverlauf wird nicht gespeichert und Cookies nur für eine Session. Der Browser verhindert Browser Fingerprinting. Dabei handelt es sich um das Sammeln von Informationen über das Gerät und den Browser eines Nutzers auf Webseiten mit speziell dafür entwickelten Skripten [16].

Außerdem hat der Tor-Browser einige Erweiterungen, um die Privatsphäre der Nutzer zu schützen. Dazu zählt unter anderem die Erweiterung "HTTPS Everywhere", die unsichere Hypertext Transfer Protocol (HTTP) Verbindungen blockiert und die Erweiterung NoScript, welche das Ausführen von JavaScript verhindert. [11]

2.3 Hidden Services

Hidden Services, auch genannt Onion Services, sind Webseiten oder Dienste, welche nur über das Tor Netzwerk erreichbar sind. Für deren Betreiber ist es möglich, online Inhalte zur Verfügung zu stellen und dabei anonym zu bleiben. Dies ist besonders in Ländern wichtig, in denen der unzensierte Internetzugang eingeschränkt ist. Denn so kann größere Sicherheit für Menschen gewährleistet werden, die zum Beispiel regierungskritische Informationen teilen.

Hidden Services existieren seit 2004 und sind durch die Uniform Resource Locator (URL) Endung .onion zu erkennen. Die URL bzw. Onion-Adresse des Hidden Service fungiert ebenfalls als Hashwert System und enthält den öffentlichen Schlüssel des Hidden Service. [11]

2.3.1 Beispiel Silk Road

Ein bekanntes Beispiel für einen Hidden Service im Tor-Netzwerk ist der ehemalige Service und Online-Marktplatz Silk Road. Im Jahr 2011 wurde er vom Amerikaner Ross Ulbricht unter dem Pseudonym “Dread Pirate Roberts” gegründet. Auf Silk Road wurden bis zur Beschlagnahmung durch das Federal Bureau of Investigation (FBI) am 1. Oktober 2013 illegale Waren und Dienstleistungen angeboten. Transaktionen fanden mit Kryptowährung statt und im Zeitraum Februar 2011 bis Juli 2013 entstand ein Umsatz von über 9,5 Millionen Bitcoins. Dies entsprach zum damaligen Zeitpunkt in etwa 1,2 Milliarden US-Dollar. [17, 18]

2.3.2 Beispiel Facebook

Während auf dem Marktplatz Silk Road hauptsächlich Drogen und andere illegale Güter verkauft wurden, gibt es unter den Hidden Services auch Webseiten und Dienste, die sich ausschließlich im legalen Rahmen bewegen. Unter anderem bieten Organisationen wie Facebook zusätzlich zu ihrem Auftritt im Surface Web einen Hidden Service Dienst im Dark Web an. So können auch Menschen auf die Plattform zugreifen, die in Ländern leben, welche die Nutzung sozialer Medien einschränken.

Die aktuelle Onion-Adresse von Facebook lautet

`facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion`. [19]

2.3.3 Funktionsweise

Bevor ein Client über das Tor-Netzwerk mit einem Hidden Service kommunizieren kann, muss dieser Hidden Service zuerst im Netzwerk registriert werden. Dieser Vorgang wird in Abbildung 2.4 dargestellt.

1. Zuerst wählt der Hidden Service drei Relays aus dem Tor-Netzwerk aus, die als sogenannte Introduction Points gelten sollen. Über diese wird später der Kontakt zum Hidden Service initiiert. Zu diesen Introduction Points werden Verbindungen über jeweils zwei weitere reguläre Tor-Knoten aufgebaut, damit der Standort des Servers des Hidden Service nicht bekannt wird. [9, 11, 13, 14, 20]

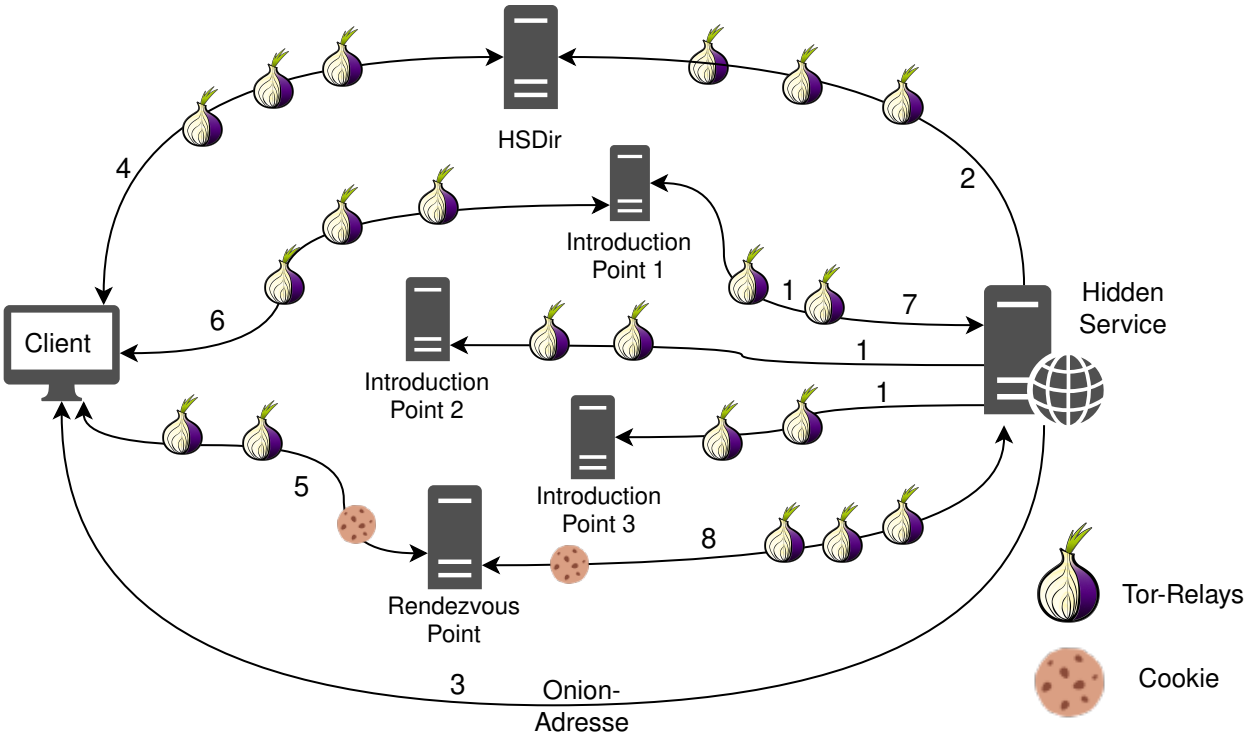

Abbildung 2.4: Funktionsweise Hidden Services

2. Als nächstes erstellt der Hidden Service einen Onion Service Descriptor. Dieser enthält die Liste der Introduction Points und den öffentlichen Schlüssel des Hidden Service. Den Onion Service Descriptor sendet der Hidden Service nun an ein Hidden Service Directory (HSDir). Dabei handelt es sich um eine verteilte Hash Wert Tabelle (engl. Distributed Hash Table), die aus Relays besteht, die mit der Flag HSDir gekennzeichnet sind. Auch die Verbindung zum Hidden Service Directory besteht aus mehreren Tor-Relays, damit der Hidden Service anonym bleiben kann. [9, 11, 13, 14, 20]

3. Zuletzt veröffentlicht der Hidden Service seine Onion-Adresse. Über diese kann ein Nutzer vom Hidden Service Directory die nötigen Informationen erhalten. Die Onion-Adresse kann zum Beispiel über eine Webseite im Clear Web oder im persönlichen Kontakt per E-Mail veröffentlicht werden. Seit der Version drei besteht die Adresse aus 56 Zeichen. Zuvor waren es 16. [9, 11, 13, 14, 20]

Ein Client kann nun auf den Hidden Service zugreifen. Dafür müssen folgende Schritte ausgeführt werden:

4. Als erstes baut der Client eine Verbindung zum Hidden Service Directory auf. Von diesem erhält er den Onion Service Descriptor, der zu der Onion-Adresse passt, die er angefragt hat. [9, 11, 13, 14, 20]

5. Danach baut der Client über mehrere Relays eine Verbindung zu einem Relay auf, den er auffordert zum Rendezvous Point zu werden. Zum Treffpunkt für den Client und den Hidden Service. Diesem Rendezvous Point teilt der Client einen zufälligen 20-Byte Wert mit. Dieser Wert wird auch als Cookie bezeichnet und gilt nur einmalig für eine Verbindung. Später wird der Cookie verwendet, um den Hidden Service zu verifizieren. [9, 11, 13, 14, 20]

6. Anschließend verbindet der Client sich mit einem der Introduction Points des Hidden Service. Die Adressen der Introduction Points hat er mit dem Onion Service Descriptor erhalten. Dem Introduction Point übermittelt der Client den Cookie und die Adresse des ausgewählten Rendezvous Point. [9, 11, 13, 14, 20]

7. Der Introduction Point gibt die Adresse und den Cookie an den Hidden Service weiter. Dieser führt nun Verifizierungsprozesse aus und entscheidet, ob der Client vertrauenswürdig ist und er sich mit ihm treffen will. [9, 11, 13, 14, 20]

8. Stimmt der Hidden Service dem Treffen zu, dann baut er eine Verbindung zum Rendezvous Point auf. Diesem übergibt er den erhaltenen Cookie. Der Rendezvous Point vergleicht den Cookie mit dem, den er zu Beginn vom Client erhalten hat. Stimmen beide überein lässt der Rendezvous Point die Verbindung zu. [9, 11, 13, 14, 20]

Der Client und der Hidden Service können nun über den Rendezvous Point miteinander kommunizieren. Zwischen ihnen befinden sich sechs Relays des Tor Netzwerkes. Zwei Relays führen vom Client zum Rendezvous Point, der den dritten Relay darstellt. Die weiteren drei Relays befinden sich auf der Route zwischen dem Rendezvous Point und dem Hidden Service. [9, 11, 13, 14, 20]

So bleiben beide Parteien vollständig anonym.

2.4 Stand der Forschung

Über das Dark Web und das Tor-Netzwerk wurde bereits seit dessen Anfängen Literatur veröffentlicht und ausführliche Untersuchungen angestellt. Die Inhalte der Forschung sind breit aufgestellt.

Roger Dingledine, Nick Mathewson und Paul Syverson veröffentlichten 2004 mit ihrem Paper “Tor: The Second-Generation Onion Router” erstmals detaillierte Informationen zum Design und der Funktionsweise des Onion Routings im Tor-Netzwerk. Bereits damals gingen sie auf Sicherheitsrisiken und Möglichkeiten für Weiterentwicklung in der Zukunft ein. [9]

2.4.1 Sicherheit

Auch heute beschäftigen sich viele Forscher damit, die Sicherheit des Tor-Netzwerks zu analysieren. Die dabei entstehenden Arbeiten lassen sich grundsätzlich in zwei Bereiche einteilen. Einerseits die, die sich damit beschäftigen, Attacken gegen das Tor-Netzwerk vorzubeugen und zu verhindern. Andererseits Arbeiten, die sich damit befassen, Attacken auf das Tor-Netzwerk durchzuführen, um die Möglichkeit aufzuzeigen oder mehr Informationen zu erhalten. Dabei handelt es sich hauptsächlich um Denial of Service Attacken. Bei diesen wird ein Internetdienst angegriffen, in dem dessen Server mit einer übermäßigen Anzahl von Anfragen überlastet wird. [11]

Auch De-Anonymization Attacken, durch die Kommunikation von Nutzern des Tor-Netzwerks überwacht werden kann, werden durchgeführt. Das Ziel dieses Angriffes ist es den Anfangs- und End-Knoten einer Tor-Verbindung zu kontrollieren, um so den Datenverkehr eines Nutzers mitlesen zu können. [11]

2.4.2 Finden von Onion-Adressen

Trujillo et al. klassifizierten 70 ausgewählte wissenschaftliche Arbeiten nach ihren Forschungsgebieten. Dabei hatten Arbeiten, die sich mit der Sicherheit von Tor beschäftigten, mit 28 Arbeiten den größten Anteil. Der zweitgrößte Bereich der Forschung war Content Klassifizierung mit 17 Arbeiten. An dritter Stelle befand sich mit 12 Arbeiten die Kategorie “Discovery and Measurement", die sich mit dem Entdecken einer möglichst hohen Anzahl von Onion-Adressen beschäftigt. [11]

Eine große Anzahl von Onion-Adressen ist eine wichtige Grundlage für weitere Forschung, wie beispielsweise die Klassifizierung der Inhalte von Hidden Services. Denn wie bereits in 2.4 beschrieben, ist für den Zugriff auf einen Hidden Service die Kenntnis seiner Onion-Adresse eine Voraussetzung. Nur so kann der Client von einem Hidden Service Directory die Adressen der Introduction Points des Hidden Service, den er besuchen möchte, erhalten und über diese den Aufbau der Verbindung beginnen.

Da Onion-Adressen jedoch nicht von herkömmlichen Suchmaschinen wie Google indexiert werden, müssen sie auf andere Weise erhalten werden.

Für das Sammeln von Onion-Adressen gibt es verschiedene Ansätze. Pastor-Galindo et al. fanden in ihrer Arbeit fünf verschiedene Methoden. Drei der Methoden sind externe Methoden, die auf dem Surface Web durchgeführt werden. Dabei handelt es sich um Onion Suchmaschinen, Verzeichnisse (engl. Repositories) und generische Suchmaschinen. [21]

Außerdem wurden zwei interne Methoden gefunden, die innerhalb des Tor-Netzwerks durchgeführt werden. Tor Crawling und Relay Injection. Im Folgenden werden die verschiedenen Methoden kurz erläutert. Sie können einzeln oder kombiniert angewendet werden. [21]

Onion Suchmaschinen: Da Onion-Adressen mit normalen Suchmaschinen schwer zu finden sind, wurden Tor-spezifische Suchmaschinen entwickelt. Beispiele hierfür sind unter anderem Onion City, Onion Live, Tor Link oder Ahmia. Hierbei ist anzumerken, dass Onion City zwar für vergangene Forschung verwendet wurde, aber mittlerweile nicht mehr aktiv ist. [21]

Um eine solche Suchmaschine zu nutzen, gibt der Forscher eine Liste an Stichwörtern (engl. Keywords) ein, die von Interesse sind. Die Suchmaschine wandelt die Eingabe in Abfragen (engl. Queries) für die interne Datenbank um. Diese Datenbank wird kontinuierlich mit Links aktualisiert, die von sogenannte Spiders, auch als Crawler bezeichnet, gefunden wurden.

Anschließend gibt die Suchmaschine die gefundenen Onion-Adressen aus. Die Ergebnisse werden basierend auf der spezifischen Suchanfrage und speziellen Ranking Algorithmen sortiert. Der Forscher erhält so direkt eine Liste mit Onion-Adressen, die zu seinen angegebenen Keywords passen. [21]

Diese Methode ist leicht anzuwenden und einfach verfügbar. Allerdings ist das Ergebnis stark durch die verwendeten Wörter, sowie durch die von der Suchmaschine verwendeten Ranking- und Suchalgorithmen beeinflusst. Zusätzlich auch durch die Effektivität der Crawler im Hintergrund der Suchmaschine. [21]

Repositories: Repositories, zu Deutsch Verzeichnisse, sind Ressourcen, die darauf spezialisiert sind, zentralisierte Listen von Onion-Adressen zur Verfügung zu stellen. Sie werden durch Communities oder einzelne Nutzer erstellt und erhalten ihre Informationen aus anderen Verzeichnissen, Datenbanken, Social Media Streams oder intelligenten Ressourcen. [21]

Forscher können direkt auf diese Listen zugreifen und sie herunterladen. Dies kann manuell geschehen, wird aber meist mit Hilfe von Scripts oder Scrapern in ein größeres System integriert. [21]

Eine bereits bestehende Link-Sammlung zu nutzen ist der direkteste Weg an Onion-Adressen zu gelangen. Außerdem vermutlich auch der Weg, auf dem die meisten Nutzer des Tor-Netzwerk an ihre Links kommen.

Allerdings ist auch hier das Ergebnis stark von der Liste und ihren Erstellern beeinflusst. Des Weiteren enthalten solche Repositories auch oft Links, die aufgrund der kurzen Lebenszeit der Hidden Services bereits nicht mehr funktionieren. Die Aktualität solcher Listen ist abhängig von aktiven Nutzern und Betreibern der Verzeichnisse.

Die am häufigsten verwendeten Repositories sind The Hidden Wiki und Ahmia. Letzteres kann sowohl als Suchmaschine, als auch als Verzeichnis verwendet werden. Weitere Quellen sind die Hidden Services Deeb Web Links und Dark Web Links, sowie das Forum Reddit oder das Tor2Web Open Data project. [21]

Generische Suchmaschinen: Traditionelle Suchmaschinen aus dem Clear Web können ebenfalls verwendet werden, um Onion-Adressen zu erhalten. Auch hierfür gibt der Forscher eine Liste an Keywords an die Suchmaschine, die diese in eine Abfrage für die interne Datenbank umwandelt.

Als Ergebnis werden passende Webseiten zurückgegeben, die Algorithmus basiert sortiert wurden. So erhält der Forscher eine Liste mit Webseiten, die zu seinen angegebenen Keywords passen und Onion-Adressen enthalten. Diese müssen individuell betrachtet werden, um aus ihnen die Onion-Adressen zu extrahieren. Dazu wird der Hypertext Markup Language (HTML)-Korpus verarbeitet. Mit String Comparison, Link Discovery oder Regular Expressions, die Strings von 56 Zeichen enthalten und auf .onion enden.

So werden Onion-Adressen im freien Text identifiziert, aus denen dann die finale Liste gebildet werden kann. [21]

Diese Methode ist intuitiv für alle Nutzer oder Analysten. Die Herausforderung besteht darin spezifische und geeignete Keywords zu wählen, mit denen Webseiten vermieden werden können, auf denen sich keine Onion-Adressen befinden. Außerdem muss aus das Ergebnis noch weiter verarbeitet werden, damit eine saubere Liste an Onion-Adressen erhalten werden kann.

Wie bereits bei den Onion-Suchmaschinen ist das Ergebnis stark abhängig von den verwendeten Keywords, den internen Algorithmen und den Crawlern der jeweiligen Suchmaschine. Neben Google werden auch die Suchmaschinen Bing, DuckDuckGo oder Yahoo von Forschern verwendet. [21]

Tor Crawling; Crawling ist eine Technik, bei der durch rekursives Folgen von Links und das Speichern der Onion-Adressen das Tor-Netzwerk automatisch erschlossen wird. [21]

Dazu designt, implementiert und startet der Forscher einen Crawler im Dark Web. Als Ausgangspunkt, auch Seed genannt, kann eine einzelne Onion-Adresse, Listen oder Verzeichnisse genutzt werden. Die Software verbindet sich dann automatisch mit dem Tor-Netzwerk, besucht rekursiv die Hidden Services durch die gefundenen Links und durchsucht die Seiten, um aus ihnen weitere Onion-Adressen zu extrahieren.

Die dabei entstehende Liste wird dem Forscher zurückgegeben. Entweder als Streams, Batches oder erst nach Ende des Crawling-Prozesses. Der Crawler kann für eine bestimmte Zeit konfiguriert werden oder auf ein numerisches Endziel an Onion-Adressen ausgelegt werden. Der Prozess endet ebenfalls, wenn keine neuen Adressen mehr gefunden werden. [21]

Diese Methode ist durch das erforderliche Erstellen eines Crawlers und die eventuell auftretenden Probleme mit Anti-Crawling Hindernissen wie Logins oder Captchas deutlich aufwendiger.

Die Ergebnisse sind abhängig von den als Seed verwendeten Adressen bzw. Listen und beinhalten nur Hidden Services, die auf anderen Seiten verlinkt sind. Im Gegensatz zu den vorherigen Methoden erhält man mit Tor Crawling eine deutlich höhere Anzahl an aktiven Hidden Services. Zumindest zum Zeitpunkt der Sammlung. Die Performance dieser Methode hängt jedoch stark von den Einstellungen, von der Dauer der Durchführung und den verfügbaren Ressourcen wie zum Beispiel der Bandbreite ab. [21]

Relay Injection: Jeder Nutzer kann freiwillig einen Knoten für das Tor-Netzwerk zur Verfügung stellen. Unter bestimmten Voraussetzungen erhalten Knoten spezielle Flags wie Guard, Exit, Fast, Stable oder HSDir. Wenn ein von Forschern eingesetzter Knoten das HSDir-Flag erhält, fungiert er als Hidden Service Directory. Dadurch kann auf die Onion Service Descriptors von Hidden Services zugegriffen werden. [21]

Diese enthalten die Introduction Points der Hidden Services, über die der Verbindungsaufbau begonnen wird. Sowie den öffentlichen Schlüssel des Hidden Service.

Durch eine Lücke in der Version zwei des Protokolls konnte aus dem öffentlichen Schlüssel der Hidden Services mit einer Umkehrfunktion die Onion-Adresse ermittelt werden.

Mit dieser Methode kann eine sehr große Menge an verschiedenen Onion-Adressen erhalten werden. Sie verstößt jedoch gegen die ethischen Richtlinien der Forschung im Tor-Netzwerk. Außerdem ist es seit dem Update auf Version drei nicht mehr möglich, aus dem öffentlichen Schlüssel die Onion-Adresse eines Hidden Service zu ermitteln. [21]

2.4.3 Analyse der Inhalte

Wenn eine Grundmenge an Onion-Adressen verfügbar ist, können die entsprechenden Hidden Services, sofern sie noch aktiv sind oder beim Crawlen die Webseite direkt heruntergeladen wurde, untersucht werden. Einige Paper befassen sich mit dem Klassifizieren der Hidden Services nach ihren angebotenen Inhalten. Um so einen statistischen Überblick über die Aktivitäten im Tor-Netzwerk geben zu können.

Meist wird mindestens in die Kategorien legal und illegal, bzw. ethisch und unethisch klassifiziert. Des Weiteren werden auch spezifischere Kategorien verwendet, z.B. Drogen, Schwarzmarkt, Child Sexual Abuse Material, Waffen, Hacking, Hit Man, Kryptowährung und Foren.

Das erste Paper zur Klassifizierung von Inhalten von Hidden Services wurde 2013 von Guitton veröffentlicht. Neun Jahre nachdem das Tor-Projekt Hidden Services zur Verfügung stellte. In diesem wurden 1171 Hidden Services in 23 Kategorien eingeteilt. Alle Hidden Services wurden außerdem in “ethical” (deutsch: ethisch) und “unethical” (deutsch: unethisch) unterschieden. Diese Einteilung wurde an Stelle von legal und illegal vorgenommen, da diese Kategorien auf den Gesetzen eines jeweiligen Landes basieren. Es liegt jedoch in der Natur der Hidden Services, dass nicht bekannt ist aus welchem Land heraus sie zur Verfügung gestellt wurden. [22]

Beispielsweise ist in vielen afrikanischen und asiatischen Ländern die Herstellung, der Besitz und der Verkauf von pornografischen Inhalten gesetzlich verboten, während es in den meisten europäischen Ländern, unter anderem in Deutschland, legal ist [23]. Ebenso unterscheidet sich die Legalität bestimmter Drogen, wie beispielsweise Cannabis je nach Land, bzw. Bundesstaat [24].

Guitton klassifizierte “pornography” (deutsch: Pornographie) genau wie “child pornography” (deutsch: Kinderpornographie) als unethisch. Child Pornography machte mit 206 Hidden Services den größten Anteil (18%) der untersuchten Services aus. Pornography befand sich knapp hinter Black Market, also dem Schwarzmarkt auf dem dritten Platz - beide entsprachen sechs Prozent. [22]

Insgesamt wurden 45% der Hidden Service als unethisch klassifiziert und 47% als ethisch. In der Kategorie ethisch finden sich unter anderem persönliche Webseiten, Filesharing-Anwendungen und Services in Verbindung mit Bitcoin. [22]

Biryukov et al. kamen ein Jahr später (2014) zu ähnlichen Ergebnissen. Sie klassifizierten bei der Untersuchung von 1813 Hidden Services 44% als illegal. Hier befanden sich an erster Stelle “adult” Inhalte, also Pornographie, und Drogen. [25]

Auch in der folgenden Forschung stellte sich heraus, dass ein großer Teil der Hidden Services in Verbindung mit Drogen steht. Owen und Savage fanden bei der Klassifizierung von 80000 Hidden Services heraus, dass die meisten Seiten der Kategorie Drogen zuzuordnen waren. Sie untersuchten die Hidden Services auch hinsichtlich des täglichen Datenverkehrs. Hier stellte ein Hidden Service der Kategorie “Abuse“ (deutsch: Missbrauch) mit 168152 Anfragen pro Tag die deutliche Mehrheit dar. Dahinter befand sich ein zu Silk Road gehörender Service mit 8067 Anfragen pro Tag. Sie fanden in ihrer Arbeit ebenfalls heraus, dass Botnetze einen weiteren relevanten Anteil des Tor-Netzwerks ausmachten. [26]

Li et al. entwickelten 2016 einen Ranking Algorithmus für die Relevanz von Hidden Services. Mit diesem bestimmten sie die zehn relevantesten Hidden Services. Darunter befanden sich mehrere Dark Web Markplätze mit Russian Anonymous Market Place an erster Stelle. Außerdem die ehemalige News Seite DeepDotWeb, welche von 2013 bis 2019 Nachrichten und Reviews rund um das Dark Web veröffentlichte. Sowie die Suchmaschine DuckDuckGo und die Plattform Facebook. Des Weiteren der ehemalige Webhosting Dienst FreedomHosting, ein E-Mail-Service und The Pirate Bay, eine Webseite, die als Hilfsmittel zum Herunterladen digitaler Inhalte dient. [27]

Al-Nabki et al. entwickelten 2019 ebenfalls einen Ranking Algorithmus, um die einflussreichsten Hidden Services zu ermitteln. Der Algorithmus beschränkt sich jedoch nur auf potenziell kriminelle Aktivitäten. Sie verwendeten einen Datensatz mit 10367 Onion-Adressen. Davon klassifizierten sie 20% als verdächtig. Die drei häufigsten Unterkategorien waren Drogen, geklaute Kreditkarten und Pornographie. 48% der Hidden Services wurden als normal klassifiziert. Bei den nicht verdächtigen Services handelt es sich bei 47% um Hosting Server und 17% standen in Verbindung zum Handeln mit Kryptowährungen. [28]

Bei Anwendung ihres Ranking Algorithmus ToRank wurden unter den Top zehn einflussreichsten Hidden Services vor allem Drogen und Pornographie festgestellt. Dabei befanden sich die Hidden Services im Bereich Drogen auf den Plätzen eins, vier, fünf, sechs und zehn. Services mit pornografischen Inhalten befanden sich auf Platz zwei, sowie auf den Plätzen acht und neun. Auf Platz drei befand sich der Marketplace HANSA market, auf dem bis zum Juni 2017 illegale Produkte gehandelt wurden. An siebter Stelle befand sich ein Hidden Service, der seinen Kunden gefälschte Reisepässe verkaufte. [28]

Weitere Arbeiten im Bereich Klassifizierung kamen zu teilweise sehr unterschiedlichen Ergebnissen. Faizan und Khan kamen 2019 auf einen illegalen Anteil von nur 38% [29]. Im Gegensatz dazu fanden Spitters et al. 2014 in den meisten der 1481 Hidden Services, die sie untersuchten illegale oder zumindest kontroverse Inhalte [30].

Eindeutige Aussagen zum Anteil von illegalen Diensten unter den Hidden Services sind aufgrund der großen Bandbreite der Ergebnisse nicht möglich. Ebenso wenig lässt sich feststellen, ob die Menge der unethischen bzw. illegalen Inhalte in den letzten Jahren gesunken oder gestiegen ist.

Gründe dafür sind die unterschiedlichen Arten der Sammlung von Onion-Adressen und damit auch die variierenden Datensatzgrößen. Außerdem die Unterschiede der verwendeten Klassifizierungsansätze und Definitionen von illegalen bzw. unethischen Inhalten.

Festzustellen ist aber, dass allen Arbeite, die Hidden Services nach ihrer Relevanz oder den Aufrufen pro Tag ordnen, zu dem Ergebnis kommen, dass illegale bzw. unethische Services, wie Drogen oder Pornographie besonders häufig genutzt werden.

Übereinstimmungen sind außerdem bei der Sprachverteilung der Hidden Services zu finden. Der Großteil der Services im Tor-Netzwerk wird auf Englisch angeboten. Danach kommen europäische Sprachen, vor allem Russisch, Deutsch, Französisch und Spanisch. [25, 28, 31]

3 Methoden

Ziel der Arbeit ist es, Hidden Services im Dark Web zu untersuchen und eine aktuelle Übersicht zu erstellen. Der erste Schritt bestand deshalb im Erhalten von Onion-Links zu möglichst vielen, aber auch aussagekräftigen Hidden Services.

Da sich bereits viele Forscher und Forschungsgruppen in der Vergangenheit mit diesem Thema beschäftigten und dabei umfassende Ergebnisse erhielten, wurden zunächst die Autoren mehrerer solcher Arbeiten kontaktiert.

Die Forschungsgruppe, Al-Nabki et al. stellte freundlicherweise die bei der Forschung erhaltene Link Sammlung zur Verfügung. Dabei handelt es sich um einen Ordner mit rund 10.000 Unterordnern, benannt nach den Onion-Adressen. In diesen Unterordnen befindet sich jeweils ein heruntergeladenes HTML Dokument des betreffenden Hidden Services. Darüber ist es möglich, Webseiten, die zum Zeitpunkt des Herunterladens online waren, auch jetzt noch in diesem Zustand zu betrachten. Die im Datensatz enthaltenen Hidden Services wurden 2018 heruntergeladen.

Bei den Onion-Links handelt es sich um Links der Version zwei, die inzwischen vom Tor Netzwerk und dem Tor Browser nicht mehr unterstützt werden. Deshalb kann der Zugriff auf die entsprechenden Hidden Services nur noch über die heruntergeladenen Versionen erfolgen.

Neben den Onion-Links enthält der Datensatz ebenfalls ein Excel Dokument, in dem alle Hidden Services aufgelistet und ihnen verschiedenen Kategorien zugeordnet sind.

Mit Hilfe dieses Datensatzes und der enthaltenen Hidden Services konnte ein erster Überblick über die im Dark Web verfügbaren Inhalte gewonnen werden. Außerdem konnte anhand der Daten bei Bedarf Aussagen über die Entwicklung bestimmter Hidden Services im Laufe der Zeit getroffen werden.

Onion-Links zu aktuellen Hidden Services wurden auf andere Art erhalten. Hier wurde ein Ansatz gewählt, der ähnlich der Art ist, auf die auch normale Tor-Netzwerk Nutzer Zugriff zum Dark Web erhalten und es navigieren.

Dazu wurden sogenannte Verzeichnisse aufgesucht, die im nächsten Kapitel noch näher beschrieben werden. In diesen Verzeichnissen befinden sich Sammlungen von Onion-Links zu bestimmten Hidden Services.

Die Link Sammlungen sind meist in verschiedene Kategorien unterteilt. Diese Kategorien geben bereits einen ersten Aufschluss darüber, wofür das Dark Web aktuell am meisten genutzt wird.

Solche Link Sammlungen gibt es nicht nur im Dark Web selbst, sondern auch im Clear Web. Hier gibt es zum einen identische Versionen mancher Verzeichnisse, aber unter anderem auch Zeitungsartikel oder Blogeinträge, die eine bestimmte Anzahl an Onion-Links empfehlen.

Auch in Clear Web Foren wie Reddit, genauer im Subreddit r/Onions, werden Onion-Links zu Hidden Services geteilt. Hier gibt es sowohl allgemeine Link Sammlungen, als auch die Möglichkeit als Nutzer nach speziellen Links zu fragen. [32]

Wie aus Literatur ersichtlich wird, gibt es auch weitere Methoden an möglichst viele Onion-Links zu gelangen. Dennoch wurde für diese Arbeit nur die oben beschriebenen Methoden angewandt. Erstens sind manche dieser Methoden aufgrund der Updates und Verbesserung der Sicherheit des Tor-Netzwerkes inzwischen nicht mehr möglich. Außerdem verbrauchen andere Methoden oft Ressourcen, die für diese Arbeit nicht zur Verfügung stehen. Es wurde deshalb davon Abstand genommen, zum Beispiel einen Crawler zu bauen und zu nutzen.

Des Weiteren beschäftigt sich diese Arbeit eher mit einer qualitativen Analyse von Hidden Services anstatt einer quantitativen. Es ist nicht das Ziel, so viele Onion-Links wie möglich zu erhalten. Denn für eine ausführliche Analyse ist es notwendig, die einzelnen Hidden Services manuell aufzusuchen, zu durchsuchen und genau zu betrachten, um sie so vergleichen und analysieren zu können.

Diese Vorgehensweise sorgt dafür, dass die Anzahl der zu besuchenden Hidden Services begrenzt ist. Um einen Überblick über die im Dark Web angebotenen Services zu erhalten, reicht es aus, eine bestimmte Anzahl von stellvertretenden Webseiten für eine Kategorie zu besuchen. Denn oft stellte sich beim Untersuchen von kleineren Stichproben bereits heraus, dass bestimmte Ähnlichkeiten, Unterschiede und allgemeine Tendenzen schnell zu erkennen waren.

Für einen Überblick über das Dark Web ist es außerdem wichtig zu beachten, wie dieses von den Tor-Nutzern genutzt wird. Während über einen Crawler oder andere Ansätze Hidden Services gefunden werden, die über den bloßen Gebrauch von Verzeichnissen und Suchmaschinen nicht auffindbar sind, so wird doch der durchschnittliche Tor-Nutzer keinen Crawler verwenden. Stattdessen navigieren Nutzer in der Mehrzahl über genannte Verzeichnisse, Suchmaschinen und persönliche Empfehlungen von Dritten.

Es kann im Rahmen dieser Arbeit davon ausgegangen werden, dass Hidden Services, die besonders oft in Verzeichnissen verlinkt oder von Internetnutzern im Clear Web erwähnt werden, auch proportional oft von Dark Web Nutzern aufgesucht werden.

Im Kontrast dazu kann ebenfalls davon ausgegangen werden, dass Hidden Services, die nur an äußerst wenigen Stellen verlinkt werden, eher selten aufgesucht und genutzt werden.

Zusätzlich wurde für die Recherche nach Onion-Links hauptsächlich die wohl populärste Dark Web Suchmaschine Ahmia.fi genutzt. Diese Suchmaschine wird im Abschnitt 4.1.2 näher beschrieben. Ein wichtiger Grund für die Benutzung war unter anderem der eingebaute Filter zum Vermeiden von kinderpornografischen Inhalten.

4 Ergebnisse und Auswertung

In diesem Kapitel werden die gefundenen Hidden Services beschrieben und untersucht. Für erhöhte Übersichtlichkeit sind sie sortiert in die Unterkapitel Einstiegsstellen, Legale Inhalte, Rechtliche Grauzone und Illegale Inhalte.

4.1 Einstiegsstellen

Die Nutzung des Dark Webs unterscheidet sich für die Nutzer in einigen Punkten von der Nutzung des Clear Webs. Wie bereits in 2.4 erwähnt, kann das Dark Web nicht mit herkömmlichen Suchmaschinen durchsucht werden, um die gewünschten Webseiten aufzufinden.

Deswegen haben sich unter anderem auf das Dark Web spezialisierte Suchmaschinen entwickelt. Diese werden in diesem Abschnitt näher betrachtet. Ebenso wie die bereits erwähnten Verzeichnisse, auch genannt Repositories. Zusammen stellen diese Arten der Hidden Services für die Nutzer Einstiegspunkte in das Dark Web dar.

Hier erhalten Nutzer erste Onion-Adressen über deren Hidden Services sie später an weitere Onion-Adressen kommen können.

4.1.1 Verzeichnisse

Als Startpunkt können Verzeichnisse, oft auch Hidden Wiki genannt, genutzt werden. Die Bezeichnung, die im Deutschen „Verstecktes Wiki“ bedeutet, geht zurück auf die Linksammlung The Hidden Wiki. Dieser Hidden Service wurde 2004 gegründet und enthielt eine Sammlung von Onion-Links zu verschiedenen Webseiten [33]. 2014 wurde der Hidden Service, vermutlich im Zuge der Operation Onymous, von Behörden übernommen.

Operation Onymous war eine internationale Maßnahme, bei der mehrere polizeiliche Behörden zusammenarbeiteten. Die Identitäten vieler Personen, die im Dark Web illegale Aktivitäten durchführten, konnten aufgedeckt und diese Personen verhaftet werden. Mehrere illegale Hidden Services wurden gesperrt, darunter vor allem Dark Web Märkte, auf denen illegale Güter angeboten und verkauft wurden. [34]

Das originale The Hidden Wiki enthielt Links zu solchen Marktplätzen, aber verlinkte ebenfalls Hidden Services, auf denen kinderpornographische Inhalte geteilt wurden [35]. Dies scheinen die Gründe für die Übernahme durch die Behörden zu sein. Jedoch ist zu beachten, dass die Domäne des The Hidden Wiki bereits Monate zuvor gehackt worden war und der Hidden Service in Folge dessen auf mehrere identische Webseiten mit unterschiedlichen Onion-Adressen gespiegelt wurde [36].

Seit dem Zeitpunkt der Operation Onymous im Jahr 2014 haben sich mehrere Nachfolger des Originals gebildet. Heute gibt es sehr viele verfügbare Hidden Services, die Onion-Links in gesammelter Form zur Verfügung stellen. Viele dieser Hidden Services sind immer noch nach dem The Hidden Wiki benannt. Der Name sich zu einer Art Deonym entwickelte, ein von einem Eigennamen abgeleitetes Wort.

Bei der Recherche wurden unter anderem vier verschiedene Hidden Services mit dem Titel “The Hidden Wiki” gefunden [37–40] . Zwei weitere tragen jeweils die Titel “The Uncensored Hidden Wiki” und “Another Hidden Wiki” [41, 42].

Andere Verzeichnisse benutzen Namen wie “Onion Links” oder “Tor Links” [43, 44]. Aber auch Namen, die auf den ersten Blick weniger auf die Art des Hidden Services hinweisen. Zum Beispiel “tor.taxi” und “The Dark Web Pug” [45, 46].

Als Einstiegsstelle ins Dark Web sind einige dieser Hidden Services auch im Clear Web als Webseiten zu finden [47, 48].

Des Weiteren werden sie oft von erfahrenen Nutzern als Einstiegspunkt weiterempfohlen oder auf Foren wie Reddit verlinkt. Darüber hinaus bietet das Reddit Unterforum r/onions auch eine eigene Linksammlung an. [32]

Auch einige Webseiten oder Blogs im Clear Web bieten eine eigene Sammlung an Onion-Adressen an. Für diese Arbeit wurden jedoch nur diese betrachtet, welche ebenfalls einen Hidden Service im Tor-Netzwerk anbieten.

Der grundsätzliche Aufbau der Verzeichnisse ist oft ähnlich. Die meisten bestehen aus einer einzelnen Seite, auf der die Onion-Links in verschiedenen Kategorien aufgelistet sind. "The Uncensored Hidden Wiki"besteht hingegen aus verschiedenen Unterseiten an Stelle von einer bloßen Auflistung der Kategorien. Die Onion-Links in diesem Verzeichnis sind jedoch alle noch im Format der Version zwei, das vom Tor Browser nicht mehr unterstützt wird. [41]

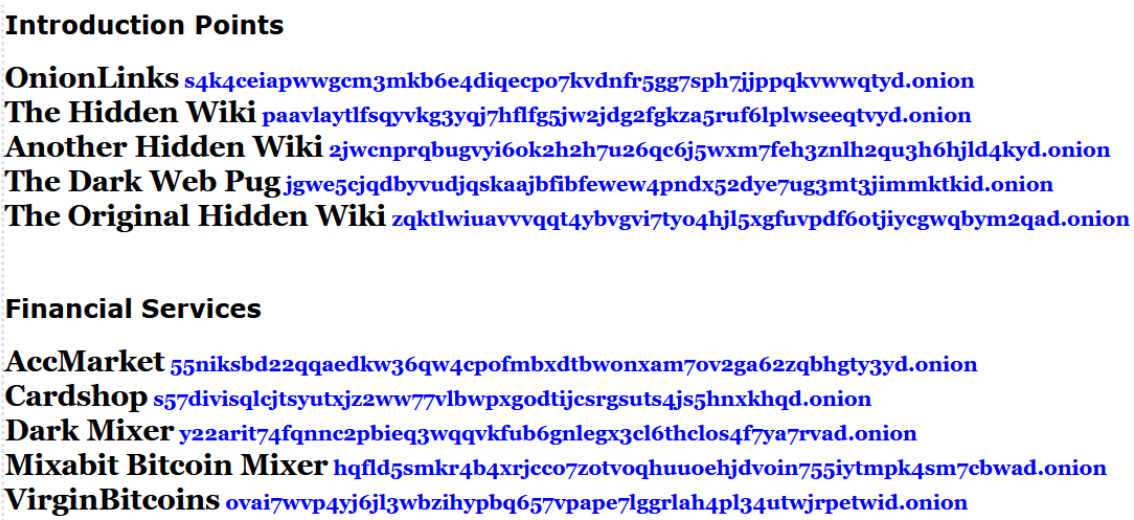

Abbildung 4.1: Hidden Service Verzeichnis OnionLinks [43]

Neben dem ähnlichen Aufbau teilen die Verzeichnisse auch das oft schlichte Design. Anders als viele Webseiten im Clear Web sind diese Seiten sehr einfach gestaltet. Es werden wenige Farben und Formatierungsarten verwendet. Einige der Seiten sind besonders durch ihre Farbwahl oder fehlenden Platz bei der Auflistung der Links visuell weniger ansprechend als vergleichbare Webseiten im Clear Web. Erkennbar ist dies am Beispiel des Hidden Service OnionLinks in Abbildung 4.1. Die Priorität liegt hier eindeutig auf Funktion anstatt Darstellung.

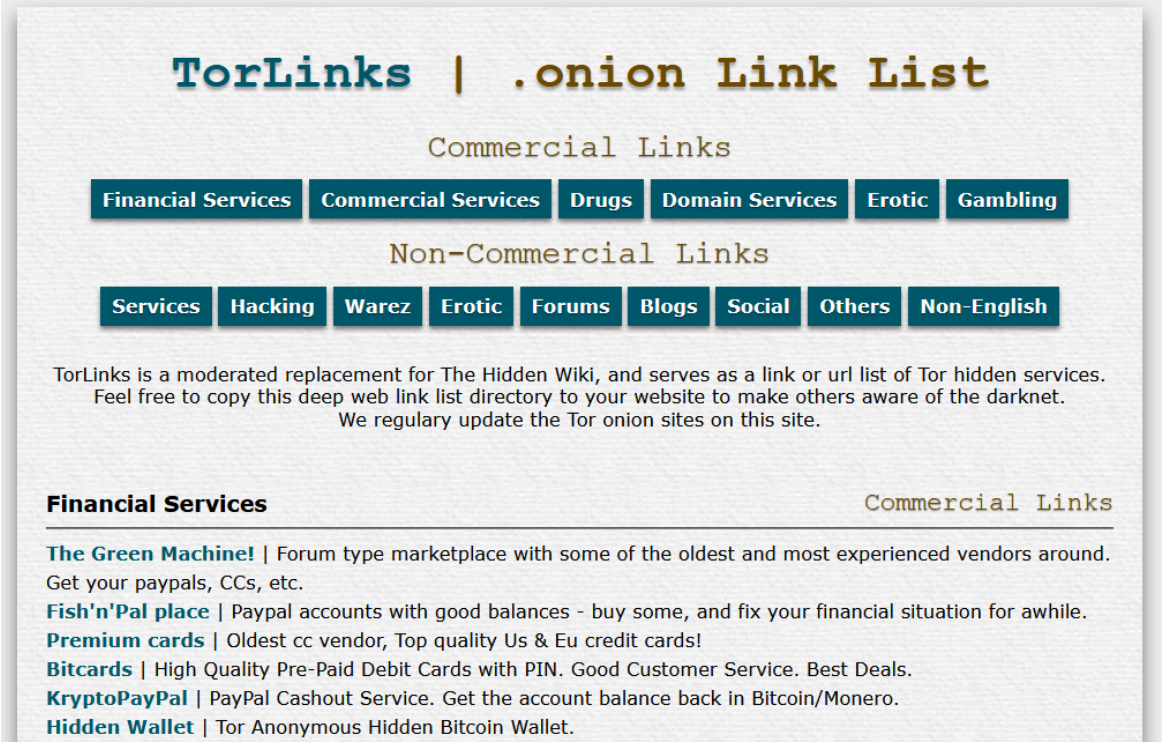

Abbildung 4.2: Hidden Service Verzeichnis TorLinks [44]

Der Hidden Service TorLinks fällt in Bezug auf das Design positiv auf. Er ist vergleichbar mit manchen mittelgroßen Webseiten des Clear Webs. Wie in Abbildung 4.2 zu sehen ist sind die verwendeten Farben und Schriftarten gut lesbar und übersichtlich.

Die Kategorien, in welche die Verzeichnisse ihre Linksammlung unterteilen, unterscheiden sich in ihrer Spezifität. Manche Hidden Services unterscheiden ihre Onion-Adressen lediglich in kommerziell und nichtkommerziell. Die Mehrheit listet jedoch kleinere Kategorien auf. Die häufigsten sind Suchmaschinen, Nachrichten, Marktplätze, Drogen, Finanzielle Services und E-Mail-Anbieter. Weitere verwendete Kategorien sind Hacking, Foren, Sicherheit und Privatsphäre, Chans, Erotik, Glücksspiel, Hosting, File Sharing und Whistleblowing.

Die genannten Kategorien, sowie deren Bezeichnungen und Inhalte werden in später folgenden Abschnitten näher erklärt.

Fast alle der verlinkten Hidden Services sind in englischer Sprache. Während der Recherche wurde kein deutsches Verzeichnis gefunden. Nur wenige Verzeichnisse, beispielsweise TorLinks, bieten Onion-Links zu nicht-englischen Hidden Services an. Der Hidden Service

TorLinks listet Seiten mit den Sprachen Finnisch, Französisch, Deutsch, Italienisch, Japanisch, Chinesisch, Polnisch, Russisch, Spanisch, Portugiesisch und Schwedisch auf. Dies spiegelt die allgemeine Sprachverbreitung im Dark Web wieder. [44]

Wie bereits an den Kategorien zu erkennen ist, verlinken alle beobachteten Hidden Services nicht nur legale Inhalte, sondern auch solche, deren Legalität fragwürdig bis hin zu illegal ist. Mit Ausnahme von einem Fall verlinken alle Verzeichnisse Hidden Services der Kategorie Drogen. Auch Ressourcen oder Anbieter zum Thema Hacking werden oft verlinkt. Genauso wie Hidden Services, deren Angebote als Finanzielle Services bezeichnet werden. Dabei handelt es sich oft um Seiten, auf denen kopierte bzw. gestohlene Bankkarten oder gehackte Paypal- oder Ebay-Accounts verkauft werden.

Nur wenige Hidden Services verlinken hingegen pornographische Inhalte. Lediglich die Verzeichnisse TorLinks und tor.taxi enthalten einen Onion-Link zur Pornowebseite PornHub [44, 45]. Dabei handelt es sich nicht um eine explizit auf kinderpornographische Inhalte spezialisierte Seite. Jedoch steht PornHub heftig in der Kritik, da Nutzer weiterhin Inhalte hochladen in denen minderjährige und/oder sexuelle Gewalt zu sehen ist [49]. Der PornHub Hidden Service ist zurzeit offline.

Der Anteil an Onion-Links zu Hidden Services mit illegalen Inhalten ist je nach Verzeichnis unterschiedlich, liegt jedoch oft bei ungefähr fünfzig Prozent.

Ebenso unterschiedlich ist der Anteil der Onion-Links, die tatsächlich zu aktuell verfügbaren Hidden Services führen, die zum Zeitpunkt des Aufrufes online sind. Dies liegt an der Volatilität des Dark Webs. Viele Hidden Services sind nur für kürzere Zeiträume, meist nur Monate oder gar Wochen verfügbar. Manche Webseiten wechseln nach Serverproblemen auf einen komplett neu erstellten Hidden Service mit einer anderen Onion-Adresse.

Einige Webseiten, wie beispielsweise tor.taxi und Dark Fail bieten an, Informationen zum aktuellen Status von Hidden Services zur Verfügung zu stellen [45]. Sie geben an, ob Hidden Services seit längerer Zeit offline sind oder aktuell aufgrund von beispielsweise Distributed Denial of Service-Attacken oder Wartungsarbeiten nicht erreichbar sind. Distributed Denial of Service Attacken sind Angriffe bei denen ein Server von mehreren Geräten, oft auch von Botnetzen, mit Anfragen überflutet wird bis dieser nicht mehr funktioniert.

Einige Hidden Services bereiten sich auf den Fall von Angriffen von Dritten vor. Dazu spiegeln sie ihre Inhalte auf mehrere Onion-Adressen. Einige Verzeichnisse listen deshalb mehrere Onion-Links für einen Hidden Services auf.

Nahezu jedes Verzeichnis enthält mehrere Onion-Links die zurzeit nicht funktionieren. Manche weisen explizit darauf hin, dass ein Hidden Service, der im Moment offline ist, nicht sofort aus der Auflistung entfernt wird, da solche Abwesenheiten oftmals nur temporär sind.

Zu den aufgelisteten Onion-Links bieten die Verzeichnisse meist nur wenige Informationen an. Manche Seiten wie zum Beispiel OnionLinks geben zu den von ihnen aufgelisteten Links nur den Titel der Webseite an [43]. Andere enthalten eine kurze Beschreibung wie beispielsweise

“Anonymous bitcoin mixer” (anonymer Bitcoin Mixer), “Coffee Shop grade Cannabis from the netherlands” (Coffee Shop Level Cannabis aus den Niederlanden) oder “Fake passports and ID cards for bitcoin” (gefälschte Pässe und Ausweise für Bitcoins).

Es ist klar ersichtlich, dass es zwischen den Verzeichnissen starke Überlappungen bei den verlinkten Hidden Services gibt. Bestimmte Hidden Services werden auf nahezu allen Verzeichnis-Webseiten verlinkt. Dies deutet zum einen auf die Popularität dieser Hidden Services, aber auch darauf, dass die Verzeichnisse ihre Onion-Links eventuell aus gleichen Quellen oder direkt von anderen Verzeichnissen beziehen.

Der Aufbau und die Funktionsweise eines Verzeichnisses werden nun am Beispiel The Hidden Wiki mit der Onion-Adresse http://paavlaytlfsqyvkg3yqj7hflfg5jw2jdg2fgkza5ruf6lplwseeqtvyd.onion/ näher betrachtet.

Das Design erinnert an das der Clear Web Enzyklopädie Wikipedia. Der Hintergrund ist weiß, der Text schwarz und die Onion-Links sind Blau dargestellt. Es wird lediglich der Name des Hidden Services angezeigt und nicht der Link selbst. Dadurch erscheint die Seite im Vergleich zu einigen anderen Verzeichnissen übersichtlicher.

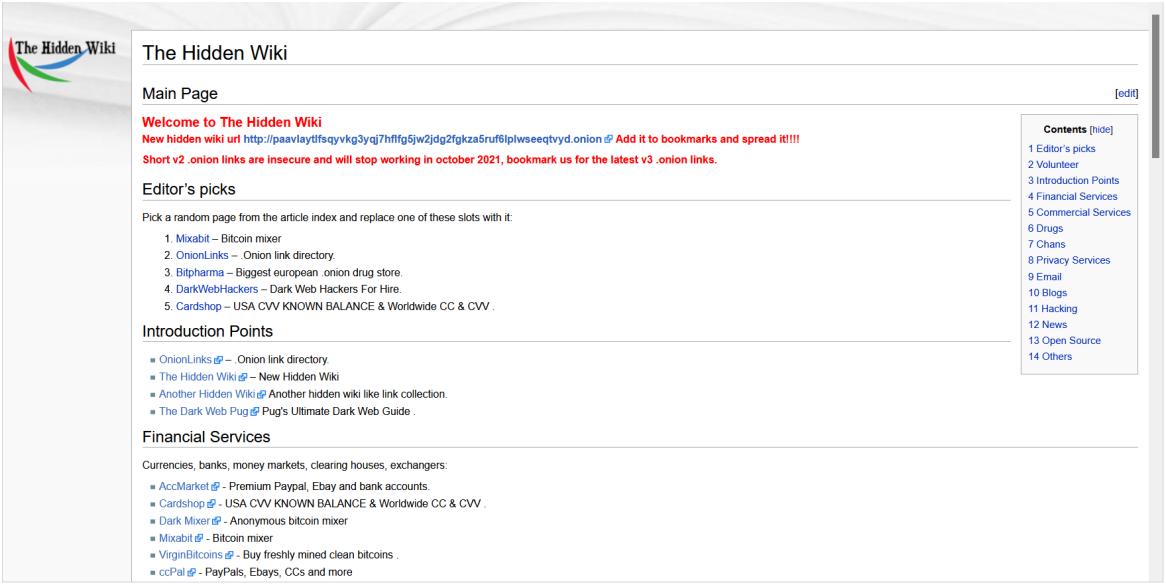

Abbildung 4.3: The Hidden Wiki

Die einzelnen Kategorien sind außerdem durch klar erkennbare Überschriften und Trennstriche abgegrenzt. Zur Navigation befindet sich am oberen rechten Rand ein Inhaltsverzeichnis, das die jeweiligen Kategorien verlinkt.

Die Linksammlung ist unterteilt in folgende Kategorien :

Editor’s picks: zu Deutsch Auswahl des Redakteurs. Hier werden ein Bitcoin Mixer, ein weiteres Verzeichnis, ein Drogen Onlineshop, ein Hacking Service und ein Shop, der Bankkarten verkauft, verlinkt.

Introduction Points: zu Deutsch Einstiegspunkte, listet weitere Onion-Link Verzeichnisse auf.

Financial Services: zu Deutsch finanzielle Services, enthält Links zu Hidden Services, auf denen Falschgeld, geklaute Bankkarten oder Paypal-Accounts und Dienste im Zusammenhang mit Kryptowährungen angeboten werden.

Commercial Services: zu Deutsch kommerzielle Services, sind Webseiten, auf denen Dienstleistungen im Bereich Hacking angeboten werden oder technische Geräte, Waffen, gefälschte Pässe und Medikamente zur Behandlung erektiler Dysfunktion verkauft werden.

Drugs: zu Deutsch Drogen, listet Hidden Services auf, die Drogen, insbesondere Cannabis verkaufen.

Chans: auch genannt Imageboards. Dabei handelt es sich um Foren, in denen anonym Bilder und Texte ausgetauscht werden können. Drei der fünf Onion-Links funktionieren nicht.

Privacy Services: Services zum Schutz der Privatsphäre sind Hidden Services, die zum Beispiel VPNs anbieten. Zwei der fünf Links funktionieren nicht.

Email: in dieser Kategorie werden E-Mail-Provider aufgelistet. Zwei der vier Services sind nicht erreichbar.

Blogs and Personal Sites: zu Deutsch Blogs und persönliche Seiten, listet Blogs und persönliche Seiten von Einzelpersonen auf. Mit sechs von neun Links ist die Mehrheit dieser Hidden Services nicht erreichbar.

Hacking: listet nur die Defcon Seite auf. Defcon ist eine der weltweit größten Veranstaltungen für Hacker [50].

News Sites: zu Deutsch Nachrichtenseiten, listet zwei Seiten auf, die Nachrichten zum Dark Web und zum allgemeinen Weltgeschehen publizieren.

Open Source Software: sind Onion-Links zu Hidden Services von beispielsweise Betriebssystemen oder Filesharing-Diensten. Einer der vier Onion-Links funktioniert nicht.

Other Sites: zu Deutsch andere Seiten, beinhalten die offizielle Seite der Central Intelligence Agency (CIA) und weitere Hidden Services, unter anderem einen, der die Bibel anbietet. Einer der sechs Onion-Links funktioniert nicht.

Die Mehrzahl der Onion-Links in diesem Verzeichnis führen zu Hidden Services mit illegalen Inhalten, wie Drogen, Waffen und gefälschte Dokumente. Im Gegensatz zu anderen Verzeichnissen funktionieren jedoch auch die Mehrheit der Onion-Links und verlinken Hidden Services, die derzeit online sind.

The Hidden Wiki ist ein Beispiel von vielen ähnlich aufgebauten Hidden Services. Anhand der aufgelisteten Onion-Adressen lässt sich bereits vermuten, dass Nutzer das Tor-Netzwerk sowohl für legale als auch für illegale Zwecke nutzen.

4.1.2 Suchmaschinen

Die Standardsuchmaschine des Tor Browsers ist DuckDuckGo. Mit ihr lassen sich jedoch aufgrund der Funktionsweise des Tor-Netzwerks und der Hidden Services keine Onion-Links finden.

Dennoch gibt es Suchmaschinen, mit denen sich das Dark Web durchsuchen lässt. Diese Hidden Services benutzen wie auch Suchmaschinen im Clear Web einen Crawler, um die Webseiten aus dem Tor-Netzwerk zu indexieren. Auf den so entstehenden Datenbanken werden dann die Suchanfragen durchgeführt und die Ergebnisse danach an den Nutzer ausgegeben. Ebenso ist es bei manchen Suchmaschinen, wie beispielsweise Ahmia möglich, als Betreiber eines Hidden Services diesen zur Datenbank hinzuzufügen [51].

Fast alle dieser Suchmaschinen sind nicht nur im Dark Web sondern auch im Clear Web verfügbar. Die Onion-Links die als Ergebnis erhalten werden, können jedoch nur mit dem Tor Browser geöffnet werden. Die Ergebnisse der Clear Web Versionen sind identisch mit denen der Dark Web Versionen. Wenn die Suchmaschinen nicht ebenfalls im Clear Web verfügbar sind, so haben sie dennoch oft eine Webseite dort, die über den Onion-Link auf die Dark Web Version verweist.

Im Gegensatz zu vielen Clear Web Suchmaschinen bieten die meisten Suchmaschinen im Dark Web jedoch oft keine Suchkategorien wie Bilder, Videos, Einkaufen, Nachrichten oder Karten an. Außerdem unterscheiden sie sich in der Anzahl der Ergebnisse bei einer Anfrage.

Verwendet man beispielsweise den Begriff “drugs”, zu Deutsch Drogen, als Suchanfrage, so reicht die Anzahl der Ergebnisse von 51 (VormWeb) bis hin zu 30638 (Tordex). Nutzer müssen hier zwischen dem Wunsch viele Ergebnisse zu erhalten und dem Bedürfnis möglichst passende Hidden Services zu ihren Suchanfragen zu bekommen, abwägen.

Die Suchmaschinen unterscheiden sich nicht nur in der Anzahl der Ergebnisse, sondern auch in der Art der Ergebnisse. So filtert die Suchmaschine Ahmia beispielsweise alle Hidden Services mit kinderpornographischen Inhalten aus den Suchergebnissen heraus.

Bei Ahmia handelt es sich um die wohl meist verlinkte und auch bekannteste Suchmaschine des Dark Web. Ihr Quellcode steht frei auf Github zur Verfügung und die Link Struktur der Suchmaschine kann eingesehen werden.

Der Hidden Service bietet zusätzlich zur Suchfunktion auch Listen an, auf denen beispielsweise alle gesperrten Hidden Services aufgezählt sind. Ebenso gibt es eine Liste aller, der Suchmaschine bekannten, nicht gesperrten Hidden Services.

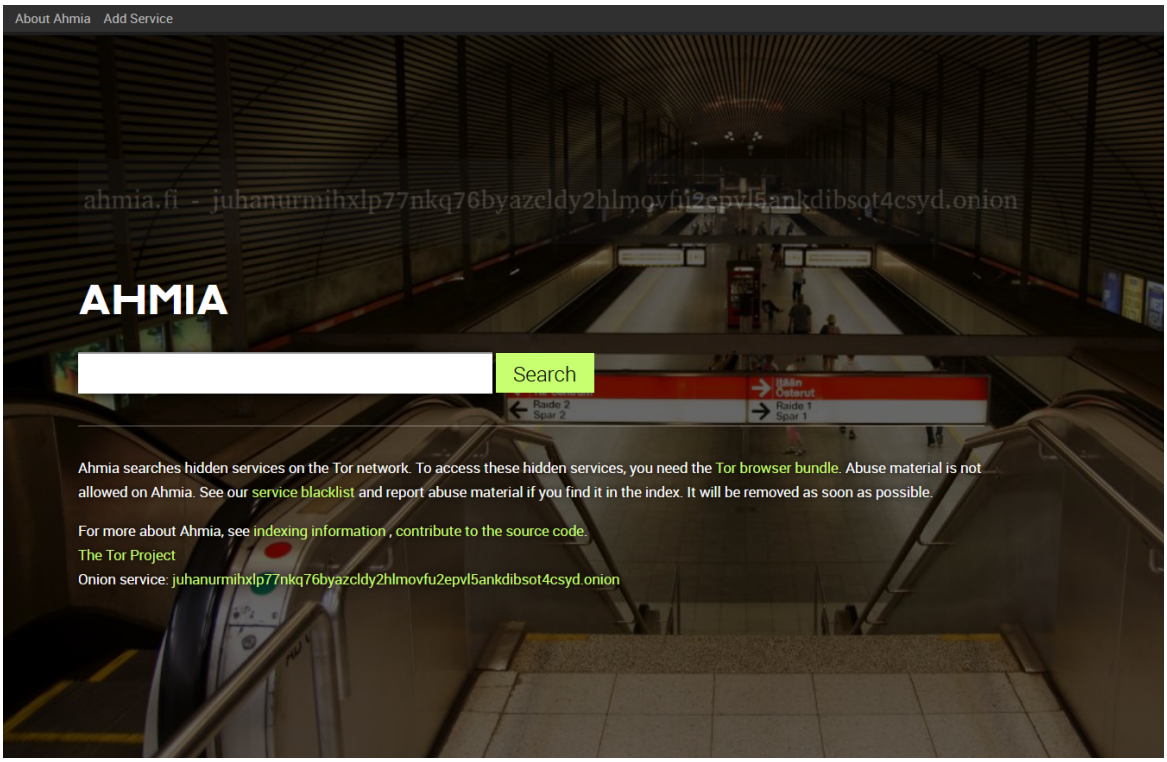

Abbildung 4.4: Suchmaschine ahmia.fi [51]

Für die Betreiber von Hidden Services gibt Ahmia die Möglichkeit, deren Hidden Services über ein Eingabefeld zur Datenbank und damit der Indexierung manuell hinzuzufügen. Außerdem stellen die Suchmaschine eine Sperrliste von Hidden Services mit sogenannten Child Sexual Abuse Material (CSAM), also kinderpornographischen Inhalten, zur Verfügung. Die Onion-Adressen der betroffenen Hidden Services werden in Form eines MD5 Summen Hashwertes gespeichert. So ermöglicht Ahmia es den Betreibern von anderen Suchmaschinen durch einen Hash-Abgleich bekannte Seiten mit diesen Inhalten aus den Suchergebnissen auszuschließen. Es filtern jedoch nicht alle Suchmaschinen kinderpornographisches Material aus ihren Ergebnissen heraus.

Weitere Suchmaschinen sind zum Beispiel Haystak, VormWeb, Onion Land, Tordex, Tor66 und Excavator [52–57].

Bei VormWeb handelt es sich dabei um eine deutsche Suchmaschine, die jedoch auch fremdsprachige Ergebnisse liefert. [53]

Nur wenige der genannten Suchmaschinen bieten auch eine Bildersuchfunktion an. So zum Beispiel der Hidden Service Tordex. Die Suchmaschine verwendet Scraper, um das Dark Web nach Dateien im png, jpg und webp Format zu durchsuchen. Basierend auf ihren Titel und alternativen Beschreibungen werden sie indexiert. Eine Suche nach dem Begriff “drugs” (Drogen) liefert zum Beispiel 2101 Ergebnisse. [55]

Zusätzlich zur Suchfunktion enthält der Tordex Hidden Service auch ein Verzeichnis mit Onion-Links, unterteilt in zehn Kategorien von Marktplätzen bis Hosting. Zu jedem Hidden Service sind dessen Titel, der Onion-Link und eine kurze Beschreibung angegeben. Sowie ein kleines Bild, bei dem es sich um das Logo des jeweiligen Hidden Service handelt.

Die Suchmaschine Tordex bezeichnet sich selbst als unzensierter Index von Hidden Services und liefert im Gegensatz zu Ahmia auch Hidden Services als Suchergebnis, die kinderpornographische Inhalte enthalten.

Auf der Webseite des Hidden Services befinden sich unterhalb des Eingabefeldes für die Suchbegriffe mehrere Werbeanzeigen. Dabei handelt es sich um sowohl legale Hidden Services wie beispielsweise Suchmaschinen oder Foren, aber auch um Hidden Services mit pornographischen oder illegalen Inhalten.

Auch die Suchmaschine Onion Land enthält eine Bildersuchfunktion. Der Begriff “drugs” liefert hier 6274 Ergebnisse. Außerdem gibt es mit der Schaltfläche “I’m feeling Lucky”, zu Deutsch ich fühle mich glücklich, bzw. ich denke ich habe Glück, die Möglichkeit nach einem zufälligen Begriff zu suchen. Es gibt zusätzlich die Funktion “Random Onion”, die auf einen zufälligen Hidden Service verlinkt. [54]

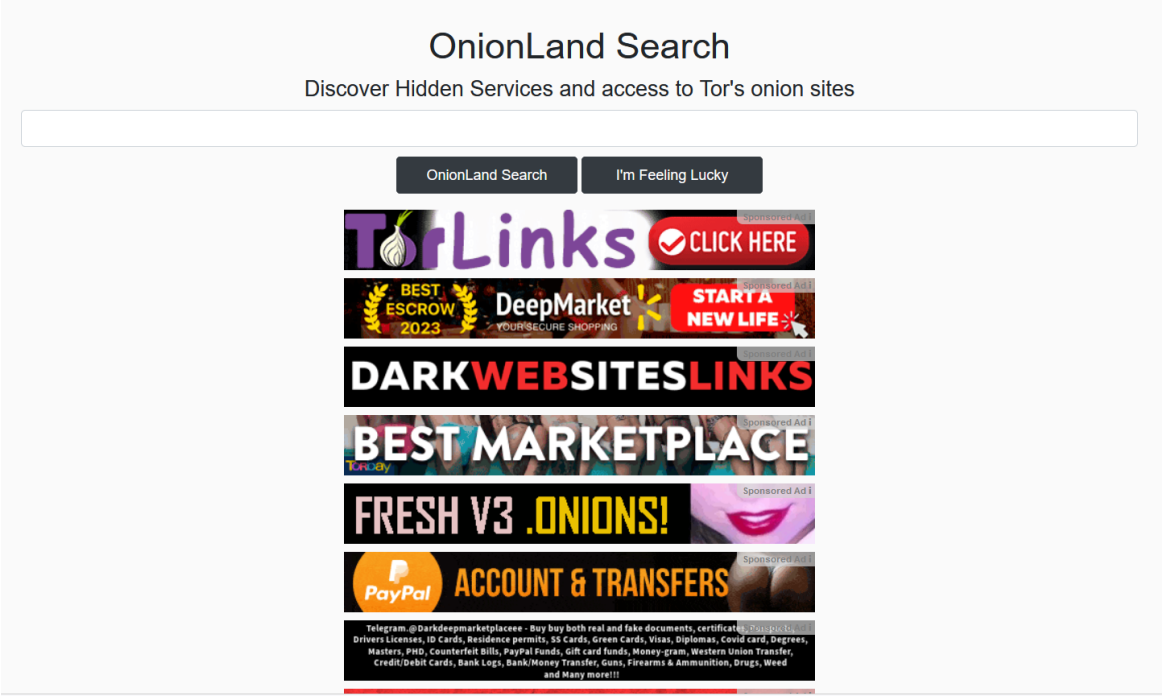

Abbildung 4.5: Suchmaschine Onion Land [54]

Onion Land enthält ebenfalls eine Liste der populärsten Hidden Services, sortiert basierend auf einem Algorithmus der Webseite. Hier werden die Position, der Onion-Link, der Titel und eine Beschreibung sowie das Datum, an dem der Service zuletzt online war, aufgelistet.

Auch diese Suchmaschine filtert keine kinderpornographischen Inhalte heraus. So befindet sich zum Beispiel auf dem zehnten Platz eine Webseite mit dem Titel “CP Porn Video”. Die Abkürzung CP steht in diesem Fall für Child Pornography, zu Deutsch Kinderpornografie. Auch auf dieser Webseite befinden sich Werbeanzeigen der gleichen Art wie bei Tordex.

Ein ähnliches Ranking bietet die Suchmaschine Tor66 an. Hier werden die 100 populärsten Hidden Services aufgelistet. Es ist möglich, nach speziellen Sprachen zu filtern. Jedoch sind zur jeweiligen Webseite nur der Titel und der Onion-Link, sowie das Logo angegeben. Auch bei dieser Suchmaschine sind Werbeanzeigen ähnlich derer auf den Seiten Tordex und Onion Land zu sehen. Außerdem werden bei Suchergebnissen zunächst drei sogenannte “promoted Sites”, zu Deutsch beworbene Seiten, angezeigt. [56]

Solche beworbenen Seiten sind auch auf der Webseite der Suchmaschine Excavator zu sehen. Hier handelt es sich unter anderem auch um Hidden Services, die explizit angeben, kinderpornographisches oder jugendpornographisches Material anzubieten. Die Webseite wirbt damit, für 150$ pro Monat dort eine Anzeige schalten zu können. [57]

Zusammenfassend lässt sich feststellen, dass Suchmaschinen, die das Dark Web durchsuchen, illegale Inhalte nicht nur indexieren, sondern teilweise auch bewerben. Nutzern des Dark Webs wird die Suche und der Zugriff auf solche Hidden Services so deutlich erleichtert. Nur wenige Suchmaschinen entscheiden sich dazu, kinderpornographische Inhalte herauszufiltern.

4.2 Legale Inhalte

Neben vielen eindeutig illegalen Inhalten und Hidden Services, die sich in einer rechtlichen oder ethischen Grauzone bewegen, gibt es im Dark Web auch einige Hidden Services, die legale Dienste anbieten. Dabei handelt es sich hauptsächlich um Services, welche die Ziele verfolgen, für welche das Tor Netzwerk zunächst gegründet wurde. Das Vermeiden von Zensur und das Fördern der Privatsphäre der Nutzer.

Beispiele hierfür sind Services im Bereich Whistleblowing, also das Teilen von geheimen oder geschützten Informationen, die für die Öffentlichkeit wichtig sind. Ebenso zählen Hidden Services, die Betriebssysteme zum Download und zur Nutzung anbieten, in den legalen Bereich. Genauso wie Nachrichtenmedien, die mit ihrem Auftritt im Dark Web Informationen für Menschen in Ländern mit zensiertem Internetzugriff anbieten.

4.2.1 Whistleblowing

Der Duden bezeichnet Whistleblowing als “Aufdeckung von Missständen [in Unternehmen, Behörden o. Ä.]” [58]. Bei solchen Missständen handelt es sich oft um Straftaten, wie beispielsweise Korruption, Insiderhandel, Menschenrechtsverletzungen oder Datenmissbrauch.

Sogenannte Whistleblower, im Deutschen auch als Informanten oder Hinweisgeber bezeichnet, machen sich dabei teilweise selbst strafbar oder riskieren ihr Arbeitsverhältnis sowie ihre eigene Unversehrtheit. So gibt es dokumentierte Fälle von Auftragsmorden an Whistleblowern oder auch Whistleblower, die in relativ jungen Alter auf ungeklärte Weise versterben oder angeblich Suizid begehen. [59]

Zu bekannten Whistleblowern zählt unter anderem Edward Snowden, der das US-amerikanische Programm Planning tool for Resource Integration, Synchronization, and Management (PRISM) aufdeckte [59, 60]. Außerdem auch Chelsea Manning, die auf der Plattform Wikileaks Informationen des US-amerikanischen Militärs über den Irakkrieg und den Afghanistan-Krieg veröffentlichte [59, 61]. Daniel Ellsberg, der die Pentagon-Papiere über das Fehlverhalten mehrerer US-Regierungen während des Vietnamkriegs veröffentlichte, zählt ebenfalls zu den Whistleblowern [59].

Auch an der Watergate-Affäre, die zum Rücktritt des US-Präsidenten Richard Nixon führte, war unter einem Decknamen ein Whistleblower beteiligt. Die Identität dieses Whistleblowers als FBI-Agent Mark Felt wurde erst 33 Jahre später bekannt. [59]

Die Wichtigkeit und Legalität des Whistleblowings werden immer noch diskutiert, insbesondere im Zeitalter von Plattformen wie Wikileaks, die es ermöglichen, auch anonym Informationen zu veröffentlichen [62].

Die Möglichkeit solche Daten weiterzugeben bieten nicht mehr nur spezielle Whistleblowing-Plattformen, sondern auch viele Zeitungen. Dafür wird besonders oft der Service SecureDrop (deutsch: Sicherer Einwurf) verwendet. Dabei handelt es sich um eine freie Plattform zur sicheren Kommunikation zwischen Journalisten und Whistleblowern.

Die Webseite des Dienstes ist auch im Clear Web verfügbar. Dort wird allerdings ausdrücklich darauf hingewiesen, dass zur Benutzung der Tor Browser nötig ist.

Die Funktionsweise des Service lässt sich an der Abbildung 4.6 erkennen.

Eine Quelle, also ein Informant lädt seine Informationen über den Tor-Browser hoch. Die Nachrichtenstelle hat dort eine Art Postfach eingerichtet. [63]

Der Journalist verbindet sich mit SecureDrop über eine sogenannte Journalist Workstation, die von einem Universal Serial Bus (USB)-Stick aus gestartet wird. Dann erhält er die Daten aus dem Postfach. [63]

Die Daten werden anschließend auf physischem Weg, zum Beispiel auf einem USB-Stick oder einer Compact Disc (CD), zu einem getrennten und nicht mit dem Internet verbundenen Gerät, der Secure Viewing Station, gebracht. Auf diesem Gerät kann der Journalist nun die Daten einsehen, verarbeiten, ausdrucken oder auf ein weiteres Gerät exportieren. [63]

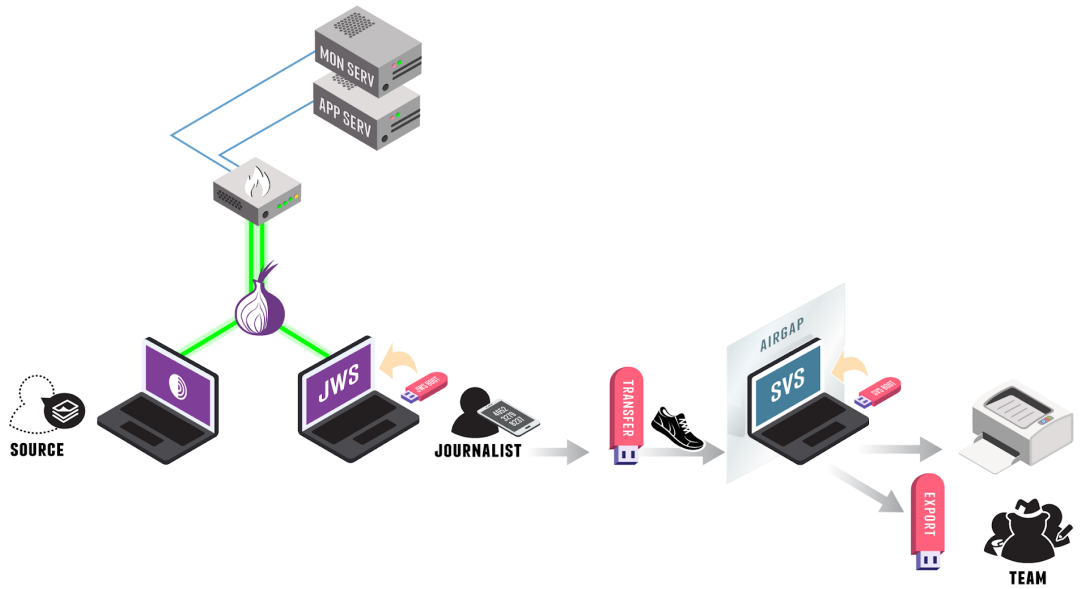

Abbildung 4.6: SecureDrop Funktionsweise [63]

SecureDrop gibt an, dass keine Dritten Zugriff auf die Daten erhalten können, da der Server komplett im Besitz der Nachrichten-Organisation ist. Außerdem werden so wenig Metadaten wie möglich gespeichert, weder über den Browser noch über die IP-Adresse. Zusätzlich wirbt SecureDrop mit Verschlüsselung der Daten und Schutz gegenüber Hackern. [63]

Organisationen, die auf dem SecureDrop Hidden Service ein Postfach haben, sind unter anderem The Washington Post, The Guardian, ProPublica, The Intercept, Al Jazeera Media Network und TechCrunch, sowie viele weitere.

Neben dem direkten Kontakt zu bekannten Nachrichten-Organisationen und Zeitungen gibt es noch weitere Hidden Services, die im engeren oder weiteren Sinne zum Bereich Whistleblowing gehören.

Einer diesen Hidden Services ist SpecTor. Dabei handelt es sich um einen Service der niederländischen Polizei und weiteren Behörden in Verbindung mit der gleichnamigen Operation SpecTor. Bei dieser internationalen Maßnahme wurde der sogenannte “Monopoly Market”, ein Drogen Marktplatz, übernommen und basierend auf den so erlangten Beweisen mehrere Ermittlungsverfahren und Festnahmen durchgeführt. [64]

Die SpecTor Webseite listet verhaftete Verkäufer mit ihrem Benutzernamen und ihrer Nationalität auf. Außerdem verweist sie im Bereich Frequently Asked Questions (FAQ), oft gestellte Fragen, auf eine Stelle, an der anonym Informationen über Verkäufer auf Dark Web Marktplätzen an die niederländische Polizei weitergegeben werden können.

Ähnlich ist auch der Hidden Service, den die US-amerikanische Organisation CIA im Dark Web zur Verfügung stellt. Es handelt sich um die gleiche Webseite, die auch im Clear Web verfügbar ist. Auch hier gibt es, über ein Online-Formular, die Möglichkeit, Informationen zu hinterlassen. [65]

Ähnlich wie die Webseite von SpecTor bietet auch The Northern California Illicit Digital Economy (NCIDE) Task Force einen Hidden Service an. Auf diesem sind sowohl verhaftete Verkäufer als auch Verkäufer, die mit Behörden kooperieren, aufgelistet. Die Möglichkeit, Informationen an diese Organisation weiterzugeben, wird aufgelistet, aber der Link funktioniert nicht. [66]

Bei Distributed Denial of Secrets handelt es sich um einen weiteren Hidden Service aus dem Bereich Whistleblowing, der ebenfalls im Clear Web und im Dark Web verfügbar ist. Der Hidden Service bietet ein Archiv für Daten und Informationen, die veröffentlicht wurden und von Interesse für die Öffentlichkeit sind. Eingereichte Informationen werden dabei auf ihren Wahrheitsgehalt überprüft. [67]

Die Website bietet zwei Möglichkeiten als Kontakt an. Einen Link zu GlobaLeaks, einer Software ähnlich wie SecureDrop und eine E-Mail-Adresse sowie die Anweisung, die E-Mail mit dem Pretty Good Privacy (PGP)-Schlüssel der Organisation zu verschlüsseln. Außerdem gibt es auch ein SecureDrop Postfach des Institute for Quantitative Social Science der Harvard Universität, welches mit der Organisation zusammenarbeitet. Neben diesen Möglichkeiten werden außerdem Hinweise für Whistleblower und den Umgang mit den veröffentlichten bzw. weitergegebenen Daten bereitgestellt.

Whistleblowing ist eine Verwendung des Dark Webs, die oft als Pro-Argument für das Tor-Netzwerk aufgebracht wird. Unabhängig von der rechtlichen oder moralischen Beurteilung des Whistleblowings ist klar, dass über das Tor-Netzwerk eine zusätzliche Sicherheit für Whistleblower gewährleistet wird.

4.2.2 Betriebssysteme

Wie bei vielen legalen Inhalten, die im Dark Web angeboten werden, sind auch manche Betriebssysteme sowohl im Clear- als auch Dark Web verfügbar. Dies sind meist Betriebssysteme, die einen größeren Fokus auf IT-Sicherheit und das Schützen der Privatsphäre der Nutzer legen.

Dass diese Betriebssysteme auch über das Dark Web und den Tor Browser angeboten werden, ist verständlich. Denn Nutzer des Tor-Netzwerks und der Hidden Services haben großes Interesse am Schutz ihrer Privatsphäre. [68]

Qubes OS stellt ein Beispiel eines Systems dar, dass sowohl im Clear- als auch im Dark Web angeboten wird. Das Betriebssystem hat zum Ziel, Sicherheit durch Isolation zu erreichen. Dafür kommen mehrere virtuelle Maschinen zum Einsatz. [69]

Ein weiteres Betriebssystem, das ebenfalls auf einem Hidden Service bereitgestellt wird, ist Whonix. Dabei handelt es sich um eine Linux-Distribution basierend auf Debian. Im Fokus steht die Privatsphäre der Nutzer, sowie Sicherheit und Anonymität im Internet. Dazu wird jede Netzwerkkommunikation über das Tor Netzwerk durchgeführt. [70]

Auch dieses Betriebssystem arbeitet mit virtuellen Maschinen. Eine wird als sogenannte Workstation verwendet, in der alle Applikationen des Benutzers laufen und eine zweite als Gateway für das Tor-Netzwerk. [70]

Ebenfalls auf Debian basiert das Betriebssystem The Amnesic Incognito Live System (Tails). Auch dieses ist über das Dark Web zum Download verfügbar. Auch hier sind die Ziele Anonymität und das Schützen der Privatsphäre, wofür ebenfalls auf das Tor-Netzwerk gesetzt wird. [71]

Es ist möglich, Tails direkt von einem USB-Stick oder einer Live CD zu booten. Das Betriebssystem schreibt nicht auf der Festplatte, sondern arbeitet nur im Arbeitsspeicher, welcher beim Herunterfahren vollständig gelöscht wird. So hinterlässt es keine Spuren auf dem Computer. [71]

Doch nicht nur auf Debian basierende Betriebssysteme, sondern auch Debian selbst ist über das Dark Web verfügbar [72].

Insbesondere bei Betriebssystemen, die bereits den Tor-Browser vorinstalliert zur Verfügung stellen, ist es sehr nachvollziehbar, dass diese ebenfalls einen Internetauftritt im Dark Web haben, damit die Nutzer sie sicher und anonym herunterladen und benutzen können.

4.2.3 Nachrichtenmedien

Unabhängige Medien, Berichterstattung und Journalismus, sowie die Möglichkeit der freien Meinungsäußerung sind essenziell für das Erhalten einer Demokratie. In unterdrückten und autokratischen Ländern werden Nachrichtenmedien oft vom Staat kontrolliert oder zensiert. Der Zugang zu unabhängiger oder regierungskritischer Berichterstattung ist oft erschwert oder illegal.

Auch der Internetzugang wird oft eingeschränkt, ein aktuelles Beispiel ist das Projekt „Great Firewall of China“. Sowohl das Veröffentlichen als auch das Einsehen von Informationen im Internet wird durch die chinesische Regierung zensiert. [73]

Das Tor-Projekt gibt auf seiner Webseite deswegen an, wie auch in China der Tor-Browser und das Tor-Netzwerk genutzt werden können. So kann die Zensur umgangen und die freie Meinungsäußerung, sowie die Informationsfreiheit geschützt werden. [74]

Um Menschen in Ländern mit Internetzensur speziell den Zugang zu Nachrichten zu erleichtern, gibt es einige Nachrichtenmedien, die ihre Inhalte auch auf dem Dark Web in Form eines Hidden Service veröffentlichen.

Von den meisten großen Nachrichtenorganisationen und Zeitungen gibt es nur SecureDrop Postfächer. Deutlich weniger Organisationen stellen ihre Nachrichten auch über einen Hidden Service zur Verfügung. Bekannte Nachrichtenseiten mit Dark Web Auftritt sind unter anderem die britische öffentlich-rechtliche Organisation British Broadcasting Corporation (BBC) und die US-amerikanische Tageszeitung The New York Times. Auf beiden Webseiten wird sowohl über nationale als auch über internationale Themen berichtet.

The New York Times ist weltweit die Zeitung mit den meisten Pulitzer Preis Auszeichnungen und den meisten Abonnenten. Seit 2017 ist die Onlineausgabe der Tageszeitung auch im Dark Web verfügbar. [75]

Die BBC ist seit 2019 im Dark Web vertreten. Laut eigenen Angaben hatten zuvor unter anderem die Länder China, Iran und Vietnam versucht, die Zugänge zu den BBC News, den Nachrichten der BBC, zu blockieren. Neben der internationalen Version gibt es auch eine ukrainische und eine russische Version. Auf diesen werden national relevante Nachrichten in den entsprechenden Sprachen veröffentlicht. [76]

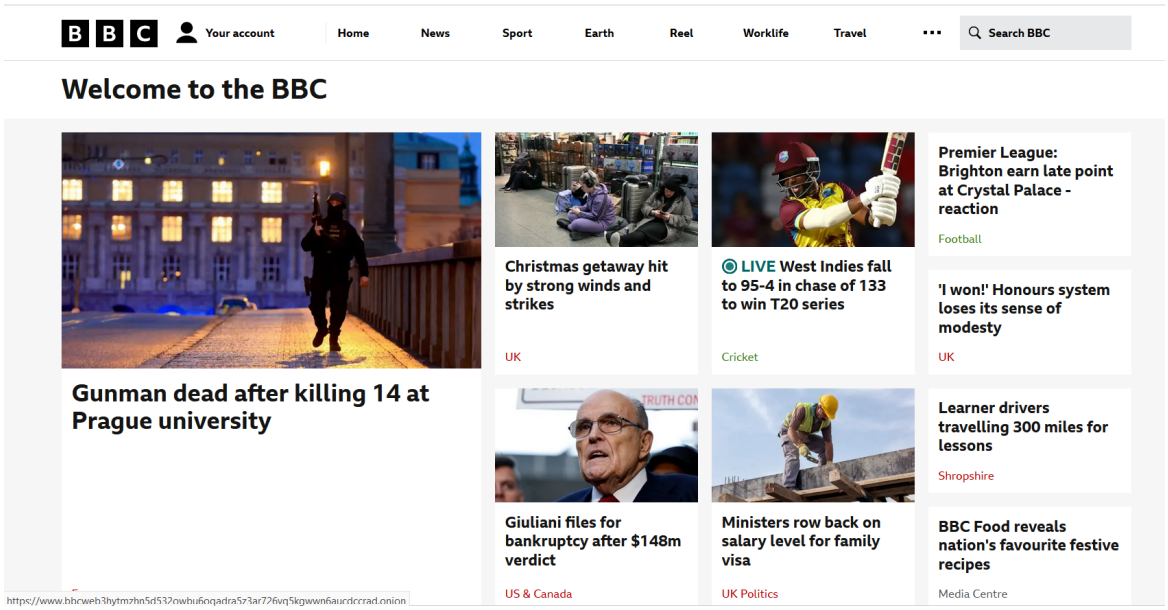

Abbildung 4.7: Hidden Service BBC News [76]

ProPublica ist eine weitere Nachrichtenquelle im Dark Web. Dabei handelt es sich um einen 2007 gegründeten Non-Profit-Newsdesk für investigativen Journalismus und die größte Organisation dieser Art. 32 festangestellte Journalisten und über 2200 Freiwillige arbeiten bei ProPublica an der Aufrechterhaltung des investigativen Journalismus. Diesen sieht die Organisation in den USA als vernachlässigt. [77]

Der Newsdesk wird von mehreren Stiftungen finanziell unterstützt und hat bereits mehrere Auszeichnungen für seine journalistischen Leistungen erhalten. Seit 2016 ist ProPublica in Folge einer Recherche über die Internetzensur in China auch als Hidden Service im Dark Web verfügbar. [77]

Eine deutsche Organisation, die auch im Dark Web internationale Nachrichten anbietet, ist die Deutsche Welle. Mit der internationalen DW-Webseite will die unabhängige Medienorganisation laut eigenen Angaben die “Förderung einer friedlichen, stabilen Weltgemeinschaft erreichen”. Berichtet wird in 32 Sprachen über Themen wie "Freiheit und Menschenrechte, Demokratie und Rechtsstaat, Welthandel und soziale Gerechtigkeit, gesundheitliche Aufklärung und Umweltschutz, Technologie und Innovation". [78]

Seit 2019 ist die Webseite auch als Hidden Service im Dark Web verfügbar. Zurzeit werden insbesondere Nachrichten zum Nahost-Konflikt und der Ukraine priorisiert. [78]

Ein Hidden Service der sich speziell mit Nachrichten über das Dark Web selbst befasst ist DarkNetLive. Die Webseite ist auch im Clear Web verfügbar. Publiziert werden zum Beispiel Nachrichten über Verhaftungen von Verkäufern auf Dark Web Marktplätzen. [79]

Außerdem listet die Webseite auch die Onion-Adressen von neun verschiedene Dark Web Märkten auf. DarkNetLive enthält generell eine umfassendere Liste von Onion-Links, die zu Hidden Services verschiedener Kategorien von Suchmaschinen bis VPNs oder Foren führen. Darin werden unter anderem auch explizit Marktplätze aufgelistet, die inzwischen nicht mehr aktiv sind. [79]

Die veröffentlichten Artikel über Nachrichten können mit Hilfe eines Tagsystems durchsucht werden. Tags sind eine Art Markierung von Inhalten mit Schlagwörtern. Besonders häufig verwendet werden die Tags General-News (1020), Dark Web-Vendors (352), Arrested (225) und Drug-Bust (211). Auf Deutsch bedeuten diese Tags in etwa allgemeine Nachrichten, Dark Web Verkäufer, Verhaftet und Drogen Razzia. [79]

Die Artikel sind meist kurze Zusammenfassung von verlinkten Nachrichtenmeldungen oder Presse Veröffentlichungen. Unter den Artikeln haben Nutzer die Möglichkeiten Kommentare zu hinterlassen. Oft äußern sich die kommentierenden Nutzer negativ über die in den Artikeln betroffenen, beispielsweise verhafteten Personen. [79]

4.2.4 Kommunikationsdienste

Neben sozialen Medien, die auch im Clear Web verbreitet sind, zählen zu den Kommunikationsdiensten im Dark Web vor allem Chats oder sogenannte Chat Rooms, zu Deutsch Chat Räume. Außerdem werden für den Zweck dieser Arbeit auch E-Mail-Provider im weiteren Sinne als Kommunikationsdienste angesehen. Foren hingegen werden aufgrund ihrer größeren Eigendynamik und der teilweise zweifelhafteren Legalität separat betrachtet.

Kommunikationsdienste im Dark Web erfüllen ähnliche Funktionen wie ihr Äquivalent im Clear Web. Nutzer können in Echtzeit mit Hilfe von Textnachrichten über das Internet miteinander kommunizieren, teilweise anonym.

Wie bereits in 2.3.2 erwähnt, bietet Facebook seine Webseite auch als Hidden Service unter einer Onion-Adresse an. So erhalten Nutzer mehr Schutz ihrer Privatsphäre als bei der Nutzung über das Clear Web. Jedoch ist immer noch ein Einloggen erforderlich und es müssen außerdem die gleichen Datenschutzbedingungen des Konzerns Meta akzeptiert werden.

Anders verhält es sich mit dem Dienst Nitter. Dieser ist sowohl im Clear- als auch im Dark Web verfügbar. Es handelt sich um einen kostenlosen open source Dienst mit dem Tweets (Posts auf der Plattform Twitter, mittlerweile genannt X) angesehen werden können, ohne sich einloggen zu müssen. Das Einloggen ist bei der von Elon Musk übernommenen Plattform inzwischen Pflicht, um sich Inhalte anzusehen. [80]

Durch die Nutzung von Nitter können die Nutzer ihre Privatsphäre schützen und weiterhin anonym bleiben.

Man kann auf der Webseite lediglich spezifisch nach einem Nutzer anhand seines Namens suchen. Selbst Posts verfassen, Kommentare schreiben, Liken oder Einträge teilen kann man mit dem Dienst nicht. Dies würde sich negativ auf das Erhalten der Anonymität ausüben.

Wer selbst über das Dark Web kommunizieren will kann zum Beispiel einen Chatraum benutzen. Es gibt mehrere Hidden Services, die solche Chaträume zur Verfügung stellen. Diese Chats sind meist anonym und temporär. Der Nutzer weist sich selbst durch Eingabe in ein Textfeld einen Benutzernamen, genannt Nickname, zu. Eventuell wählt er noch eine Farbe, in der dieser Name im Chat erscheinen soll. Anschließend wird er direkt in den Chatraum weitergeleitet, in dem sich weitere Nutzer befinden. Mit diesen kann dort über Textnachrichten kommuniziert werden.

Manche Hidden Services zeigen zuvor oder während des Chats die Anzahl der anwesenden Teilnehmer an. Bei den ausgetauschten Nachrichten handelt es sich meist um oberflächliche Gesprächsthemen, oft kommen auch keine richtigen Gespräche zustande. Stattdessen werden Nachrichten ohne Bezug auf die anderen Nutzer geschrieben. Besonders häufig werden Beleidigungen und Schimpfwörter benutzt. Teilweise wird auch nach Verkäufern für bestimmte Drogen oder andere Güter gefragt oder ein bestimmter Marktplatz bzw. Onlineshop beworben. In Abbildung 4.8 ist beispielsweise ein Auszug aus dem Chatraum Red Hat Chat dargestellt.

Viele Chaträume sind öffentlich und verlangen kein Login. Der Benutzername kann frei und unabhängig gewählt werden. Es gibt keine Möglichkeit Chatverläufe oder Kontakte zu speichern.

Anders verhält es sich beim Hidden Service ChaTor. Dieser Service bietet Einzel-Konversationen an. Er ist in der Funktion grundlegend vergleichbar mit weit verbreiteten Nachrichtendiensten wie zum Beispiel WhatsApp. Zunächst wird ein Login mit einem Benutzernamen und Passwort gefordert. Will man mit einem Nutzer kommunizieren, ist es notwendig, dessen Benutzernamen zu kennen. Anschließend kann der Einzel-Chat genutzt werden. [82]

Abbildung 4.8: Auszug aus dem Chatraum Red Hat Chat [81]

Inwiefern all diese Chat Angebote von Dark Web Nutzern tatsächlich genutzt werden, ist schwer feststellbar. Öffentliche Chaträume mit mehreren Personen scheinen wenige Nutzer zu haben. Dies kann unter anderem daran liegen, dass es sehr viele verschiedene Chaträume gibt, auf die sich die Gesamtanzahl der Nutzer verteilen kann. Außerdem erscheinen der Austausch und die Konversationen in diesen Chaträumen nur selten produktiv. Oft findet kein tatsächlicher Informationsaustausch statt. Es ist zu vermuten, dass es an anderer Stelle auch private Chaträume gibt, zu denen beispielsweise eine Einladung erfolgen muss. Oder, dass die Nutzer stattdessen eher auf Foren ausweichen.

Für eine andere Art der Kommunikation gibt es im Dark Web genau wie im Clear Web mehrere E-Mail-Anbieter.

Manche dieser Anbieter, wie zum Beispiel Onion Mail, Alt Address und Proton Mail sind auch im Clear Web verfügbar. Andere Hidden Services hingegen schränken das Versenden und Empfangen von Emails auf das Tor Netzwerk ein. So können beispielsweise über den E-Mail-Anbieter TorBox keine Emails von Diensten wie Gmail oder Yahoo empfangen werden, sondern nur Emails vom Anbieter selbst oder solche, die von anderen Mail Anbietern an diesen weitergeleitet werden [83].

Die Funktionen und das Design der E-Mail-Anbieter im Dark Web sind sehr ähnlich zu typischen E-Mail-Anbietern im Clear Web. Die E-Mail-Postfächer zeigen eingegangene und gesendete E-Mails an. Oft gibt es ebenfalls die Möglichkeit Spam-Filter einzurichten und E-Mails mit bestimmten Kriterien abzufangen. Manche Hidden Service sind jedoch simpler gehalten und bieten diese Möglichkeit nicht an.

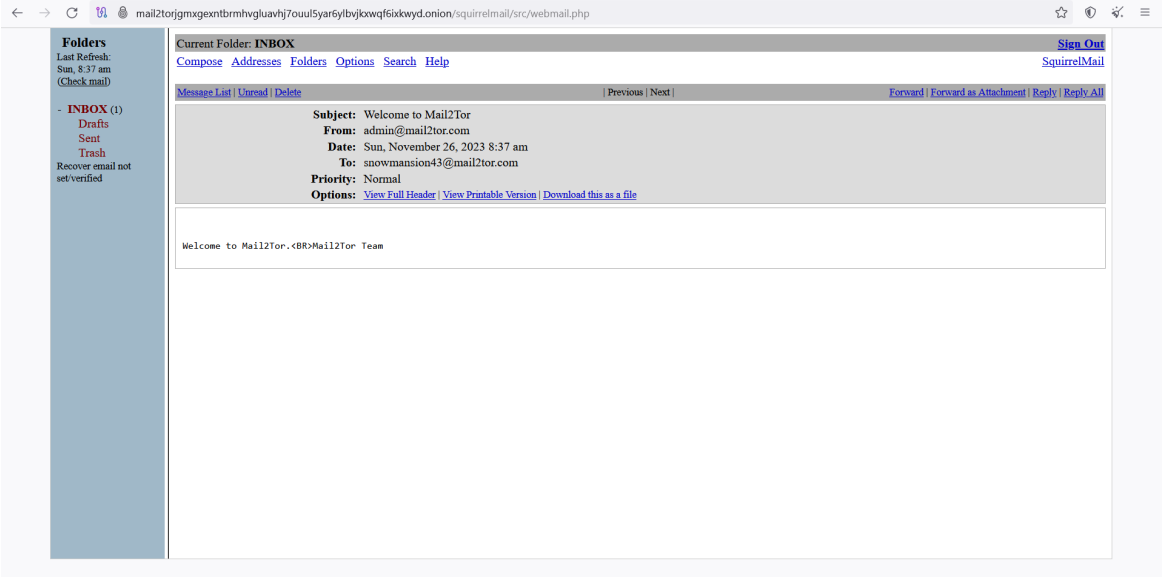

Abbildung 4.9: E-Mail-Anbieter mail2tor [84]

Einige Hidden Services wie zum Beispiel Marktplätze fordern bei der Anmeldung und der Erstellung eines Accounts das Angeben eine E-Mail-Adresse. Bei manchen Verkäufern im Dark Web findet die Kommunikation und der Kaufprozess ausschließlich per E-Mail statt. Es ist demnach für die Nutzer sinnvoll zur Aufrechterhaltung der Anonymität und Privatsphäre eine separate E-Mail-Adresse bei einem Anbieter im Tor-Netzwerk zu erstellen.

4.3 Rechtliche Grauzone

Viele Inhalte und Angebote im Dark Web sind nicht eindeutig als legal oder illegal einzuordnen. Das liegt vor allem an den unterschiedlichen Rechtslagen in unterschiedlichen Ländern. Sowie der oft nicht möglichen regionalen Zuordnung von Hidden Services. Sofern der Betreiber des Service nicht ausdrücklich über seinen Standort informiert, sind diese Informationen selten. Selbstauskünfte können darüber hinaus auch unwahr sein.

Zusätzlich gilt, auch wenn das Anbieten von beispielsweise pornografischen Inhalten im Land des Anbieters legal ist, so kann der Konsum im Rechtsgebiet der Konsumenten trotzdem verboten sein.

Im Rahmen dieser Arbeit werden Inhalte für eine Einteilung im Zweifelsfall nach deutschem Recht beurteilt .

Ein Beispiel für rechtliche Grauzonen sind Webseiten, auf denen Nutzer Inhalte hochladen können. Während die Webseite an sich nicht illegal sind, kann über die Nutzer doch illegales Material auf diese Plattformen gelangen. Diese Probleme gibt es auch bei Seiten, wie beispielsweise sozialen Medien. Oft muss hier der Anbieter Inhalte löschen, die unangemessene Fotos, Videos oder Hass und Hetze enthalten.

In eine gewisse Grauzone fallen ebenfalls Dienste, die für Filesharing genutzt werden, da hier durchaus illegale Dateien wie beispielsweise kinderpornographische Inhalte geteilt werden können. Aber auch Internetarchive und digitale Bibliotheken verletzen in manchen Fällen das Urheberrecht, bieten aber auch legale Inhalte an und sind nicht grundsätzlich verboten.

Im Bereich Kryptowährungen ist unter anderem die Legalität von sogenannten Krypto-Mixern fraglich. Es gibt noch keine Gesetze bezüglich dieser Dienstleister und in den meisten Ländern sind sie somit legal. Jedoch besteht das Risiko, in die Nähe des Straftatbestands der Geldwäsche zu kommen (§ 261 StGB). So wurde zum Beispiel im März 2023 Chipmixer, ein viel genutzter Kryptowährungs Mischdienst vom Bundeskriminalamt (BKA) Deutschland, gestoppt, da er als Geldwäsche-Plattform genutzt wurde. Laut dem BKA handelte es sich um die weltweit größte Geldwäsche-Plattform im Dark Web. [85]

4.3.1 Bibliotheken und Archive

Auch im Clear Web gibt es viele digitale Bibliotheken und Archive. Zum Beispiel das “Internet Archive” archive.org. Oder Sci-Hub, eine sogenannte Schattenbibliothek für wissenschaftliche Arbeiten und Artikel.

Bei Schattenbibliotheken handelt es sich um Datenbanken im Internet, in denen vollständige Texte zur Verfügung stehen. Sie können von der Öffentlichkeit eingesehen werden, so wie klassische Bibliotheken. Jedoch wird keine Rücksicht auf mögliche Urheberrechtsverletzungen genommen. [86]

Nicht nur Bücher und schriftliche Dokumente sind auf diese Art und Weise im Internet zu finden, sondern auch andere Medien wie Filme, Hörbücher und Serien. Zahlreiche Webseiten bieten auch im Clear Web solche Inhalte an. In vielen Ländern werden die Zugänge zu diesen Seiten mittlerweile eingeschränkt und regelmäßig gehen Seiten aufgrund von Verfahren oder Anklagen im Bereich Urheberrechtsverletzung offline.

Die im Dark Web verfügbaren Archive und Bibliotheken bzw. Schattenbibliotheken unterscheiden sich nicht wesentlich von denen im Clear Web.

Unter anderem bieten manche Betreiber dieser Art von Webseiten ihren Service in gleicher Form sowohl im Clear- als auch im Dark Web an. Zum Beispiel Z-Library, eine Schattenbibliothek, die sich selbst als größte E-Book-Bibliothek bezeichnet. Zwischenzeitlich, im November 2022, war Z-Library aufgrund von Beschlagnahmung durch das Federal Bureau of Investigation nur noch über den Hidden Service im Tor Netzwerk erreichbar. Inzwischen ist die Webseite jedoch wieder in das Clear Web zurückgekehrt. [87]

Um Bücher von der Bibliothek herunterzuladen, muss man einen Account erstellen und sich anmelden. Andere Schattenbibliotheken, wie beispielsweise Sci-Hub bieten ihre Daten auch ohne Anmeldung an.

Weitere Bibliotheken im Dark Web sind zum Beispiel Comic Book Library, Imperial Library of Trantor, Bible4u oder Just Another Library. Über diese Seiten werden Comics, Bücher, wissenschaftliche Publikationen, religiöse Texte oder Hörbücher zur Verfügung gestellt. Schriftliche Inhalte sind oft im PDF-Format zum Download verfügbar.

Manche Bibliotheken spezialisieren sich auf bestimmte Themengebiete. Besonders häufig handelt es sich dabei um religiöse Texte wie zum Beispiel die Bibel, die in unterschiedlichen Sprachen, Fassungen und Übersetzungen von mehreren Hidden Services angeboten wird. Aber auch die Bereiche Anarchismus und Marxismus haben oft eigene Bibliotheken und Archive. Hier werden neben Fachliteratur und Schriften von bekannten Persönlichkeiten wie Karl Marx und August Bebel auch Texte geteilt und zur Verfügung gestellt, die von den Nutzern und Mitgliedern verfasst wurden. Damit wird eine zusätzliche Möglichkeit des Austausches geschaffen.

In vielen englischsprachigen Ländern gehen veröffentlichte Texte nach einer bestimmten Zeit in die sogenannte Public Domain über und können von der Öffentlichkeit so genutzt werden, ohne gegen das Urheberrecht zu verstoßen. In Deutschland gibt es kein direktes Äquivalent zu diesem Prinzip. Hier gibt es lediglich die sogenannte Gemeindefreiheit, die für alle geistigen Schöpfung gilt, an denen keine Urheberrechte bestehen. Diese Werke können von jedem ohne nötige Genehmigung oder Zahlung zu beliebigen Zwecken genutzt werden. [88]

Dabei kann es sich um Werke handeln, deren Schöpfer dies von selbst verfügt hat oder deren urheberrechtlicher Schutz abgelaufen ist. In vielen Ländern endet dieser Schutz zum Beispiel 70 Jahre nach dem Tod des Verfassers. [88]

Unabhängig von der jeweiligen nationalen Rechtslage sind jedoch viele der in den Bibliotheken und Archiven verfügbaren Werke immer noch vom Urheberrecht betroffen. Die Hidden Services bewegen sich damit also oft in einer rechtlichen Grauzone oder auch klar im illegalen Handlungsfeld.

Bibliotheken, beispielsweise die Comic Book Library (siehe Abbildung 4.10), die ihrem Namen entsprechend Comicbücher anbietet, haben oft die Möglichkeit, Suchanfragen zu bestimmten Werken zu stellen. Außerdem ist die Navigation anhand von Kategorien und Sortieroptionen wie Titel, Herausgeber, Jahr und Autor möglich. Zusätzlich gibt es ein Tag-System, das es dem Nutzer ermöglicht gezielt nach bestimmten Genres oder Schlagwörtern wie zum Beispiel “Gay”, “Ducks”, “Robots”, “Monsters” oder “Iron Man” zu suchen.

Eine Besonderheit stellt der Hidden Service Webpage Archive dar. In diesem Archiv werden ähnlich wie beim Clear Web Service Wayback Machine Momentaufnahmen von Webseiten archiviert. Es gibt auf der Webseite zwei Möglichkeiten für die Nutzer. Man kann eine URL eingeben, um einen noch existierenden Hidden Services zu archivieren oder nach vergangenen Zuständen eines archivierten Hidden Service suchen. [90]

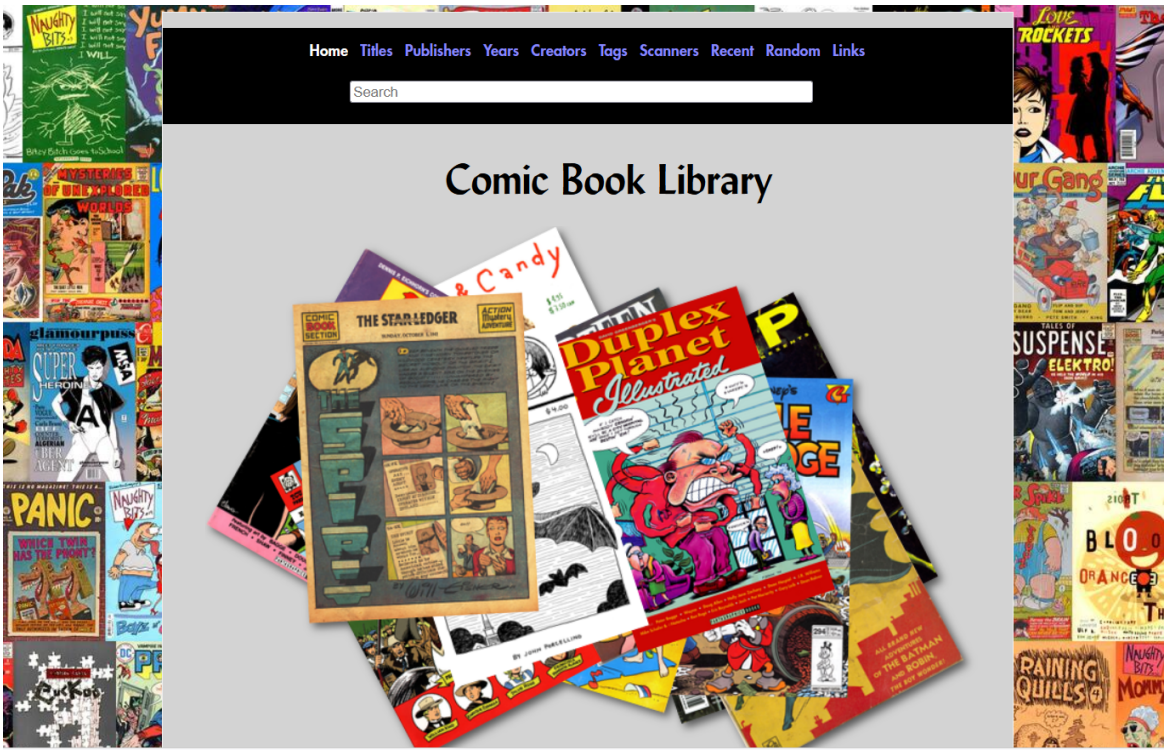

Abbildung 4.10: Hidden Service Comic Book Library [89]

4.3.2 Filesharing, Pastebins, Torrent

Neben dem Herunterladen von Dateien von Hidden Service Bibliotheken oder Archiven gibt es weitere Möglichkeiten, über das Dark Web an bestimmte Dateien zu gelangen. Zum Beispiel der gezielte Austausch mit einem oder mehreren anderen Dark Web Nutzern. Im Englischen wird dieser Austausch auch Filesharing genannt.

Es gibt verschiedene Arten des Filesharings. Entweder die direkte Kommunikation zwischen zwei Teilnehmern, sogenanntes Peer-to-Peer Filesharing oder das Teilen über Dritte. Dazu werden bestimmte Plattformen verwendet, die auch im Clear Web zu finden sind. Zum Beispiel Cloud Computing Anbieter wie Google Drive, Apple iCloud oder Microsoft OneDrive, die auf dem Prinzip des Nutzens von Speicherplatz auf fremden Servern basieren. [91]

Um kleinere Dateien für kürzere Zeiträume schnell mit anderen Nutzern teilen zu können, werden auch die sogenannten Pastebins verwendet. Dies sind Webanwendungen, über die Text veröffentlicht und somit geteilt werden kann.

Besonders häufig werden solche Pastebins unter anderem von Programmieren genutzt, die auf diese Weise Quellcode oder technische Informationen teilen. Deswegen bieten einige Services auch sogenanntes Syntax Highlighting, zu Deutsch Syntax Hervorhebung, an. Dies ist eine Funktion eines Programmes, bei der bestimmte Wörter sowie Zeichenkombination auf spezielle Art in unterschiedlichen Farben oder anderen Attributen wie Schriftstil hervorgehoben werden, ohne dass dies in der Datei gespeichert wird. Dadurch wird die Übersichtlichkeit eines Textes bzw. Quellcodes verbessert und er kann schneller erfasst werden.

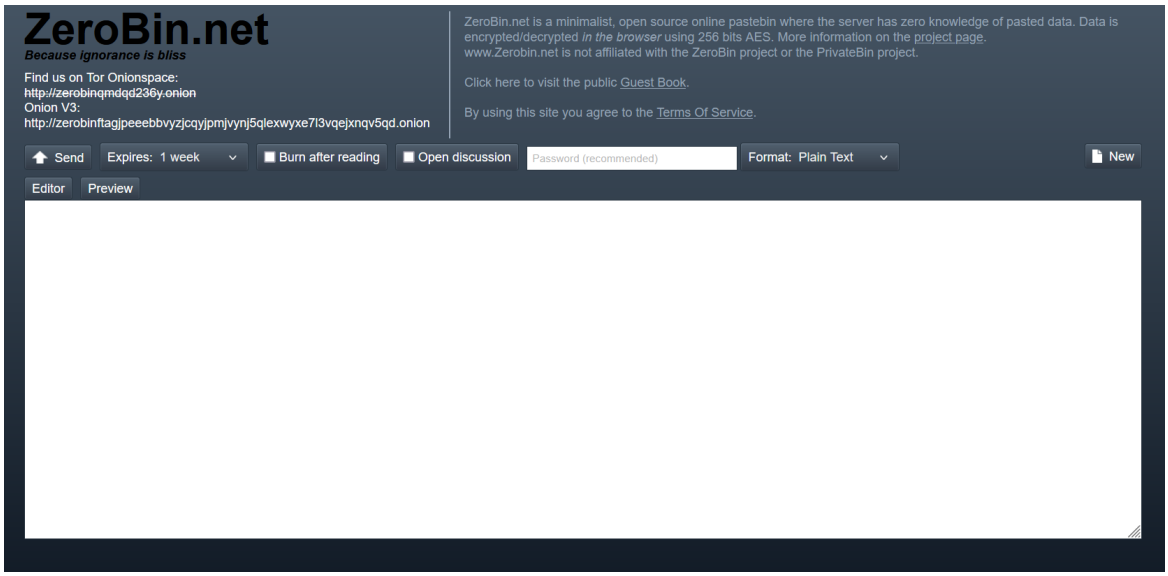

Abbildung 4.11: Hidden Service ZeroBin.net [92]

Pastebins im Dark Web sind ähnlich aufgebaut wie Pastebins im Clear Web. Dies liegt hauptsächlich an der recht simplen Funktionsweise. Abbildung 4.11 zeigt ein typisches Beispiel, den Hidden Service ZeroBin. Neben einem großen Textfeld für das Einfügen des Textes bieten die Hidden Services noch weitere Optionen wie Formatierungsoptionen oder das Einstellen eines Passwortes. Außerdem auch das Auswählen eines Ablaufdatums im Bereich von fünf Minuten bis hin zu einem Jahr oder keinem Ablaufdatum. Ebenfalls gibt es die Möglichkeit den Text nach dem Lesen direkt löschen zu lassen (Burn after reading) oder den Lesern das Kommentieren unter dem Text zu erlauben (Open discussion).

Nach der Eingabe des Textes und dem Betätigen der Schaltfläche “Send” für das Absenden des Textes wird ein Link generiert, der zum Text führt. Diesen kann der Nutzer nun kopieren und an die Personen weitergeben, mit denen er den Text teilen möchte.

Neben den Möglichkeiten, Text zu teilen, bieten einige Hidden Services auch die Möglichkeit Dateien, insbesondere Bilddateien zu teilen. Seiten wie dump.li, Starfiles und Black Cloud, von denen die beiden ersten auch im Clear Web verfügbar sind, bieten das Hochladen von Dateien an. Dump.li hat ein Limit von 3 MB, gibt die Möglichkeit ein Ablaufdatum festzulegen und fordert dazu auf, keine illegalen Dateien hochzuladen [93]. Black Cloud hat ein Limit von 300 MB [94]. Starfiles gibt kein Größenlimit an und bietet neben dem Hochladen von Dateien auch die Möglichkeiten Ordner zu erstellen, URLs zu kürzen und Youtube Videos nach URL-Eingabe in Dateien im mp4-Format umzuwandeln [95].

Eine weitere Möglichkeit, Dateien zu teilen ist die bereits erwähnte Peer-to-Peer Variante, genauer gesagt das kollaborative Filesharing-Protokoll BitTorrent.

Dies ist besonders für große Datenmengen geeignet und wird zum Beispiel vom Hidden Service The Pirate Bay genutzt. Die Startseite dieses Hidden Services ist in Abbildung 4.12 zu sehen.

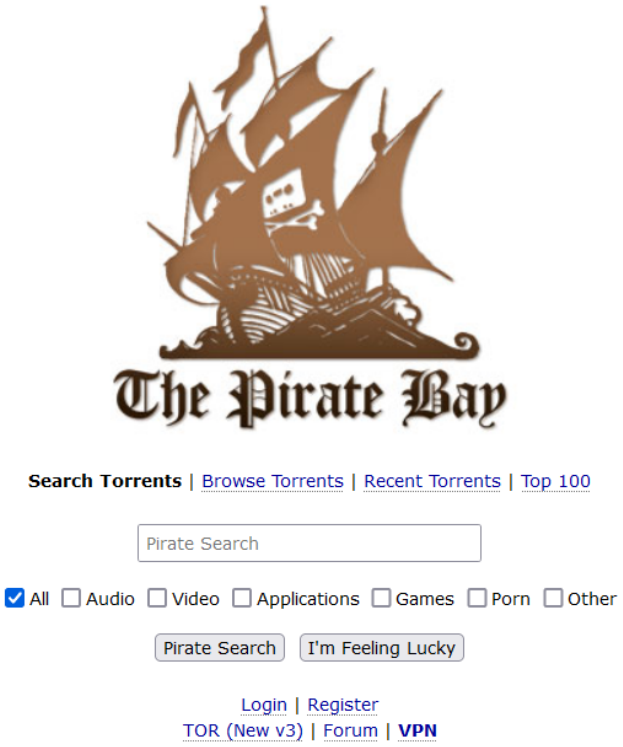

Abbildung 4.12: Hidden Service The Pirate Bay [96]

Es handelt sich um eine Webseite, die auch im Clear Web vertreten ist und digitale Inhalte, wie Filme, Serien, Bücher und Videospiele indiziert und ihren Nutzern sogenannte Torrent-Dateien zur Verfügung stellt.

Diese Torrent-Dateien, auch als Tracker oder nur als Torrent bezeichnet, sind kleine Dateien, die verfolgen, wo eine Datei sich innerhalb eines Netzwerkes von verschiedenen Computern befindet, damit diese heruntergeladen werden kann.

Mit einer speziellen Software, einem Torrent-Client wie BitTorrent, werden die Uploader und Downloader dieser Datei miteinander verbunden. Über die Torrent-Datei wird entschieden, welche Dateien freigegeben werden sollen.

Der Nutzer, der eine Datei herunterladen will, wird so mit mehreren Personen verbunden, die diese Datei hochladen. Dadurch kann er sich die gewünschte Datei in vielen Einzelteilen herunterladen und so die Downloadgeschwindigkeit erhöhen. Anschließend setzt der Torrent-Client die Datei aus den Bruchteilen wieder zusammen.

Torrenting wird so zum kostenlosen Datenaustausch über das Internet verwendet. Während das Austauschen von Daten zwischen Nutzern auf diese Weise nicht illegal ist, kommt es oft zu Urheberrechtsverletzungen. So zum Beispiel auch bei den vom Hidden Service The Pirate Bay zur Verfügung gestellten torrent Dateien.

Auf der Webseite gibt es die Kategorien All, Audio, Video, Applications (deutsch: Anwendungen), Games (deutsch: Spiele), Porn und Other. Außerdem gibt es auch Übersichten zu den zuletzt aufgerufenen Torrents und den Top 100 Torrents.

Zusätzlich bietet der Hidden Service ein dazugehöriges Forum mit dem Namen SuprBay an. In diesem wird unter anderem die Plattform selbst diskutiert, aber auch die verschiedenen Kategorien und Medienarten, die auf der Plattform zur Verfügung stehen. In einem Bereich gibt es die Möglichkeiten Malware, falsch kategorisierte Torrents sowie kinderpornographische Inhalte zu melden. Um sich die Posts im Forum anzusehen, muss man sich anmelden.

4.3.3 Foren

Foren gibt es im Dark Web nicht nur im Zusammenhang mit anderen Hidden Services, sondern auch unabhängig davon als selbstständige Hidden Services. Genau wie im Clear Web gibt es verschiedene Foren zu verschiedenen Themen. Jedoch ist der Themenbereich weniger breit gefächert.

Die meisten Foren sind in englischer Sprache, nur wenige sind nicht-englischsprachig.

Der Aufbau ist oft gleich wie bei Foren im Clear Web. Es gibt verschiedene Bereiche, oftmals unterteilt nach Thematik. In diesen Bereichen können Nutzer sogenannte Themen erstellen, auf die andere Nutzer wiederum antworten können. In manchen Foren können die Beiträge der Nutzer zusätzlich entweder positiv oder negativ bewertet werden. Ähnlich wie bei der Clear Web Plattform Reddit.

Als Nutzer kann man das Forum entweder als Gast besuchen oder durch Registrieren zum Mitglied werden. Oft können nur Mitglieder Themen erstellen oder auf Beiträge antworten. Teilweise kann das Forum sogar nur dann eingesehen werden, wenn man ein registriertes Mitglied ist. In diesen Fällen kostet die Mitgliedschaft meist entweder Geld oder man kann nur zu einem Mitglied werden, wenn man explizit von einem anderen Mitglied oder dem Administrator des Forums eingeladen wird. Die Beitrittsgebühren belaufen sich meist auf einen Betrag zwischen fünf und 250 US-Dollar. Das Forum DarkNetForum bietet zum Beispiel für fünf Dollar eine Basis Mitgliedschaft an und für fünfzig Dollar eine volle Mitgliedschaft mit komplettem Zugriff auf alle Bereiche des Forums [97].

Besonders häufig sind Formen zu den Themen Marktplätze, Produkte und Rezensionen. Hier tauschen sich die Mitglieder und Gäste über Dark Web Märkte, deren Verkäufer und die angebotenen Produkte aus. Es werden Empfehlungen ausgesprochen und Fragen gestellt oder von Verkäufern oder Produkten abgeraten.

Einige Foren weisen darauf hin, dass illegale Inhalte nicht erwünscht sind. Beispielsweise das deutsche Forum “Freies Forum”, welches sich jedoch noch im Aufbau befindet und nur wenige Mitglieder und Beiträge hat.

Auch ein weiteres deutsche Forum, das “Germania Forum”, mit 1856 Mitgliedern weist in den Forenregel darauf hin, dass bestimmte Dinge verboten sind. Konkret heißt es: “Keine scharfe Schusswaffen, Auftragsmord, Suizid, Terrorismus etc. Kein CP, nichts mit Kindern, Frauen oder Tiere!” [98]. Die Abkürzung CP steht in diesem Fall für Child Pornography, also kinderpornografische Inhalte. Ein Ausschnitt der Forenseite ist in Abbildung 4.13 zu sehen.

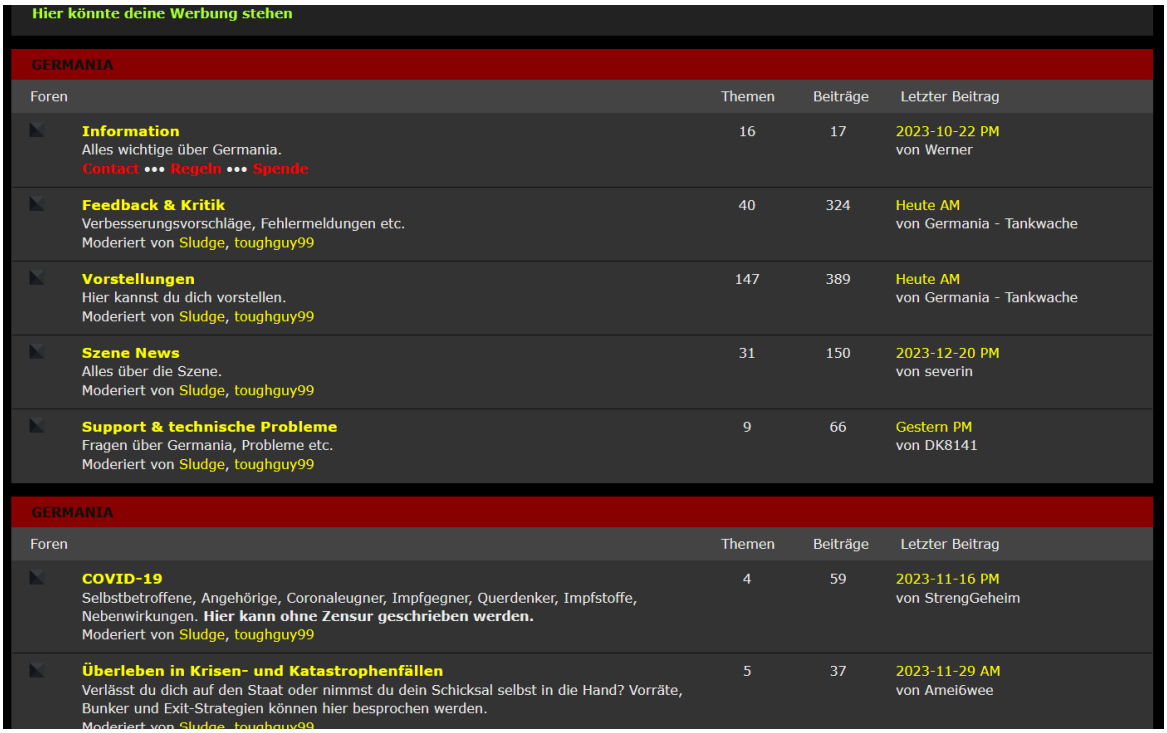

Abbildung 4.13: Forum Germania [98]

Ein Beispiel für ein deutsches Forum, in dem illegale Inhalte stattfanden, war das Forum mit dem Namen Deutschland im Deep Web. Es handelte sich mit über 23000 Mitgliedern um das größte deutschsprachige Forum im Dark Web. Das Forum war bis zur Beschlagnahmung im Oktober 2022 aktiv. Neben der Nutzung für legale Gespräche über unter anderem Politik, IT-Sicherheit und Anonymisierung wurde das Forum auch für den Verkauf von Waffen und Drogen genutzt. Zudem auch für kriminelle Aufträge und den Austausch von Anleitungen zu Hacking und Fälschung. Unter anderem der Täter des Amoklaufs in München 2016 erwarb seine Waffe über dieses Forum [99]. [100]

2017 wurde das Forum zum ersten Mal beschlagnahmt und der Administrator Alexander U. verhaftet. Danach gab es mehrmals Nachfolge-Versionen des Forums, die immer wieder aus verschiedenen Gründen offline gingen. Bis 2022 erneut ein Administrator verhaftet wurde. Seitdem führen Onion-Links zum Hidden Service auf eine Webseite mit einem Banner des BKA, welches die Beschlagnahmung des Forums verkündet (siehe Abbildung 4.14). [100]

Auch in vielen englischsprachigen Foren wird offen über den Verkauf und den Konsum von Drogen oder den Besitz von Waffen geredet. Hilfe und Anleitungen für illegale Aktivitäten wie Hacking oder das Fälschen und Kopieren von Kreditkarten werden auch dort angeboten.

Der Umgangston in den Foren ist oft weniger höflich und hilfsbereit als es bei einigen Clear Web Foren der Fall ist. Oft bleiben Beiträge oder Fragen auch unbeantwortet. Auf Rechtschreibung und Grammatik, sowie Zeichensetzung wird selten geachtet.

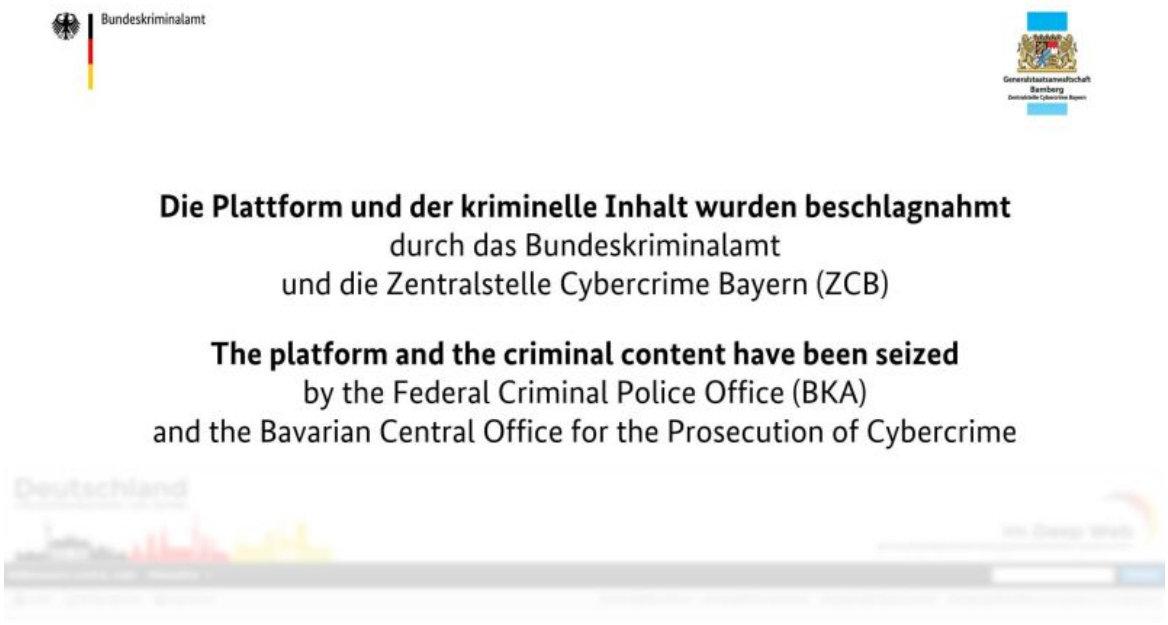

Abbildung 4.14: Bundeskriminalamt Banner auf dem Hidden Service Deutschland im Deep Web [100]

Dies ist besonders der Fall bei einer speziellen Art der Foren, den sogenannten Chans. Dabei handelt es sich um Imageboards (zu Deutsch Bilderbrett), auf denen anonym Texte und auch Bilder ausgetauscht werden. Es besteht keine Möglichkeit, ein Nutzerkonto anzulegen. Der bekannteste Vertreter dieser Art des Internetforums ist das im Clear Web verfügbare 4chan.

Die Unterforen der chans werden als Boards bezeichnet. Innerhalb der Boards können Nutzer Threads erstellen. Dies sind Diskussionsstränge, die mit einem Post beginnen, auf welchen mit weiteren Posts geantwortet wird.

Die Ursprünge der Chans kommen aus der Otaku Subkultur. Dabei handelt es sich um eine Subkultur von japanischen Fans. Das Wort hat eine ähnliche Bedeutung wie beispielsweise Nerd im Englischen. Chans sind dafür bekannt, im Umgangston besonders unfreundlich zu sein. Cybermobbing, gezielte Provokationen, Extremismus, pornografische Inhalte sowie Rassismus und Sexismus stehen an der Tagesordnung. [101, 102]

Im Dark Web gibt es mehrere solcher Chans. Zum Beispiel 8chan und Endchan. Beide weisen die typischen Merkmale dieser Foren-Art auf. Es gibt viel Pornografie, die zumindest bei Endchan mit einer Option ausgeblendet bzw. eingeblendet werden kann. Die Kommunikation findet zum Großteil auf Englisch, aber auch teilweise in anderen Sprachen statt. Der Betreiber des Hidden Services erlaubt alles, was in den Gesetzen der USA nicht verboten ist. Häufig werden Schimpfwörter oder Beleidigungen benutzt, ebenso wie Rassismus und Antisemitismus. [103]

Für Außenstehende sind die Posts in den Threads oft unverständlich, auch aufgrund von sehr vielen verwendeten Slangworten. Zusammenhänge lassen sich nur schwer erkennen und das Folgen des Gespräches fällt schwer.

Über die Boards ist das Forum in verschiedene Kategorien eingeteilt. Diese umfassen viele verschiedene Themen von “Science And Technology”, “Anime And Manga”, “Argentina”, “Crypto-Anarchism” und “Politically Incorrect” oder “Random” bis hin zu “Autism” und “World of Equestria”. Manche der Boards tragen unverständliche Bezeichnungen, durch die nicht sofort ersichtlich wird, worum es geht, auch wenn zu jedem Board eine kurze Beschreibung angegeben ist. Diese ist jedoch nicht immer aussagekräftig. Ein Ausschnitt der Übersicht über die Boards ist in Abbildung 4.15 zu sehen.

Boards on endchan

Board	Description	PPH*	Total Posts**	Users***	Tags
/polru/ - pol - Russian Edition ☆	А у нас всё по-прежнему	37	383494	91	
/agatha2/ - E-Girl Purgatory ☆	e-girl gossip & drama	8	43787	63	agatha, ciara, marky, orbiting, 3d waifus
/bb/ - b+ ☆	Наркач	10	110483	31	
/ausneets/ - AusNEETs ☆	The bored four NEETs	5	791968	29	
/rus/ - Russian ☆	На дереве почки, под ними грибочки, поставим тут точку или новую строчку?	1	28222	22	russian, random, русскоязычный, рандом
/baaa2/ - Autism ☆	Dunking on the mentally ill	3	21000	18	
/dota/ - Dota 2 ☆	Тред друзей и старых знакомых	13	65106	16	
/genshin/ - Товарищеское Издание ☆	Genshin и общение на любые темы	2	12244	10	
/b/ - Random ☆	Anything posted here are autistic works of fiction, only a fool would take them seriously.	2	49211	9	

Abbildung 4.15: Ausschnitt aus Boardübersicht des Forums Endchan [103]

Neben der Forenart der Chans gibt es auch Foren, die sich speziell mit bestimmten Hidden Services und dabei am meisten mit Dark Web Marktplätzen beschäftigen. So zum Beispiel das NZ Darknet Market Forum.

Das Forum ist unterteilt in Unterforen. General discussion behandelt die allgemeine Nutzung von Dark Web Marktplätzen, Kryptowährungen, Tor, VPNs und Verschlüsselung. Das Unterforum Product Sourcing beinhaltet Anfragen und Suchen nach bestimmten Produkten. Im Unterforum Product reviews werden detaillierte Rezensionen von Produkten und Händlern geteilt. Nachrichten und Updates zu Verkäufern werden im Bereich Vendor Updates veröffentlicht. [104]

4.3.4 Services im Zusammenhang mit Kryptowährung

Krypto-Mixer, auch Tumbler genannt, sind Dienstleister, die Transaktionen mit Kryptowährungen anonymisieren, indem sie die Ströme der Währungen mischen.

Genauer gesagt werden die Gelder der Kunden in kleinere Summen aufgeteilt und mit anderen Transaktionen von anderen Kunden vermischt. Anschließend erhält der Kunde Kryptowährung im gleichen Wert, aber aus unterschiedlichen Coins bestehend zurück. Oft wird für diesen Prozess eine gewisse Gebühr verlangt. [105]

Der Wunsch nach Anonymisierung stammt daher, dass eine Blockchain alle Transaktionen mit Kryptowährungen speichert. Zugang zum Wallet, der digitalen Börse, einer Person ermöglicht es also, Auskünfte über vergangene Transaktionen zu erhalten. [106]

Krypto-Mixer, oft auch als BitCoin Mixer bezeichnet, gibt es nicht nur im Dark Web. Einige Webseiten bieten ihre Services jedoch sowohl im Clear- als auch im Dark Web an und empfehlen ihren Nutzern die Verwendung des Tor-Browsers für zusätzliche Anonymität.

Mixer, die im Clear Web zugänglich sind, sind beispielsweise CryptoMixer, Mixer.money, UniJoin, Mixer, Coinomize oder MixBTC. Sowohl UniJoin und Coinomize als auch Mixer.money bieten ihre Dienste auch als Hidden Service an.

Zusätzlich gibt es auch einige Hidden Services, die ausschließlich im Dark Web angeboten werden. Unter anderem Dark Mixer, Mixabit, Pay Shield und Helix bzw. Helix Light. Die Abbildung 4.16 zeigt beispielhaft die Webseite des Hidden Service Helix Light.

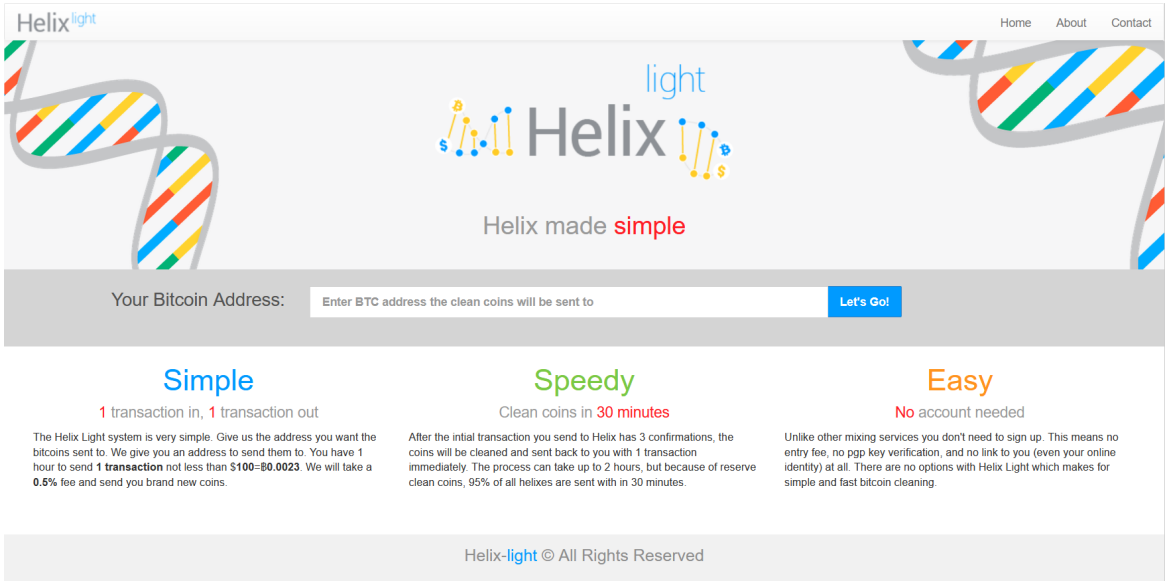

Abbildung 4.16: Bitcoin-Mixer Helix Light [107]

Die Gebühren der Services sind unterschiedlich und werden meist als Anteile des gemischten Geldes verlangt. Diese bewegen sich oft zwischen 0,5% und 5%, teilweise mit zusätzlichen festen Gebühren. Manche Hidden Services fordern eine Mindestsumme für das Nutzen ihrer Dienste. Coinomize verlangt unterschiedliche Anteile, je nach Stärke des Mischens. Von 1,5% bis 5% [108]

Neben Krypto-Mixern gibt es im Dark Web auch Hidden Services, die Wallets, also digitale Geldbörsen, für Kryptowährung anbieten. Diese Wallets, auch als Cyberwallets bezeichnet, geben den Nutzern die Möglichkeit, digitale Währungen wie zum Beispiel Bitcoin oder Monero auf elektronischen Plattformen zu speichern, indem sie private und/oder öffentliche Schlüssel zu Transaktionen mit Kryptowährungen hinterlegen. So kann das Guthaben der entsprechenden Währung versendet und verwaltet sowie neue Kryptowährung empfangen werden.

Die Wallets können jeweils nur für eine bestimmte Kryptowährung genutzt werden. Die meisten im Dark Web angebotenen Wallets sind Wallets für Bitcoins. Ein Beispiel für ein Wallet, das für eine andere Währung verwendet wird, ist der Hidden Service Feather Monero Wallet. Dieser, sowie der Hidden Service Wasabi Wallet sind auch im Clear Web verfügbar.

Andere Hidden Services bieten ihre Wallets hingegen nur im Dark Web an. So zum Beispiel EasyCoin und OnionWallet. Diese beiden enthalten einen integrierten Bitcoin Mixer und werben offen mit der Möglichkeit, diesen zum "Waschen" von Bitcoins zu benutzen. [109, 110]

Andere Services im Dark Web bieten beispielsweise an, Bitcoins zu kaufen oder zu verkaufen. Dazu zählt der Hidden Service WeBuyBitcoins. Ein weiterer Hidden Service mit dem Namen Bitcoin Investment Trust verspricht Nutzern, von ihnen hinterlegte bzw. geliehene Bitcoins zu investieren und dadurch Profit von fünf bis neun Prozent pro Woche zu erreichen [111].

Kryptowährungen, insbesondere Bitcoin, sind im Dark Web die am meisten genutzte Zahlungsmittel. Kaum ein Hidden Service nimmt andere Zahlungsmittel an, da Kryptowährungen den klaren Vorteil der erhöhten Anonymität bringen. Die Verwendung von Wallets zur Verwaltung dieser Zahlungsmittel ist also für Nutzer, die das Dark Web für Transaktionen nutzen, von besonderer Wichtigkeit.

Viele Anbieter von Wallets oder Krypto-Mixern werben mit der einfachen Nutzung, den niedrigen Gebühren oder damit der einzige sichere bzw. wirklich anonyme Service zu sein. Oft wird anderen Anbietern unterstellt, Daten weiter zu verkaufen, oder sich nicht genug um die Privatsphäre und Sicherheit der Kunden zu kümmern.

4.4 Illegale Inhalte

Über das Dark Web gibt es viele Vorstellungen und Vorurteile. Oft wird es als ein Ort angesehen, den nur Kriminelle aufsuchen, um sich zu Straftaten zu verabreden, kinderpornografische Inhalte anzusehen und zu teilen oder Drogen und Waffen zu handeln.

Während die vorherigen Kapitel zeigen, dass es im Dark Web durchaus auch viele verschiedene legale Webseiten und Services gibt, treffen die beschriebenen Vorstellungen doch zumindest teilweise zu.

Als Ort, der für anonyme Kommunikation und die Stärkung von IT-Sicherheit und Privatsphäre gegründet wurde, bietet das Dark Web gute Voraussetzungen für Nutzer, die ihre Aktivitäten verschleiern wollen. Durch die Verwendung von mehreren Relays ist es nicht möglich, über Anfragen an beispielsweise Internetprovider die Handlungen eines Tor-Nutzers im Netz zu verfolgen.

Transaktionen erlangen durch das Verwenden von Kryptowährungen, oft auch zusammen mit sogenannten Mixern, eine große Anonymität. Händler und Käufer agieren unter dem Deckmantel von Pseudonymen.

All dies sind Vorteile, die das Dark Web gegenüber dem Clear Web bietet, wenn es um das Durchführen von illegalen Handlungen geht.

Es ist davon auszugehen, dass den Akteuren die mangelnde Legalität ihrer Aktionen durchaus bewusst ist. Oft wird besonders vorsichtig vorgegangen und es werden mehrere Maßnahmen ergriffen, um die eigene Identität zu schützen. Dennoch gelingt es Behörden immer wieder, einzelne Personen, wie zum Beispiel Administratoren von Marktplätzen oder Händler von illegalen Waren zu identifizieren [1, 3]. Auch im Dark Web ist Kriminalität nicht risikofrei.

4.4.1 Finanzielle Services

In einigen Verzeichnissen, die Onion-Links zu verschiedenen Hidden Services anbieten, findet sich eine Kategorie mit dem Namen “Financial Services”, zu Deutsch “finanzielle Services”. Neben bereits erwähnten Diensten wie Wallets und Mixer für Kryptowährungen zählen zu dieser Kategorie vor allem Hidden Services, auf denen gefälschte, gestohlene oder durch Hacken erlangte Produkte angeboten werden, die sofortige Geldwerte versprechen.

Eines der meist angebotenen Produkte sind gefälschte oder geklaute Kreditkarten, sogenannte Counterfeit Cards. Hierbei kann unterschieden werden in Anbieter, die physische Karten verkaufen und solche, die lediglich die Daten der Karten verkaufen.

Physische Karten sind oft Kopien von Kreditkarten, deren Besitzer Opfer von Techniken wie Skimming, Phishing oder Social Engineering geworden sind.

Skimming, auf Deutsch auch Abschöpfen, ist eine Angriffsart, bei der Täter Daten aus den Magnetstreifen von EC- oder Kreditkarten auslesen. Für dieses Vorgehen werden oft manipulierte Geldautomaten genutzt, die von den Tätern präpariert wurden. Mit Hilfe einer versteckten Kamera kann zur gleichen Zeit auch die PIN-Eingabe abgefilmt werden, um diesen später zu verwenden. [112, 113]

In Deutschland sind die Fälle von Skimming durch manipulierte Geldautomaten und der so entstehende Geldschaden in den letzten Jahren zurückgegangen. Grund dafür ist die Verstärkung der Sicherheitsmaßnahmen. [114] Trotzdem geht von dieser Vorgehnsweise immernoch eine Gefahr aus.

Kreditkartendaten können aber ebenfalls durch gezielte Hacking Angriffe erhalten werden. So werden die Opfer beispielsweise mit Hilfe von Phishing und dem gezielten Nachbauen von Webseiten dazu gebracht, ihre Kreditkartendaten auf vom Täter kontrollierten Webseiten anzugeben.

Auch Social Engineering Attacken können darauf ausgelegt sein, diese Informationen zu erfahren. So wird zum Beispiel dem Opfer durch Kontakt per E-Mail und Telefon suggeriert, man sei ein Bankangestellter. Besonders ältere Menschen werden so dazu verleitet ihre sensiblen Daten und PINs weiterzugeben. [115]

Eine andere Variante findet vor Ort an einem Geldautomaten statt. Dort wird das Opfer bei der PIN-Eingabe beobachtet und anschließend die EC- oder Kreditkarte entwendet. Später werden die erlangten Daten der Bankkarten dann auf dafür hergestellte Kartenrohlinge kopiert. Diese können danach an Geldautomaten verwendet werden oder um online Transaktionen mit ihnen durchzuführen.

Auf vielen Hidden Services im Dark Web werden genau solche Produkte zum Verkauf angeboten. Dass die Händler die gestohlenen Daten und Karten nicht selbst verwenden, begründen sie oft mit der Notwendigkeit, nicht aufzufallen. Denn wer gestohlene Kreditkarten verwendet, riskiert beim Geld abheben von Kameras aufgezeichnet zu werden. So kann der Täter unter Umständen später identifiziert werden, wenn das Opfer den Schaden bemerkt und meldet.

Die Karten werden für einen Preis verkauft, der deutlich unter dem Kreditlimit der jeweiligen Kreditkarte liegt. Je nach Händler und Angaben kann ein Kunde so Produkte zum Wert vom bis zu 333-fachen des Verkaufspreises erhalten. Ein Hidden Service mit dem Namen Cardshop bietet für den Preis von neunzig US-Dollar zehn Karten belastbar mit 1000 bis 5000 US-Dollar [116].

Der Hidden Service Imperial Market (siehe Abbildung 4.17) bietet für den gleichen Preis eine Kreditkarte mit einem Kredit von 3200$ an. Außerdem gibt er an, dass die gekauften Karten für nur 30 Tage nach dem ersten Benutzen genutzt werden können. Es wird deshalb empfohlen in dieser Zeit den kompletten Betrag abzuheben. Imperial Market wirbt ebenfalls damit, zu jeder Karte den PIN sowie eine Anleitung zur Benutzung mitzuliefern. [117]

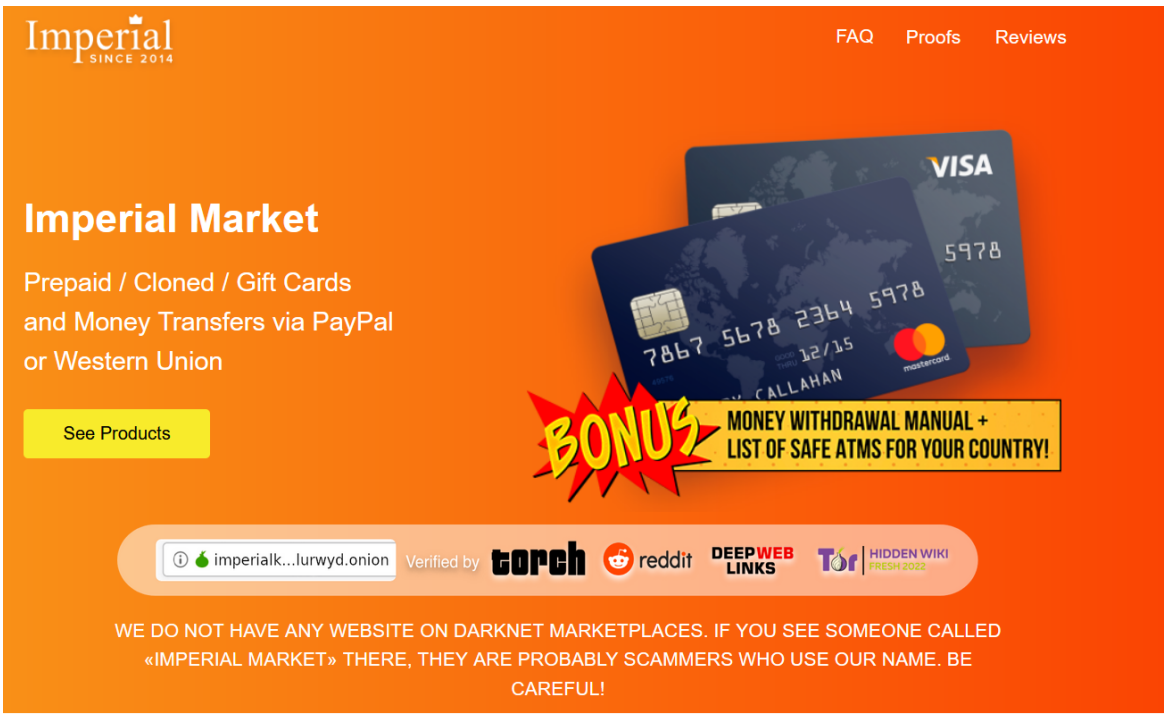

Abbildung 4.17: Hidden Service Imperial Market [117]

Ein weiteres Angebot dieser Art von Hidden Services sind Prepaid Cards. Dabei handelt es sich um Karten, die keinem bereits existierenden Bankkonto zugeordnet sind. Stattdessen werden sie mit einem bestimmten Geldbetrag aufgeladen. So können sie anonym verwendet werden.

Viele Händler geben an, das Geld, mit dem die Karten aufgeladen wurden, beispielsweise durch das Nutzen von kopierten bzw. geklauten Kreditkarten erhalten zu haben. Die Karten werden in physischer Form zusammen mit der dazugehörigen PIN verkauft.

Auch hier variieren die Preise. Der Hidden Service BitCards verkauft eine Prepaid Visa Classic Karte mit einem Guthaben zwischen 2500$ und 2800$ für 95$. Beim Erwerben von mehreren Karten auf einmal erhält man Mengenrabatt. [118] Der bereits erwähnte Hidden Service Imperial Market verkauft eine Visa Prepaid Karte mit einem Guthaben von 3100$ für einen Preis von 110$ [117].

Neben Kreditkarten werden auch Gutscheine, im Englischen Gift Cards genannt, verkauft. Dabei handelt es sich oft um verbreitete Anbieter wie Amazon oder Ebay. Aber auch Gutscheine für Visa, Steam, Asos, iTunes, Google Play, GameStop, Nike oder Walmart werden angeboten.

Der Hidden Service Fish'n'Pal verlangt für einen 100$ Amazon- oder Ebay Gutschein einen Preis von 25$ [119]. Ein anderer Anbieter, Light Money, verkauft 500$ Amazon- und Ebay Gutscheine zu einem Preis von 60$ [120].

Gehackte PayPal-Accounts, seltener auch Ebay-Accounts, werden ebenfalls oft zum Verkauf angeboten. Hier werden die Zugangsdaten verkauft. Manche Hidden Services bieten auch den direkten Transfer von Geld auf einen sich bereits im Besitz des Kunden befindenden PayPal Account an.

Preise befinden sich in einem ähnlichen Rahmen wie bei den Kreditkarten. Die Seite Krypto-PayPal verkauft Accounts zu einer Profitrate zwischen 22% und 25% [121]. Millionair Private Club bietet einen "PayPal Transfer" von 750$ für einen Preis 35$ [122]. Light Money verlangt für einen 800$ PayPal Transfer einen Betrag von 65$ [120]. Fish'n'Pal verlangt Preise zwischen zehn und dreizehn Prozent des versprochenen Wertes des Accounts [119]. AccMarket bietet zu einem Preis von 150$ zehn PayPal Accounts mit jeweils 250$ bis 500$ Guthaben an [123].

Neben digitalen Produkten wie Zugangsdaten zu Paypal-Accounts, Kreditkartendaten oder Gutscheincodes wird im Dark Web auch Bargeld zum Kauf angeboten.

Dabei handelt es sich um Falschgeld oder um Bargeld, das aufgrund von Mängeln wie Verschmutzung vernichtet werden sollte, aber auf diesem Weg abgefangen wurde.

Händler geben an, Kontakte zu haben, die dieses sogenannte Pre-Shred Cash abschöpfen und ihnen zuführen. Jedoch nur kleinere Mengen auf einmal, um nicht aufzufallen. Außerdem schreiben die Händler, dass sie nicht ohne Risiko größere Mengen dieses Geldes ausgeben können. Laut eigener Aussage verkaufen sie es deswegen für Bitcoins im Dark Web. [124]

Die Verkäufer geben des Weiteren an, dass den Käufer kein Risiko trifft, da der Verbleib des Geldes und die Seriennummern nicht bekannt wären und es nicht illegal sei, Bargeld zu kaufen. Es wirkt jedoch nicht legal Bargeld zu erwerben, dessen Erhalt zuvor als kriminell beschrieben wurde. [124]

Mehrere Hidden Services geben dieselben Informationen zu ihrem Vorgehen an. Teilweise scheinen die Texte voneinander kopiert bzw. übernommen. Es wirkt unwahrscheinlich, dass mehrere Gruppen auf dieselbe Art operieren. Doch auch im Clear Web gibt es Webseiten, deren Betreiber angeblich Pre-Shred Cash verkaufen. Zum Beispiel die Seite The Notes King [125].

Der Hidden Service Dark Web Wolf Street bietet drei verschiedene Pakete für je 360$, 1000$ und 3600$ an [124]. Der Hidden Services Mike's Grand Store bietet 500 Dollar Scheine für einen Preis von 99$ an, gibt jedoch nicht an, wie viele Scheine in diesem Preis enthalten sind [126].

Neben diesem echten, aber aus dem Zahlungsverkehr gezogenen Geld bieten einige Hidden Services auch Falschgeld an, im Englischen Counterfeit Bills genannt.

Es werden verschiedene Währungen angeboten, vor allem US-Dollar und Euros. Die Seiten Counterfeit USD und HQER scheinen zusammen zu gehören und verkaufen die jeweils erwähnte Währung zu ähnlichen Konditionen. Für 25 50-Euro-Scheine wird ein Preis von 275€ verlangt. Für 25 50-Dollar-Scheine muss ein Kunde 325$ bezahlen. [127, 128]

Beide Hidden Services geben an, dass ihre Scheine aus Baumwollpapier bestehen und alle Sicherheitsmerkmale erfüllen, um bei den meisten Geschäften verwendet werden zu können. So sollen beispielsweise der Test mit UV-Licht und einem Geldscheinprüfstift ohne Probleme bestanden werden. [127, 128]

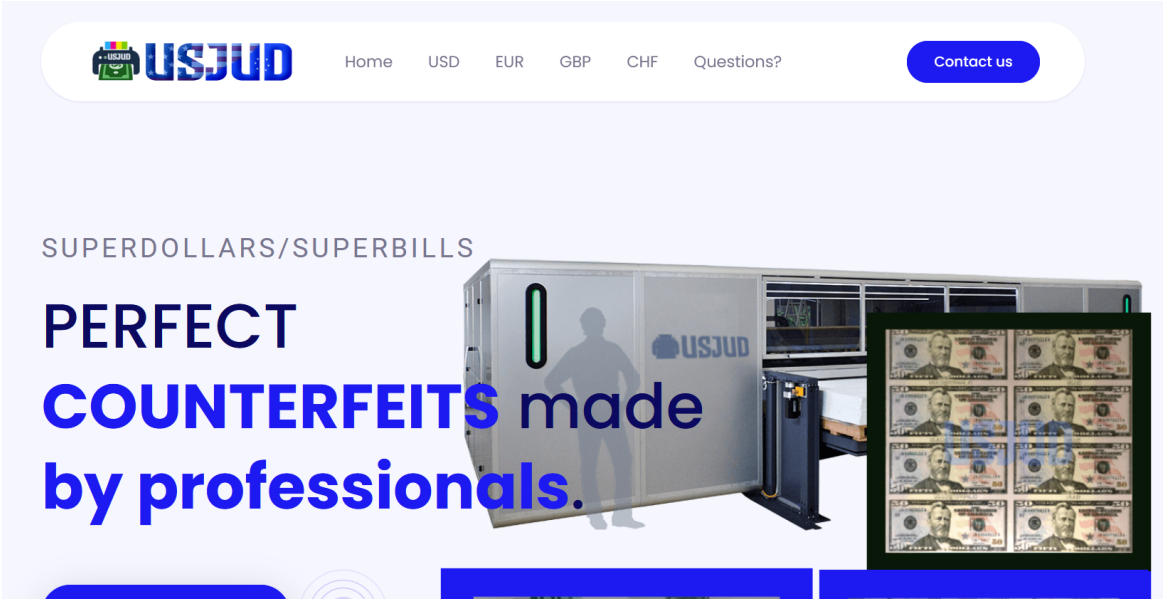

Abbildung 4.18: Hidden Service USJUD

Der Hidden Service mit dem Namen USJUD bietet Falschgeld in vier verschiedenen Währungen an. US-Dollar, Euro, Britische Pfund und Schweizer Franken. Auch dieser Service gibt an, dass die Geldscheine zu 99% nicht als Falschgeld entdeckt werden. Die Webseite wirkt deutlich professioneller als die zuvor betrachteten Hidden Services. Ein Ausschnitt der Seite ist in Abbildung 4.18 zu sehen. [129]

Der Service hat einen Mindestbestellwert von 250$ und bietet dafür sogenannte Sample Pakete, im Deutschen auch Probe- oder Probierpakete, an. Für einen Preis von 250$ erhält der Kunde ein Paket mit fünf 100-Euro-Scheinen, fünf 50-Euro-Scheinen und fünf 20-Euro-Scheinen. Alternative Angebote sind acht 50-Euro-Scheine und acht 20-Euro-Scheine zu einem Preis von 200$ oder ein Paket, das zu einem Preis von 480$ verkauft wird und jeweils zehn 20-, 50- und 100-Euro-Scheine enthält. [129]

Der Hidden Service akzeptiert wie einige weitere Hidden Services im Dark Web die Bezahlung über einen Escrow Service. Damit ist ein Service gemeint, der bei einer Transaktion als dritte Partei zwischen dem Verkäufer und dem Käufer vermittelt. So wird das Risiko des Betruges minimiert und die Zufriedenheit beider Seiten sichergestellt.

Wenn ein Käufer bei einem Händler einen Kauf über das Escrow Verfahren tätigen will, sendet er zunächst die benötigte Summe an den Escrow Service. Dieser bewahrt das Geld auf. Dann schickt der Verkäufer das Produkt zum Kunden. Empfängt der Käufer sein Produkt und hat keine Mängel zu beanstanden, so gibt er dem Escrow Service sein Einverständnis und der Service sendet das Geld weiter an den Verkäufer.

Sollte eine der beiden Seiten, entweder der Verkäufer oder der Kunde, nicht mit der Transaktion zufrieden sein, versucht der Escrow Service zwischen den Parteien zu vermitteln. Dazu verlangt er zum Beispiel weitere Nachweise über den Eingang der Sendung oder die Mängel des Produkts. Wenn der Konflikt gelöst wurde, sendet der Escrow Service das hinterlegte Geld danach entweder zurück an den Käufer oder weiter an den Händler.

Auf diese Weise werden sowohl der Käufer, der sein Geld erst freigibt, wenn er das Produkt tatsächlich erhalten hat als auch der Verkäufer geschützt. Denn dieser erhält durch das Einzahlen der Summe an den Escrow Service die Bestätigung, dass der Käufer tatsächlich zahlungsfähig ist.

Besonders im Dark Web ist so ein Service wichtig, um das Vertrauen der Kunden zu erhöhen. Denn oft besteht das Risiko, auf einen Betrug hereinzufallen. Wenn man Geld an den Betreiber eines Hidden Service bzw. einen Händler schickt und anschließend nicht die gewünschte Ware erhält, so gibt es kaum Möglichkeiten etwas dagegen zu unternehmen. Da beide Parteien durch das Tor-Netzwerk anonym bleiben, ist es nicht möglich, die Identität des Verkäufers zu ermitteln.

Außerdem handelt es sich bei vielen Transaktionen im Dark Web um illegale Güter, wodurch das Stellen einer Strafanzeige nicht möglich ist, ohne sich selbst zu belasten.

Um einen Betrug zu erkennen, hilft häufig nur das Hinterfragen der angebotenen Services und die Suche nach Rezensionen zum Anbieter. Auch die Gestaltung der Webseite kann Aufschluss liefern. So ist es zum Beispiel eher unwahrscheinlich, dass Betrüger Zeit in die aufwendige Gestaltung einer professionellen Webseite investieren. Rechtschreibfehler und widersprüchliche Angaben hingegen deuten auf verdächtige Aktivitäten hin.

Einige Dienste bieten zudem “Beweise” für ihre Vertrauenswürdigkeit an. Das sind zum Beispiel Produktfotos, auf denen handgeschriebene Zettel mit Daten des Verkäufers zu sehen sind oder Auszüge aus Kommunikation mit zufriedenen Kunden. Auch gibt es Hidden Services, die darauf spezialisiert sind Bewertungen über verschiedene Märkte und Verkäufer verfassen. Insbesondere Märkte, auf denen mehrere Händler ihre Waren verkaufen, sind oft an der Zuverlässigkeit ihrer Anbieter interessiert und überprüfen diese im Vorfeld.

4.4.2 Hitman Dienste

Einer der im Dark Web angebotenen Services, der am wenigsten vertrauenswürdig erscheint, sind sogenannte Hitman Services. Auf den Webseiten dieser Hidden Services bieten Hitmans, zu Deutsch Auftragsmörder, an für den Kunden verschiedene Dienste durchzuführen. Diese Angebote reichen von Körperverletzung, über Freiheitsberaubung oder Sexualdelikte bis hin zu tatsächlichen Auftragsmorden.

Manche Hidden Services stellen sich nur als Vermittlung zwischen Kunden und Auftragsmördern dar, andere geben an, selbst die ausführende Person zu sein. Einige Hitman Services geben an, keine Aufträge anzunehmen, bei denen die Zielperson jünger als 18 bzw. 16 Jahre alt ist. Teilweise werden auch Politiker, bekannte Persönlichkeiten und deren Familien sowie wohlhabende Menschen ausgeschlossen.

Die Preise für die angebotenen Auftragsdaten bewegen sich im Rahmen von 200 $ für Körperverletzung bis hin zu 220.000 $ für Mord. Die meisten Angebote für die Tötung von Menschen befinden sich im Preisraum um 10.000 $ bis 20.000 $. Manche Services machen ihre Preise vom Bekanntheitsgrad und dem Beruf des Zieles abhängig und verlangen zum Beispiel mehr Geld für Polizisten oder Geschäftsmänner.

Es lassen sich keine Nachweise dafür finden, dass die angebotenen Dienstleistungen tatsächlich durchgeführt werden. Viel mehr gibt es immer wieder Zeitungsberichte über Menschen die verhaftet worden, nachdem sie im Dark Web einen Mord in Auftrag gegeben haben [130].

Die Betrugsmasche läuft dabei oft wie folgt ab.

Ein Nutzer kontaktiert den Betreiber eines Hidden Service und gibt einen Mord oder andere Gewaltausübung in Auftrag. Der angebliche Auftragsmörder oder Vermittler nimmt den Auftrag an und verlangt die Vorauszahlung der Summe in Kryptowährung. Anschließend werden weitere Informationen ausgetauscht. Wenn der Zeitpunkt der geplanten Durchführung näherkommt, täuscht der Hidden Service Betreiber plötzlich Komplikationen vor. Der beauftragte Mensch sei beispielsweise von der Polizei kontrolliert und aufgrund von Waffenbesitz verhaftet worden. Nun müsse ein neues Mitglied der Gruppe den Auftrag übernehmen.

Mit jedem dieser “unvorhergesehenen” Zwischenfälle steigt der Preis. Der Kunde wird dazu bewegt, immer mehr Kryptowährung zu zahlen. Bis schließlich eine der beiden Seiten die Kommunikation abbricht. Manche Betreiber dieser Hidden Services geben an anderer Stelle an die Personen, von denen sie kontaktiert werden, der Polizei zu melden.

Ein Fall in dem scheinbar tatsächlich ein Mord über das Dark Web in Auftrag gegeben wurde ereignete sich 2019 in Russland, wo zwei Jugendliche in den Mord einer Polizistin involviert waren. Zuvor hatte der jüngere der beiden auf einem Dark Web Forum nach einem Job gesucht. Daraufhin wurde er von einer Person kontaktiert, die ihm 11000$ für den Mord an der Polizistin Yevgeniya Shishkina bezahlte. [131]

Dieser Fall zeigt jedoch, dass diese Art der Gewalttaten nicht über Hidden Services laufen, die sich auf Hitmans spezialisiert haben, sondern eher im Privaten besprochen werden. Es handelt sich höchstwahrscheinlich um einen Einzelfall.

Das Ziel der Betreiber von Hidden Services, die Auftragstaten anbieten, ist viel mehr durch ihren Betrug Geld zu verdienen. Während manche von ihnen angeben, dass sie die Ressourcen von gefährlichen Personen abfangen wollen und diese darin hindern selbst einen Mord zu verüben, ist dennoch nicht von der Hand zu weisen, dass sie sich daran bereichern. Eine Alternative wäre es, noch vor der Bezahlung die Daten der Auftraggeber an die Polizei weiterzuleiten.

Denn während es sich bei den eigentlichen Hidden Services um verhältnismäßig harmlose Webseiten handelt, die viel mehr auf Betrug als das tatsächliche Verletzen von Menschen angelegt sind, kann von den Auftraggebern durchaus eine reale Gefahr ausgehen.

Dies zeigt sich beispielsweise an einem Fall in Minnesota. Dort hatte ein Mann über das Dark Web für 6000$ einen Mord an seiner Ehefrau in Auftrag gegeben. Auch diese Seite war jedoch nur auf Betrug und das Erhalten von Kryptowährung ausgelegt. Nachdem dieser Auftrag nie durchgeführt wurde tötete der Mann seine Frau einige Zeit später selbst. Anhand seines Computers konnte er anschließend mit dem über das Dark Web gestellten Auftrag in Verbindung gestellt werden. [132]

Dieser Fall zeigt, dass solche Hidden Services auf den ersten Blick zwar leicht als Betrug zu identifizieren sind, sie jedoch trotzdem nicht ignoriert werden sollten. Die Betreiber der Hidden Services erhalten teilweise Informationen die für die Sicherheit der potenziellen Opfer von großer Bedeutung sein können. Die Kommunikation, die über solche Seiten stattfindet, sollte also auch für die Polizei von größerem Interesse sein.

Zuletzt lässt sich anmerken, dass es solche Services nicht nur im Dark Web gibt, sondern auch im Clear Web Webseiten existieren, welche angeblich anbieten für Geld Auftragsmörder anzuheuern.

4.4.3 Dark Web Märkte

Einen der größten Teile des Dark Webs machen sogenannte Märkte bzw. Marktplätze aus, die im Englischen als Marketplace oder Market bezeichnet werden. Hier bieten Verkäufer wie auf herkömmlichen Online Verkaufsplattformen wie Ebay, Amazon oder Etsy Waren und Dienstleistungen an.

Genau wie im Clear Web sind die Marktplätze sehr verschieden. Manche spezialisieren sich auf Produktkategorien wie Drogen oder gefälschte Kreditkarten oder Reisepässe, andere bieten mehrere Kategorien an. Auch der Aufbau und die Funktion unterscheiden sich. Größere Märkte haben oft Systeme, bei denen Verkäufer bewertet werden können und auch Daten angezeigt werden, die angeben, wie lange der Händler schon auf der Plattform aktiv ist und wie viele Käufe bereits bei ihm durchgeführt worden. Je länger der Händler aktiv ist und je mehr Käufe bei ihm stattfanden, desto höher ist in der Regel das Vertrauen der Kunden.

Manche Märkte verlangen außerdem eine Startgebühr von Händlern, die anfangen wollen, ihre Produkte auf diesem Markt zu verkaufen. So sollen potenzielle Betrüger abgehalten werden. Ebenso verlangen die Marktplätze einen bestimmten Anteil des Gewinns.

Marktplätze sind in fast allen Verzeichnissen verlinkt. Bei manchen dieser Hidden Services müssen die Kunden zuerst einen Account anlegen und sich einloggen, um die Plattform zu nutzen und die Produkte zu sehen. So wie viele andere Hidden Services im Dark Web werden auch Marktplätze besonders oft von sogenannten Captchas geschützt. Diese sind in Teilen ähnlich wie Captchas, die im Clear Web verwendet werden, aber oft komplizierter oder anspruchsvoll.

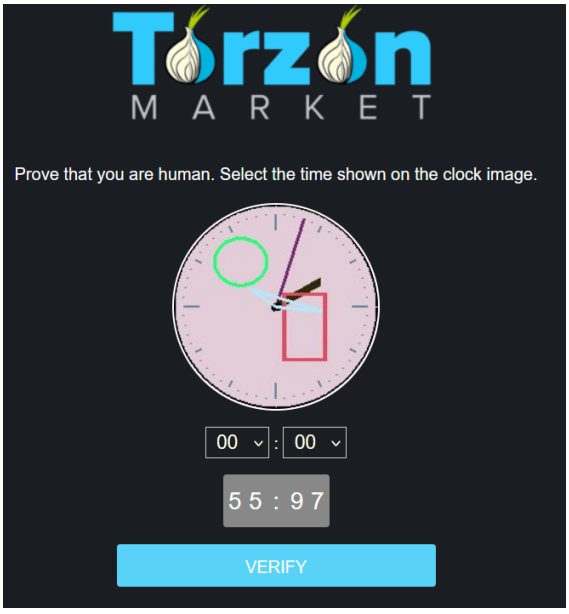

Abbildung 4.19: Captcha auf dem Hidden Service TorZon Market [133]

Es müssen zum Beispiel bestimmte Buchstaben aus der Onion-Adresse des Hidden Services eingegeben und Zahlenreihen vervollständigt werden. Ein anderes Captcha fordert den Nutzer auf innerhalb einer Minute eine Uhrzeit von einem analogen Ziffernblatt abzulesen und als digitale Uhrzeit anzugeben (siehe Abbildung 4.19).

Zum Bezahlen werden bei allen Märkten Kryptowährungen verwendet, besonders häufig Monero und Bitcoin. Manchmal wird nur eine bestimmte Währung akzeptiert. Auf dem Hidden Service Archetyp findet die Bezahlung beispielsweise ausschließlich mit Monero statt. Die meisten Märkte oder Verkäufer bieten das Nutzen eines bereits erwähnten Escrow Service an.

Teilweise gibt es auf den Webseiten FAQ-Bereiche in denen oft gestellte Fragen beantwortet werden. Dort werden auch zusätzliche Informationen und Anleitungen zum Kaufprozess zur Verfügung gestellt.

Manche Händler wickeln ihre Verkäufe nur über E-Mail-Kommunikation ab. Die meisten Hidden Services fordern zum Kauf jedoch das Erstellen eines Benutzer-Accounts und verwenden ein Warenkorb System, wie viele Onlineshops im Clear Web.

Drogen Besonders viele Märkte gibt es in der Kategorie Drogen. Am häufigsten wird hier Cannabis angeboten. Aber auch Dimethyltryptamin (DMT), "Benzos" (Benzodiazepine), Ketamin, Methylendioxymethylamphetamin (MDMA), Kokain, Speed, Lysergsäurediethylamid (LSD), Ecstasy, Oxycodon, Crystal Meth, Steroide, Viagra und Xanax.

Märkte bzw. einzelne Verkäufer, die nur Drogen verkaufen, spezialisieren sich meist auf einige bestimmte Sorten. Oft zeigt sich das auch im Namen des Hidden Services. Einige Beispiele sind DMT Carts, BestBenzos, DeDope, EuCanna oder 420prime. Eine Ansicht des Hidden Service 420prime ist in Abbildung 4.20 zu sehen.

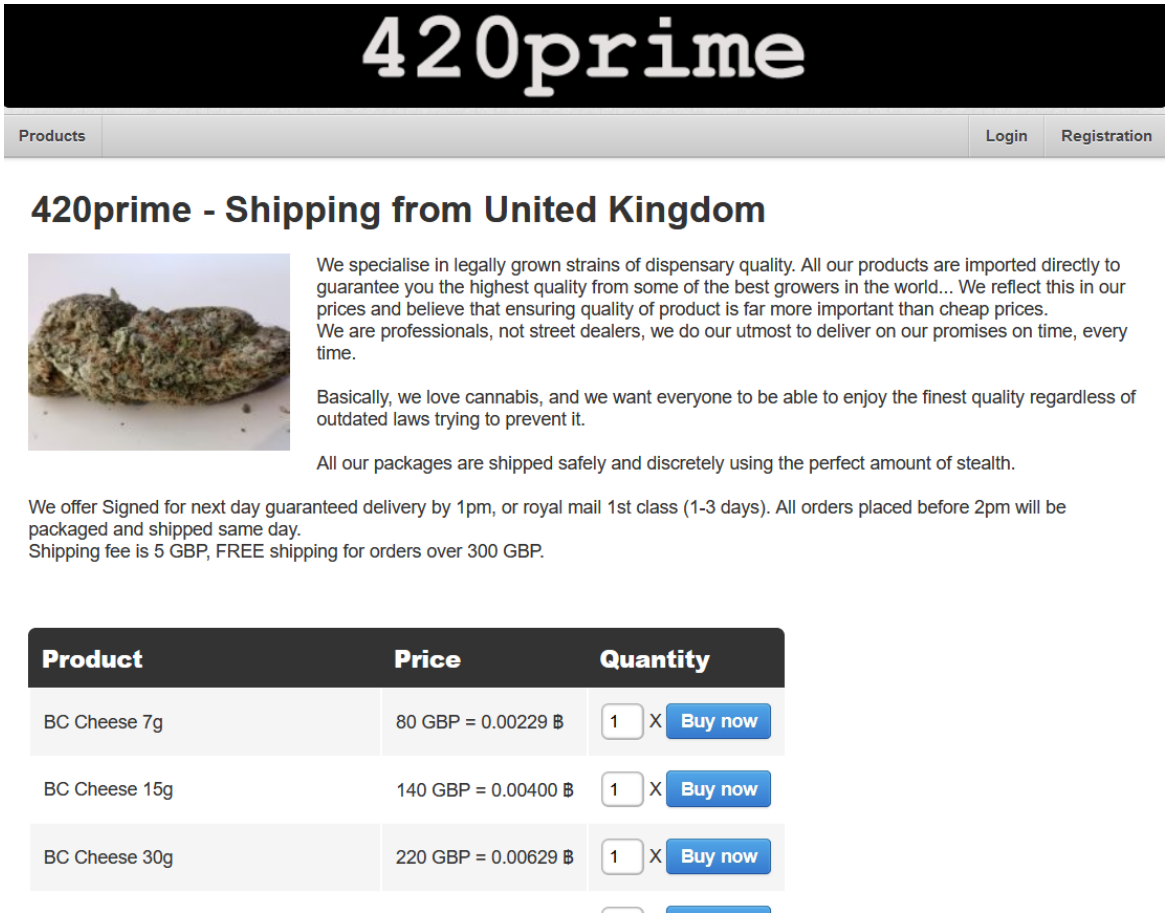

Abbildung 4.20: Hidden Service 420prime [134]

Oft scheinen hinter einem Hidden Service mehrere Personen zu stehen, es wird von der ersten Person Plural gesprochen. Das ist besonders bei Marktplätzen der Fall. Es gibt jedoch auch einige Verkäufer, die ihre Produkte über einen eigenen separaten Hidden Service anbieten.

Auch im Clear Web gibt es Online-Shops, welche Drogen verkaufen [135, 136]. Im Dark Web gibt es jedoch deutlich mehr dieser Services. Die Preise sind oft ähnlich. Cannabis wird sowohl im Clear- als auch im Dark Web für durchschnittlich zehn Euro pro Gramm verkauft. Je größer die gekaufte Menge, desto günstiger wird oft der Grammpreis. [134, 137–140]

Waffen Über das Dark Web werden auch Waffen verkauft. Die zwei Hidden Services Euro-Guns (siehe Abbildung 4.21) und UK Guns & Ammo werden von Verzeichnissen besonders oft verlinkt. Andere Services sind zum Beispiel über Suchmaschinen wie Ahmia zu finden. Im Gegensatz zu anderen Produkten und Dienstleistungen gibt es hier jedoch generell weniger Verkäufer.

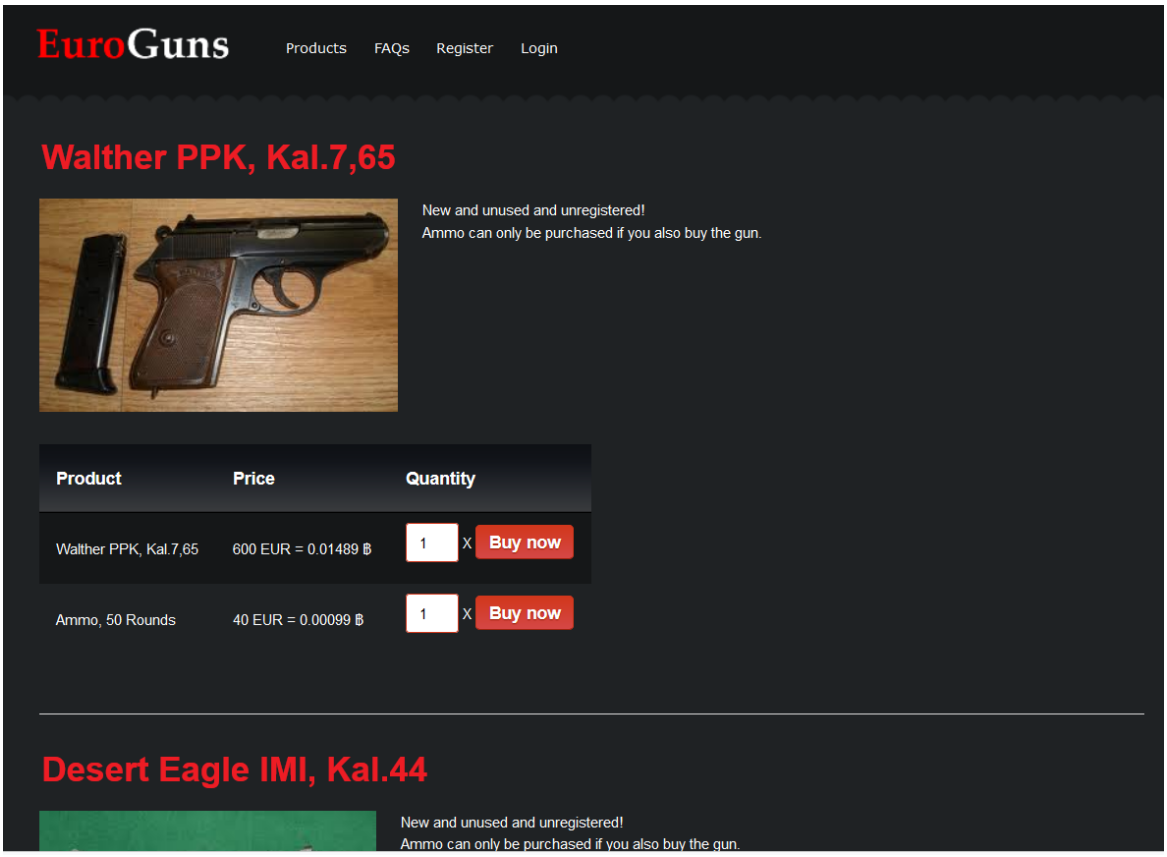

Abbildung 4.21: Hidden Service Euro Guns [141]

Dies lässt sich mit der geringeren Nachfrage begründen, da es sich bei Waffen nicht um konsumierbare Produkte handelt. Bei Drogen besteht häufig eine ständige Nachfrage, während Waffenbesitzer deutlich weniger oft Waffen bestellen. Außerdem sind die Strafen für illegalen Waffenbesitz höher. Zusätzlich ist die Beschaffung von Waffen schwieriger und die Anzahl der Verwendungszwecke geringer. Personen mit den entsprechenden Erlaubnissen können Waffen zudem auch legal offline kaufen und müssen sich dafür nicht ans Dark Web wenden.

Am meisten angeboten werden Handfeuerwaffen. Einige Hidden Services verkaufen auch Shotguns und Rifles Guns. Zusätzlich zu den Waffen kann Munition erworben werden.

Ein Shop wirbt damit, dass die Waffen neu, unbenutzt und nicht registriert sind. Andere Anbieter machen keine Angaben zur Herkunft der Waffen.

Die Preise, die im Dark Web für Handfeuerwaffen verlangt werden, liegen je nach Hidden Service zwischen 300$ und 5500$. Die meisten Anbieter befinden sich in einem Preissegment von 500$ bis 1000$. Offizielle Waffenverkäufer im Clear Web bewegen sich in einem ähnlichen Preisbereich. [141]

Für den Versand zerlegen manche Anbieter ihre Waffen in Einzelteile, um sie in anderen Gegenständen zu verstecken. Zusätzlich werden Anleitungen zum Zusammenbauen mitgeschickt.

Gefälschte Dokumente Im Dark Web werden nicht nur gefälschte Kreditkarten und Falschgeld verkauft, sondern auch gefälschte Dokumente wie beispielsweise Führerscheine oder Reisepässe. Diese Angebote richten sich an Menschen, die sich illegal in Ländern aufhalten oder bei kriminellen Aktivitäten unter einem anderen Namen agieren wollen, um Verfolgung durch Behörden zu vermeiden. Teilweise werden diese Produkte auch angeboten, um auf einfachem Weg die Staatsangehörigkeit eines bestimmten Landes zu erlangen. Da die offiziellen Wege dafür oft lang und aufwändig sind.

Preise unterscheiden sich je nach Land und Anbieter. Bei einem Verkäufer bewegen sich die Preise im Rahmen von 500€ (Brasilien) bis 790€ (USA). Eine andere Seite verkauft Reisepässe von 1250€ (Kanada) bis 1800€ (Großbritannien). An anderen Stellen kosten Reisepässe teilweise deutlich mehr. Der Verkäufer Free Republic bietet sie auf dem Marktplatz Deep Market für 1700$ an. Häufig kosten gefälschte Reisepässe zwischen 1000$ und 2000$. [142]

Führerscheine kosten beim Hidden Service USfakeIDs je 200 US-Dollar. Onion Identity Services verkauft Führerscheine für 500 bis 550€.

Weitere Dokumente, die angeboten werden, sind unter anderem digitale Zertifikate über Covid-19 Impfungen, physische Impfnachweise und ID-Cards. Da für das Bestellen solcher Produkte die eigenen Daten angegeben werden müssen, ist bei diesem Handel ein gewisses Risiko vorhanden. Die Daten könnten beispielsweise auch weiterverkauft und für missbräuchliche Zwecke verwendet werden.

Hacking Neben Waren und physischen Produkten werden auf Dark Web Märkten und von Verkäufern mit eigenem Hidden Service auch Dienstleistungen angeboten. Neben den bereits erwähnten Hitman Diensten handelt es sich dabei zum größten Teil um Angebote im Bereich Hacking.

Es werden unter anderem die folgenden Dienste angeboten: Smartphone Hacking, Computer Hacking, Website/Server Hacking, Social Media Hacking, Email Hacking, Account Recovery, Crypto Recovery, DDoS Attacken, Social Engineering, Location Tracking, University Grades Change, Exploit Selling, Malware Delivery, Reputation Destroying, Vulnerability Assessment, Crypto Tracing und Phishing Attacks.

Auf den entsprechenden Hidden Services werden sehr viele verschiedene Services aufgelistet. Dies liegt an der großen Vielfalt des Bereichs Hacking. Zusätzlich bieten die meisten Seiten auf Anfrage auch weitere personalisierte Services nach Wunsch und Bedarf an.

Einige Webseiten listen nur die Bezeichnungen ihrer Dienste auf, andere erklären diese zusätzlich in kurzen Texten. Nur wenige Hidden Services wirken professionell und oft weisen die Seiten nur minimales Webdesign auf.

Meist handelt es sich laut eigenen Angaben bei den Betreibern der Hidden Services um einzelne oder wenige Personen. Teilweise stellen diese sich selbst vor und beschreiben ihre eigenen Fähigkeiten. Im Gegensatz zu vielen anderen Shops im Dark Web wird hier die Kommunikation oft nur über E-Mails angeboten. Dies kann daran liegen, dass Dienstleistungen vermehrt individuellen Kontakt und mehr Informationen erfordern als Produkte wie Drogen. Allerdings ist so auch das Betrugsrisiko höher.

Preise bewegen sich im Rahmen von 250€ bis 1500€ je nach Komplexität des Service. Einige Hidden Services geben gar keine Preise für ihre Angebote an.

Manche teureren Services scheinen fragwürdig. Zum Beispiel das Angebot “Destroying someones life” oder “Life ruining”, die angeblich das Leben des Opfers „zerstören“ oder „ruinieren“. Oft wird angegeben, dass das Opfer dieses Prozesses öffentlich gedemütigt, bzw. der Ruf ruiniert wird und das Opfer im Gefängnis landet. Nicht alle Hidden Services geben an, wie das erreicht werden soll. Manche geben an mit dem Unterschieben von kinderpornografischen Inhalten zu arbeiten.

Die Seriosität dieser Hidden Services wirkt im Vergleich zu anderen Angeboten im Dark Web niedriger. Da es sich nicht um ein konkretes physisches Produkt handelt ist ein potenzieller Betrug einfacher. Es verhält sich ähnlich wie bei den Angeboten von angeblichen Hitmans. Dies wird auch dadurch unterstrichen, dass nur wenige Hacking Anbieter Zahlungen über Escrow akzeptieren.

Markplätze Neben Verkäufern, die auf spezielle Produkte oder Produktgruppen spezialisiert sind, gibt es auch Marktplätze, auf denen mehrere Verkäufer ihre Waren anbieten. Diese Märkte haben eine andere Organisationsstruktur und sind teilweise durch Captchas und erforderliches Einloggen geschützt.

Ein Marktplatz wird oft von einem Administrator oder einem Administrations Team geführt. Diese Einheit überwacht und organisiert den Markt. Sie ist dafür zuständig neue Händler zu akzeptieren und gegebenenfalls Händler des Marktes zu verweisen.

Auf diesen Marktplätzen werden oft verschiedene Kategorien angeboten. Die häufigsten sind Drugs (Drogen), Hacking, Forgeries/Counterfeits (Fälschung), Geld und elektronische Geräte. Manche Dark Web Märkte sind nur auf eine bestimmte Produktkategorie spezialisiert. Oft handelt es sich dabei um Drogen, so zum Beispiel auch beim Marktplatz Archetyp.

Die Struktur der Marktplätze lässt sich in zwei verschiedene Arten unterteilen. Alle Hidden Services haben zunächst Oberkategorien. Danach werden entweder Händler angezeigt, die in dieser Kategorie Produkte verkaufen (siehe Abbildung 4.22) oder es erscheint direkt eine Übersicht aller Produkte der Kategorie (siehe Abbildung 4.23). Diese zwei Varianten weisen auf unterschiedliches Nutzerverhalten hin.

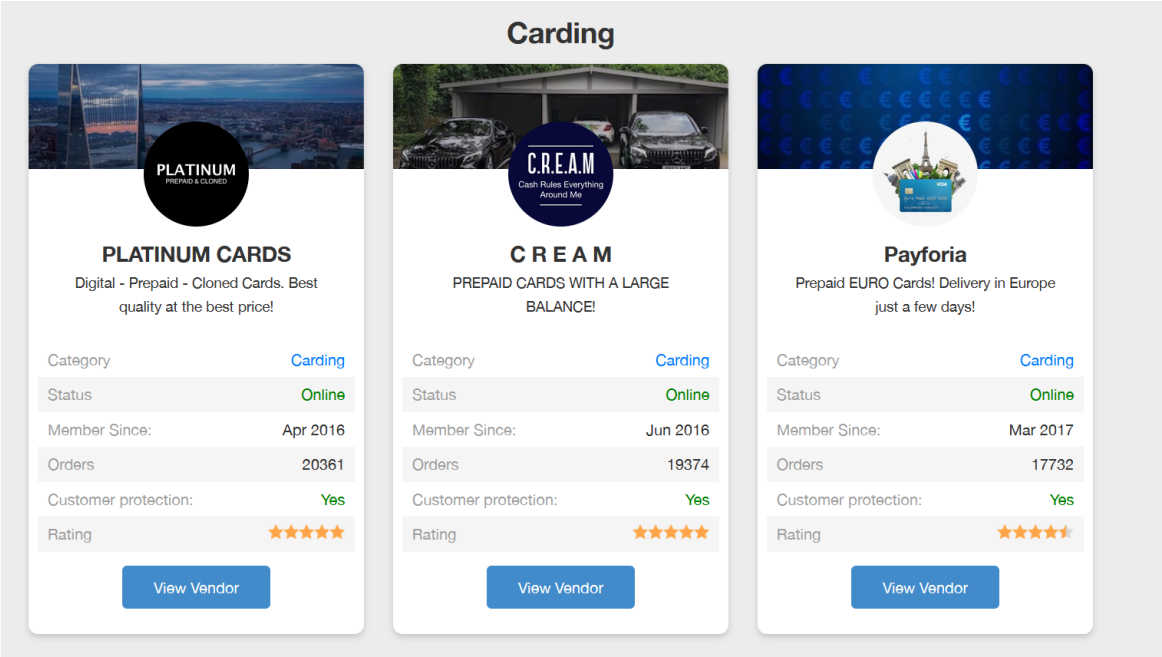

Abbildung 4.22: Hidden Service Deep Market [142]

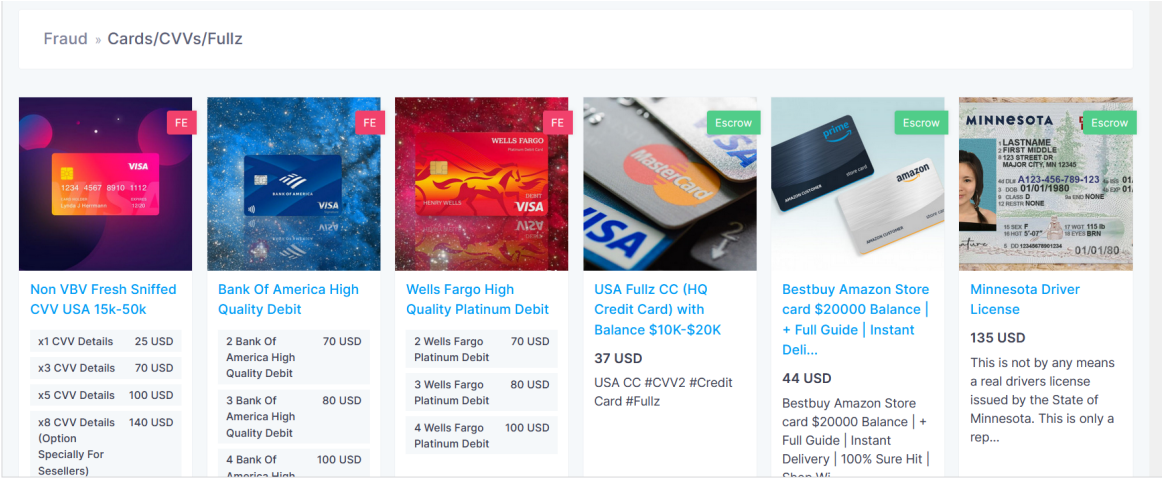

Abbildung 4.23: Hidden Service Nemesis Market [143]

Einerseits gibt es Nutzer, die Stammkunden bei bestimmten Händlern sind und deswegen auch gezielt nach deren Angeboten suchen. Besonders im Dark Web, wo Vertrauen schwierig zu gewinnen ist, erweist es sich als nützlich seine Käufe bei einem Verkäufer zu tätigen mit dem man bereits Erfahrung hat. Davon profitieren auch die Verkäufer, die sich so eine wiederkehrende Kundschaft sichern.

Andererseits scheint es auch Käufer zu geben, denen es eher um spezielle Produkte als um einen bestimmten Händler geht. Hier könnte die Risikobereitschaft höher sein oder das limitierte Angebot der Händler ist der Grund. Wenn der bisherige Verkäufer das gewünschte Produkt nicht oder nicht mehr anbietet, da es beispielsweise ausverkauft ist oder es Lieferschwierigkeiten gibt, wechseln die Kunden zu einem anderen Anbieter.

Des Weiteren sind auf Märkten mit Fokus auf die Verkäufer oft allgemein weniger Händler aktiv, was an der Anzahl der angezeigten Händler pro Kategorie zu erkennen ist. Manche Märkte zeigen bei der Suche oder dem Aufruf von Kategorien sowohl die aktiven Verkäufer als auch deren Produkte an und bilden damit eine Mischform.

Zu den Händlern werden meist verschiedene Grunddaten angegeben. Das sind häufig die Anzahl der Verkäufe und der Rezensionen, aber auch das Beitrittsdatum beim jeweiligen Markt. Des Weiteren gibt es Angaben zur durchschnittlichen Antwortzeit des Verkäufers, zum Lieferbereich oder zum Käuferschutz bzw. der Verfügbarkeit von Escrow Nutzung.

All diese Angaben stärken das Vertrauen von Nutzern gegenüber dem Verkäufer. Davon profitieren alle beteiligten Parteien. Die Händler erhalten mehr Kunden, die Kunden haben ein erhöhtes Gefühl von Sicherheit, dass sie ihr gekauftes Produkt tatsächlich erhalten, und die Marktbetreiber profitieren von jeder erfolgreichen Transaktion.

Neben Drogen und gefälschten Dokumente, gefälschten Kreditkarten oder Falschgeld bieten die Marktplätze eine große Menge weiterer Produkte an. Zum Beispiel elektronische Geräte wie Laptops, Spielekonsolen, Computer Teile, Smartphones, Smartwatches, Kopfhörer, Tastaturen, Headsets, Computermäuse, Drohnen, Staubsaugerroboter und weitere Produkte. Diese werden zu niedrigeren Preisen als bei offiziellen Clear Web Verkäufern angeboten werden. Zur Herkunft dieser Produkte wird oft keine Angabe gemacht. Es könnte sich aber beispielsweise um gestohlene Ware oder Fälschungen von Markenprodukten handeln.

Manche Marktplätze haben ein integriertes Forum, auf dem sich die Käufer und Verkäufer austauschen können. Viele Märkte haben außerdem einen Kunden Support, um Kunden bei auftretenden Problemen mit ihren Bestellungen und Lieferungen zu unterstützen.

Die Marktplätze sind ähnlich zu digitalen Marktplätzen im Clear Web. Es gibt die Möglichkeit, Rezensionen für Produkte oder Händler zu hinterlassen, sich mit einem Account einzuloggen und Bestellungen über Tracking Nummern zu verfolgen. Das Webdesign dieser Hidden Services ist oft vergleichbar mit Webseiten aus dem Clear Web und wirkt deshalb vor allem im Vergleich zu vielen Hidden Services von einzelnen Händlern professioneller und vertrauenswürdiger.

Die Produkte sind oft ähnlich zu denen, die Verkäufer auf ihren eigenen Hidden Services anbieten, die Auswahl ist jedoch wesentlich größer.

4.4.4 Weitere Hidden Services

Neben den bereits erwähnten Kategorien von Hidden Services gibt es im Dark Web, genau wie auch im Clear Web Seiten, die sich keiner Kategorie zuordnen lassen. Einige Beispiele werden nun aufgeführt, um einen erweiterten Überblick über das Dark Web und dessen Hidden Services zu geben.

Es gibt einige Hidden Services, welche Anleitungen zum Thema Hacking veröffentlichen. Außerdem auch Hidden Services im Bereich Glücksspiel und Wetten. Sowie Blogs von Privatpersonen oder Hidden Services, die Kochrezepte veröffentlichen [144]. Ein Hidden Service gibt an verschiedene Gegenstände aus der Nazi Zeit zu verkaufen, zum Beispiel Waffen, Uniformen und Flaggen [145]. Ein weiterer Hidden Service verkauft angeblich Menschenfleisch [146].

Der Hidden Service Spygame bietet “Leaks”, also unrechtmäßig veröffentlichte Daten, von Kameras in Form von Bildern und Videos an. Auf der Webseite sind tatsächlich Bilder und Videos zu sehen, bei denen es sich hauptsächlich um Aufnahmen von leicht bekleideten Frauen handelt. [147]

Ein Hidden Service mit dem Titel “Beyond the Styx” bietet angeblich unter anderem die Tatvideos des Kannibalen von Rotenburg zum Kauf an [148].

5 Fazit

In dieser Arbeit wurde ein aktueller Überblick über die im Tor-Netzwerk verfügbaren Hidden Services und ihre Inhalte erstellt. Die untersuchten Hidden Services wurden nach Kategorien sortiert und bezüglich ihrer Legalität unterteilt.

Als oft genutzte Einstiegspunkte in das Dark Web wurden Suchmaschine und Verzeichnisse gefunden. Auf diesen wurden Onion-Adressen gesammelt.

Es wurden sowohl legale als auch illegale Inhalte gefunden. Zusätzlich auch Inhalte, die sich nicht eindeutig diesen Kategorien zuordnen lassen. Es ist zu erkennen, dass die Anzahl der Hidden Services mit illegalen Inhalten deutlich überwiegt.

Die Inhalte der untersuchten Hidden Services sind oft in ähnlicher Form auch im Clear Web zu finden. Allerdings bietet das Tor-Netzwerk mit seinen Hidden Services eine deutlich größere Anzahl an illegalen Angeboten.

Besonders häufig treten digitale Marktplätze auf. Der Verkauf von illegalen Produkten macht einen großen Teil des Dark Webs aus. Hierbei werden Drogen und finanzielle Produkte am häufigsten angeboten. Die Preise auf diesen Verkaufsplattformen sind entweder ähnlich oder niedriger als im Clear Web. Bezahlt werden die Produkte mit Kryptowährungen und oft über ein spezielles Escrow System.

Neben den Marktplätzen gibt es viele weitere Hidden Services mit verschiedenen Inhalten. Insbesondere sind Bibliotheken, E-Mail, Anbieter und Foren zu erwähnen. Viele der legalen Inhalte befinden sich auf Hidden Services, die in gleicher Form auch im Clear Web zu finden sind. Das gilt vor allem für Nachrichtenmedien und Anbieter für Whistleblower.

Des Weiteren wurden der oft unfreundliche Umgangston in Foren und Konversationen, die häufige Nutzung von komplexen Captchas und das erhöhte Vorkommen von Betrugs Webseiten festgestellt.

Abschließend kann festgehalten werden, dass im Dark Web legale, aber auch vorwiegend illegale Inhalte angeboten werden. Stetig werden neue Methoden für erhöhte Anonymität entwickelt, aber dennoch gelingt es staatlichen Behörden immer wieder, die Identitäten von kriminellen Dark Web Nutzern aufzudecken und diese zu verhaften. Dies sollte stets weiterverfolgt werden. Auch das Internet und insbesondere das Dark Web sollte kein rechtsfreier Raum sein.

6 Ausblick

Ausgehend von den in dieser Arbeit gefundenen Inhalten können weitere Forschungen angestellt werden.

Datenverkehr Es gab bereits Ansätze, den Datenverkehr zu bestimmten Hidden Services zu untersuchen. Dies könnte weiterverfolgt und in größerem Rahmen durchgeführt werden, um die tatsächliche Nutzung der jeweiligen Hidden Services besser erfassen zu können.

Moralische Fragen Die festgestellte große Menge an illegalen Inhalten wirft Fragen zur moralischen Vertretbarkeit des Tor-Netzwerkes auf. Sollten die Betreiber des Tor Projects mehr dafür tun, gegen illegale Inhalte vorzugehen und wie kann Kriminalität im Dark Web eingedämmt oder bekämpft werden?

Strafverfolgung Besonders für die Strafverfolgung ist es von Interesse, neue Methoden zur De-Anonymisierung von Dark-Web-Nutzern zu entwickeln. Fälle, in denen Waffen aus dem Dark Web für Amokläufe und Gewalttaten genutzt wurden, zeigen die möglichen Auswirkungen dieses unkontrollierten Raumes.

Hidden Services Angeblich von Hidden Services angebotene Auftragsmorde, könnten ebenfalls von großem Interesse sein. Von Personen, die diese Dienste kontaktieren und in Anspruch zu nehmen versuchen, geht potenziell eine große Gefahr aus. Hier wäre die Übernahme solcher Hidden Services oder das Abfangen der Kommunikation mögliche Forschungsziele. Insbesondere um die potenziellen Opfer zu schützen und Straftaten zu verhindern.

Literaturverzeichnis

[1] „Student aus Landshut wegen Drogenhandel im Darknet verurteilt“. (2023), Adresse: https://www.bild.de/regional/muenchen/muenchen-aktuell/student-aus-landshut-wegen-drogenhandel-im-darknet-verurteilt-86462670.bild.html (besucht am 21. 12. 2023).

[2] „Gestohlene Daten und Zugänge von jedem dritten Unternehmen im Darknet“. (2023), Adresse: https://www.it-daily.net/it-sicherheit/cybercrime/gestohlene-daten-und-zugaenge-von-jedem-dritten-unternehmen-im-darknet (besucht am 21. 12. 2023).

[3] „Drogenhandel: Europol schließt Dark-Web-Portal Monopoly Market – fast 300 Festnahmen“. (2023), Adresse: https://t3n.de/news/operation-spector-europol-dark-web-monopoly-market-darknet-drogen-1549919/ (besucht am 21. 12. 2023).

[4] R. Liggett, J. R. Lee, A. L. Roddy und M. A. Wallin, „The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets“, in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt und A. M. Bossler, Hrsg., Cham: Springer International Publishing, 2020, S. 91–116, ISBN: 978-3-319-78439-7. DOI: 10.1007/978-3-319-78440-3_17.

[5] „Tor Overview“. (2019), Adresse: https://2019.www.torproject.org/about/overview.html.en#overview (besucht am 16. 12. 2023).

[6] „Tor Project - History“. (2023), Adresse: https://www.torproject.org/about/history/ (besucht am 25. 10. 2023).

[7] „The Tor Project - Annual Report 2021“. (2023), Adresse: https://www.torproject.org/static/findoc/2020-2021-TorProject-Annual-Report.pdf?h=3fdc0ff6 (besucht am 25. 10. 2023).

[8] „Tor Project - Users - Tor Metrics“. (2023), Adresse: https://metrics.torproject.org/ (besucht am 20. 12. 2023).

[9] R. Dingledine, N. Mathewson und P. Syverson, „Tor: The Second-Generation Onion Router“, *Paul Syverson*, Jg. 13, Juni 2004. Adresse: https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router.

[10] S. Saleh, J. Qadir und M. U. Ilyas, „Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research“, *Journal of Network and Computer Applications*, Jg. 114, S. 1–28, 2018, PII: S1084804518301280, ISSN: 10848045. DOI: 10.1016/j.jnca.2018.04.002.

[11] D. L. Huete Trujillo und A. Ruiz-Martínez, „Tor Hidden Services: A Systematic Literature Review“, *Journal of Cybersecurity and Privacy*, Jg. 1, Nr. 3, S. 496–518, 2021, PII: jcp1030025. DOI: 10.3390/jcp1030025.

[12] A. Shoker, „TorMass: Tor for the Masses Domestic and Monetized Anonymous Communication“, *Procedia Computer Science*, Jg. 181, S. 1216–1224, 2021, PII: S1877050921003707, ISSN: 18770509. DOI: 10.1016/j.procs.2021.01.319.

[13] B. Huang und Y. Du, „Discovering onion services through circuit fingerprinting attacks“, *High-Confidence Computing*, Jg. 3, Nr. 1, S. 100 099, 2023, PII: S2667295222000514, ISSN: 26672952. DOI: 10.1016/j.hcc.2022.100099.

[14] A. Biryukov, I. Pustogarov und R. Weinmann, „Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization“, in *2013 IEEE Symposium on Security and Privacy*, (Berkeley, CA), IEEE, 2013, S. 80–94, ISBN: 978-0-7695-4977-4. DOI: 10.1109/SP.2013.15.

[15] A. Skerritt. „How Does Tor Really Work? The Definitive Visual Guide (2023)“. (2023), Adresse: https://skerritt.blog/how-does-tor-really-work/ (besucht am 25. 10. 2023).

[16] P. Laperdrix, N. Bielova, B. Baudry und G. Avoine, „Browser Fingerprinting: A Survey“, *ACM Trans. Web*, Jg. 14, Mai 2020. DOI: 10.1145/3386040.

[17] K. Finklea, „Dark Web“, *Congressional Research Service*, März 2017. Adresse: https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf.

[18] J. Pace, „Exchange relations on the dark web“, *Critical Studies in Media Communication*, Jg. 33, Okt. 2016. DOI: 10.1080/15295036.2016.1243249.

[19] „Facebook - Facebook over Tor“. (2023), Adresse: https://www.facebook.com/facebookcorewwwi/posts/3727741430665883 (besucht am 26. 10. 2023).

[20] „Tor Project - How Do Onion Services Work?“ (2023), Adresse: https://community.torproject.org/onion-services/overview/ (besucht am 21. 10. 2023).

[21] J. Pastor-Galindo, F. Gómez Mármol und G. Martínez Pérez, „On the gathering of Tor onion addresses“, *Future Generation Computer Systems*, Jg. 145, S. 12–26, 2023, PII: S0167739X23000651, ISSN: 0167739X. DOI: 10.1016/j.future.2023.02.024.

[22] C. Guitton, „A review of the available content on Tor hidden services: The case against further development“, *Computers in Human Behavior*, Jg. 29, Nr. 6, S. 2805–2815, 2013, PII: S0747563213002690, ISSN: 07475632. DOI: 10.1016/j.chb.2013.07.031.

[23] C. Person, S. Hurka und C. Knill, „Opposite Trends in the Regulation of Pornography? Policy Differentiation and Policy Convergence Across 26 Countries Between 1960 and 2010“, *The Journal of Sex Research*, Dez. 2015. DOI: 10.1080/00224499.2015.1100701.

[24] J. Williams und A. L. Bretteville-Jensen, „Does liberalizing cannabis laws increase cannabis use?“, *Journal of Health Economics*, Jg. 36, Juli 2014. DOI: 10.1016/j.jhealeco.2014.03.006.

[25] A. Biryukov, I. Pustogarov, F. Thill und R.-P. Weinmann, „Content and Popularity Analysis of Tor Hidden Services“, in *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops*, (Madrid, Spain), IEEE, 2014, S. 188–193, ISBN: 978-1-4799-4181-0. DOI: 10.1109/ICDCSW.2014.20.

[26] G. Owen und N. Savage, „Empirical analysis of Tor Hidden Services“, *IET Information Security*, Jg. 10, Nr. 3, S. 113–118, 2016, ISSN: 1751-8717. DOI: 10.1049/iet-ifs.2015.0121.

[27] K. Li, P. Liu, Q. Tan, J. Shi, Y. Gao und X. Wang, „Out-of-band discovery and evaluation for tor hidden services“, in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, (Pisa Italy), S. Ossowski, Hrsg., New York, NY, USA: ACM, 2016, S. 2057–2062, ISBN: 9781450337397. DOI: 10.1145/2851613.2851798.

[28] M. W. Al-Nabki, E. Fidalgo, E. Alegre und L. Fernández-Robles, „ToRank: Identifying the most influential suspicious domains in the Tor network“, *Expert Systems with Applications*, Jg. 123, S. 212–226, 2019, PII: S0957417419300296, ISSN: 09574174. DOI: 10.1016/j.eswa.2019.01.029.

[29] M. Faizan und R. A. Khan, „Exploring and analyzing the dark Web: A new alchemy“, *First Monday*, 2019. DOI: 10.5210/fm.v24i5.9473.

[30] M. Spitters, S. Verbruggen und M. Van Staalduinen, „Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services“, in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, S. 220–223. DOI: 10.1109/JISIC.2014.40.

[31] I. Sanchez-Rola, D. Balzarotti und I. Santos, „The Onions Have Eyes“, in *Proceedings of the 26th International Conference on World Wide Web*, (Perth Australia), R. Barrett, R. Cummings, E. Agichtein und E. Gabrilovich, Hrsg., Republic und Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee, 2017, S. 1251–1260, ISBN: 9781450349130. DOI: 10.1145/3038912.3052657.

[32] „Reddit r/onions“. (2023), Adresse: https://www.reddit.com/r/onions/ (besucht am 20. 12. 2023).

[33] M. Chertoff, „A public policy perspective of the Dark Web“, *Journal of Cyber Policy*, März 2017. DOI: 10.1080/23738871.2017.1298643.

[34] M. Blowers, *Evolution of Cyber Technologies and Operations to 2035* (Advances in Information Security). Springer Cham, 2016, ISBN: 978-3-319-23584-4.

[35] C. Williams. „The Hidden Wiki: an internet underworld of child abuse“. (2011), Adresse: https://www.telegraph.co.uk/technology/internet/8851242/The-Hidden-Wiki-an-internet-underworld-of-child-abuse.html (besucht am 20. 12. 2023).

[36] DeepDotWeb. „The Hidden Wiki Seized (Old Domain)“. (2014), Adresse: https://web.archive.org/web/20150628213012/https://www.deepdotweb.com/2014/11/15/the-hidden-wiki-seized/ (besucht am 20. 12. 2023).

[37] „The Hidden Wiki“. (2023), Adresse: http://paavlaytlfsqyvkg3yqj7hflfg5jw2jdg2fgkza5ruf6lplwseeqtvyd.onion/ (besucht am 20. 12. 2023).

[38] „The Hidden Wiki“. (2023), Adresse: http://xsglq2kwy47ucaz2vekgd5y6ni46fl2gskjyhmtfln3wmcppsbp7asad.onion/ (besucht am 20. 12. 2023).

[39] „The Hidden Wiki“. (2023), Adresse: http://wiki5pbx73nfvmd7lug3siudagdbbdli7ta4ed2cklux4bbd6utc5byd.onion/ (besucht am 20. 12. 2023).

[40] „The Hidden Wiki“. (2023), Adresse: http://c2qqwyq6owprbuhcewn6wcwwuxmupojji4slfxzttuyyjnbkoklltcqd.onion/ (besucht am 20. 12. 2023).

[41] „The Uncensored Hidden Wiki“. (2023), Adresse: http://xs66xa6vh2vro5g5v2d476lahkhey4l6jsdkt6klxcz3ytz2i6silhyd.onion/index.html (besucht am 20. 12. 2023).

[42] „Another Hidden Wiki“. (2023), Adresse: http://2jwcnprqbugvyi6ok2h2h7u26qc6j5wxm7feh3znlh2qu3h6hjld4kyd.onion/ (besucht am 20. 12. 2023).

[43] „Onion Links“. (2023), Adresse: http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/ (besucht am 20. 12. 2023).

[44] „Tor Links“. (2023), Adresse: http://torlinksge6enmcyyuxjpjkoouw4oorgdgeo7ftnq3zodj7g2zxi3kyd.onion/ (besucht am 20. 12. 2023).

[45] „tor.taxi“. (2023), Adresse: http://tortaxi2dev6xjwbaydqzla77rrnth7yn2oqzjfmiuwn5h6vsk2a4syd.onion/ (besucht am 20. 12. 2023).

[46] „The Dark Web Pug“. (2023), Adresse: http://jgwe5cjqdbyvudjqskaajbfibfewew4pndx52dye7ug3mt3jimmktkid.onion/ (besucht am 20. 12. 2023).

[47] „The Hidden Wiki (Clear Web)“. (2023), Adresse: https://thehiddenwiki.com/ (besucht am 20. 12. 2023).

[48] „The Hidden Wiki (Clear Web)“. (2023), Adresse: https://the-hidden.wiki/ (besucht am 20. 12. 2023).

[49] Deutschlandfunk. „„Transparenzbericht“ von Sex-PortalSo wenig tut Pornhub gegen Missbrauch und Ausbeutung“. (2021), Adresse: https://www.deutschlandfunk.de/transparenzbericht-von-sex-portal-so-wenig-tut-pornhub-100.html (besucht am 20. 12. 2023).

[50] „Def Con Hacking Conference“. (2023), Adresse: https://defcon.org/index.html (besucht am 20. 12. 2023).

[51] „Ahmia“. (2023), Adresse: http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/ (besucht am 21. 12. 2023).

[52] „Haystak“. (2023), Adresse: http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/ (besucht am 21. 12. 2023).

[53] „VormWeb“. (2023), Adresse: http://volkancfgpi4c7ghph6id2t7vcntenuly66qjt6oedwtjmyj4tkk5oqd.onion/ (besucht am 21. 12. 2023).

[54] „Onion Land“. (2023), Adresse: http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/ (besucht am 21. 12. 2023).

[55] „Tordex“. (2023), Adresse: http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onion/ (besucht am 21. 12. 2023).

[56] „tor66“. (2023), Adresse: http://zozcz662yrb56oiuddiur22jlj37rmbnc3wlte5q6y5behlhr7peh4yd.onion/ (besucht am 21. 12. 2023).

[57] „Excavator“. (2023), Adresse: http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5fad.onion/ (besucht am 21. 12. 2023).

[58] „Duden Whistleblowing“. (2023), Adresse: https://www.duden.de/rechtschreibung/Whistleblowing (besucht am 20. 12. 2023).

[59] P. D. Salvo, *Digital Whistleblowing Platforms in Journalism*. Palgrave Macmillan Cham, 2020, ISBN: 978-3-030-38504-0.

[60] W. E. Scheuermann, „Whistleblowing as civil disobedience: The case of Edward Snowden“, *Philosophy and Social Criticism*, Jg. 40, Juni 2014. DOI: 10.1177/0191453714537263.

[61] D. L. Rothe und K. F. Steinmetz, „The case of Bradley Manning: state victimization, realpolitik and WikiLeaks“, *Contemporary Justice Review*, Jg. 16, Mai 2013. DOI: 10.1080/10282580.2013.798694.

[62] „WikiLeaks“. (2023), Adresse: https://wikileaks.org/ (besucht am 21. 12. 2023).

[63] „What Is SecureDrop?“ (2023), Adresse: https://docs.securedrop.org/en/stable/what_is_securedrop.html (besucht am 20. 12. 2023).

[64] „SpecTor“. (2023), Adresse: http://tcecdnp2fhyxlcrjoyc2eimdjosr65hweut6y7r2u6b5y75yuvbkvfyd.onion/ (besucht am 21. 12. 2023).

[65] „Central Intelligence Agency“. (2023), Adresse: http://ciadotgdlae22h5klxbn4yfnshykhnqmucnukqclss2x3ow6n46jn4id.onion/ (besucht am 21. 12. 2023).

[66] „The Northern California Illicit Digital Economy (NCIDE) Task Force“. (2023), Adresse: http://ncidetf3iyl2fxubhudskrhdz3ds2u3ohetmz3jk75wnkael77av5qqd.onion/ (besucht am 21. 12. 2023).

[67] „Distributed Denial of Secrets“. (2023), Adresse: http://ddosxlvzzow7scc7egy75gpke54hgbg2frahxzaw6qq5osnzm7wistid.onion/wiki/Contact (besucht am 21. 12. 2023).

[68] „Tor Browser User Survey Report“. (2021), Adresse: https://gitlab.torproject.org/tpo/ux/research/-/blob/master/reports/2021/tor-browser-user-survey-public.pdf (besucht am 21. 12. 2023).

[69] „Qubes OS: A reasonably secure operating system“. (2023), Adresse: http://www.qubesosfasa4zl44o4tws22di6kepyzfeqv3tg4e3ztknltfxqrymdad.onion/ (besucht am 20. 12. 2023).

[70] „Whonix - Superior Internet Privacy with Whonix“. (2023), Adresse: http://www.dds6qkxpwdeubwucdiaord2xgbbeyds25rbsgr73tbfpqpt4a6vjwsyd.onion/ (besucht am 20. 12. 2023).

[71] „Tails“. (2023), Adresse: http://tzoz3bensgxyzs7da7lpgsn3a74h7hlbm4wa6ytq2tg6ktd57w22vqqd.onion/ (besucht am 20. 12. 2023).

[72] „Debian“. (2023), Adresse: http://5ekxbftvqg26oir5wle3p27ax3wksbxcecnm6oemju7bjra2pn26s3qd.onion/index.en.html (besucht am 20. 12. 2023).

[73] R. Ensafi, P. Winter, A. Mueen und J. R. Crandall, „Analyzing the Great Firewall of China Over Space and Time“, *Proceedings on Privacy Enhancing Technologies*, Feb. 2015. DOI: 10.1515/popets-2015-0005.

[74] „How to circumvent the Great Firewall and connect to Tor from China?“ (2023), Adresse: https://support.torproject.org/censorship/connecting-from-china/ (besucht am 20. 12. 2023).

[75] „The New York Times“. (2023), Adresse: https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/ (besucht am 20. 12. 2023).

[76] „BBC News“. (2023), Adresse: https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/ (besucht am 20. 12. 2023).

[77] „ProPublica“. (2023), Adresse: http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion/ (besucht am 20. 12. 2023).

[78] „DW News“. (2023), Adresse: https://dwnewsgngmhlplxy6o2twtfgjnrnjxbegbwqx6wnotdhkzt562tszfid.onion/en/top-stories/s-9097 (besucht am 20. 12. 2023).

[79] „DarkNetLive“. (2023), Adresse: http://darknetlidvrsli6iso7my54rjayjursyw637aypb6qambkoepmyq2yd.onion/ (besucht am 20. 12. 2023).

[80] „Nitter“. (2023), Adresse: http://nitter.g4c3eya4clenolymqbpgwz3q3tawoxw56yhzk4vugqrl6dtu3ejvhjid.onion/ (besucht am 21. 12. 2023).

[81] „Red Hat Chat“. (2023), Adresse: http://3bu5sy446zbvqugbomvulx4ev43s2tgqcilvsg5oqlvguuziutljzgad.onion/index.php (besucht am 21. 12. 2023).

[82] „ChaTor“. (2023), Adresse: http://chatorcvcyvhnrv4zgpg2bok62eijzqc446oxzjsylskshb77uajt6yd.onion/dashboard.php (besucht am 21. 12. 2023).

[83] „TorBox“. (2023), Adresse: http://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion/ (besucht am 21. 12. 2023).

[84] „Mail2Tor“. (2023), Adresse: http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion/ (besucht am 21. 12. 2023).

[85] „BKA schaltet weltweit größten Geldwäschedienst im Darknet ab“. (2023), Adresse: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2023/Presse2023/230314_Geldwaesche_Darknet.html (besucht am 20. 12. 2023).

[86] J. Karaganis, *Shadow Libraries - Access to Knowledge in Global Higher Education*. The MIT Press, 2018, ISBN: 9780262535014.

[87] „Mutmaßliche Betreiber von Schattenbibliothek festgenommen“. (2022), Adresse: https://www.golem.de/news/z-library-mutmassliche-betreiber-von-schattenbibliothek-festgenommen-2211-169860.html (besucht am 20. 12. 2023).

[88] A. Peukert, *Die Gemeinfreiheit. Begriff, Funktion, Dogmatik*. Mohr Siebeck, 2012, ISBN: 978-3-16-151714-3.

[89] „Comic Book Library“. (2023), Adresse: http://nv3x2jozywh63fkohn5mwp2d73vasusjixn3im3ueof52fmbjsigw6ad.onion/ (besucht am 21. 12. 2023).

[90] „Webpage Archive“. (2023), Adresse: http://archiveiya74codqgiixo33q62qlrqtkgmcitqx5u2oeqnmn5bpcbiyd.onion/ (besucht am 21. 12. 2023).

[91] F. Oberholzer-Gee und K. Strumpf, „File Sharing and Copyright“, *Innovation Policy and the Economy*, Jg. 10, 2010. DOI: 10.1086/605852.

[92] „ZeroBin.net“. (2023), Adresse: http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/ (besucht am 21. 12. 2023).

[93] „Dump.li“. (2023), Adresse: http://dumpliwoard5qsrrsroni7bdiishealhky4snigbzfmzcquwo3kml4id.onion/ (besucht am 21. 12. 2023).

[94] „Black Cloud“. (2023), Adresse: http://bcloudwenjxgcxjh6uheyt72a5isimzgg4kv5u74jb2s22y3hzpwh6id.onion/ (besucht am 21. 12. 2023).

[95] „Starfiles“. (2023), Adresse: http://starfilesmj35tuw5bf7qaxfpf4d6tydvqjbftzw23t3ghtjreyx45id.onion/ (besucht am 21. 12. 2023).

[96] „The Pirate Bay“. (2023), Adresse: http://piratebayo3klnzokct3wt5yyxb2vpebbuyjl7m623iaxmqhsd52coid.onion/index.html (besucht am 21. 12. 2023).

[97] „DarkNetForum“. (2023), Adresse: http://3otgxq7d33rwspxfquwkqlp7r4yoicofniypk7hcxxqefrwhptqp7zad.onion/ (besucht am 21. 12. 2023).

[98] „Germania“. (2023), Adresse: http://germania7zs27fu3gi76wlr5rd64cc2yjexyzvrbm4jufk7pibrpizad.onion/ (besucht am 21. 12. 2023).

[99] „ZOLL-F: Festnahme des mutmaßlichen Lieferanten der beim Amoklauf in München am 22.07.2016 verwendeten Schusswaffe und Munition“. (2016), Adresse: https://www.presseportal.de/blaulicht/pm/116258/3405387 (besucht am 20. 12. 2023).

[100] Bundeskriminalamt. „Darknet-Marktplatz: Mutmaßlicher Administrator festgenommen“. (2022), Adresse: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/221027_PM_Darknet_Markplatz_Festnahme.html (besucht am 20. 12. 2023).

[101] L. Knuttila, „User unknown: 4chan, anonymity and contingency“, *First Monday*, Jg. 16, Sep. 2011. DOI: 10.5210/fm.v16i10.3665.

[102] B. Crawford, F. Keen und G. Suarez-Tangil, „Memes, Radicalisation, and the Promotion of Violence on Chan Sites“, *International AAAI Conference on Web and Social Media*, Jg. 15, Mai 2021. DOI: 10.1609/icwsm.v15i1.18121.

[103] „Endchan“. (2023), Adresse: http://enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj5smdad.onion/ (besucht am 21. 12. 2023).

[104] „NZ Darknet Market Forum“. (2023), Adresse: http://nzdnmfcf2z5pd3vwfyfy3jhwoubv6qnumdglspqhurqnuvr52khatdad.onion/ (besucht am 21. 12. 2023).

[105] K. Ren u. a., „Towards Understanding and Demystifying Bitcoin Mixing Services“, *Proceedings of the Web Conference 2021*, Juni 2021. DOI: 10.1145/3442381.3449880.

[106] J. A. Álvarez-Bermejo, Á. J. Varela-Vaca und F. J. de Haro-Olmo, „Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review“, *Sensors*, Jg. 20, Dez. 2020. DOI: 10.3390/s20247171.

[107] „Helix Light“. (2023), Adresse: http://mixerrzn5i6ypnujj2wtzioqnscfzpjooajl26w36kj74wehcqsdfeyd.onion/ (besucht am 21. 12. 2023).

[108] „Coinomize“. (2023), Adresse: http://coino2q64k4fg3lkjsnhjeydzwykw22a56u5nf2rdfzkjuy3jbwvypqd.onion/ (besucht am 21. 12. 2023).

[109] „EasyCoin“. (2023), Adresse: http://mp3fpv6xbrwka4skqliiifoizghfbjy5uyu77wwnfruwub5s4hly2oid.onion/ (besucht am 21. 12. 2023).

[110] „Onion Wallet“. (2023), Adresse: http://p2qzxkca42e3wccvqgby7jrcbzlf6g7pnkvybnau4szl5ykdydzmvbid.onion/ (besucht am 21. 12. 2023).

[111] „Bitcoin Investment Trust“. (2023), Adresse: http://2ezyoplodesxxtyxpoixa3vju2ecpdpnxo2ulcpdzijdmv7cahy3hgqd.onion/ (besucht am 21. 12. 2023).

[112] S. Bakshi, „Credit Card Fraud Detection : A classification analysis“, in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, 2018, S. 152–156. DOI: 10.1109/I-SMAC.2018.8653770.

[113] K. Guers, M. M. Chowdhury und N. Rifat, „Card Skimming: A Cybercrime by Hackers“, in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022, S. 575–579. DOI: 10.1109/eIT53891.2022.9813890.

[114] Bundeskriminalamt, „Angriffe auf Geldautomaten Bundeslagebild 2022“, Juli 2023. Adresse: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/AngriffeGeldautomaten/angriffeGeldautomatenBundeslagebild2022.html?nn=60672.

[115] F. Salahdine und N. Kaabouch, „Social Engineering Attacks: A Survey“, *Future Internet*, Jg. 11, 2019. DOI: 10.3390/fi11040089.

[116] „Cardshop“. (2023), Adresse: http://s57divisqlcjtsyutxjz2ww77vlbwpxgodtijcsrgsuts4js5hnxkhqd.onion/ (besucht am 21. 12. 2023).

[117] „Imperial Market“. (2023), Adresse: http://imperialk4trdzxnpogppugbugvtce3yif62zsuyd2ag5y3fztlurwyd.onion/ (besucht am 21. 12. 2023).

[118] „BitCards“. (2023), Adresse: http://bitcardshwnfg5ikvdgvwacotaxkiwbccrye6pbfjm7xckwl6mssq4ad.onion/index.html (besucht am 21. 12. 2023).

[119] „Fish'n Pal“. (2023), Adresse: http://56dlutemceny6ncaxolpn6lety2cqfz5fd64nx4ohevj4a7ricixwzad.onion/ (besucht am 21. 12. 2023).

[120] „Light Money“. (2023), Adresse: http://3apfeu2mlmbhnmsfbeaoc6nonjtme7gpo5lkqsjvnurnurw2qfisosid.onion/ (besucht am 21. 12. 2023).

[121] „KryptoPayPal“. (2023), Adresse: kptv3bqspwhe33ypttpblrbwmjt5la3xco6iuvzcfyldvksw2fc6pwyd.onion/ (besucht am 21. 12. 2023).

[122] „Millionair Private Club“. (2023), Adresse: http://p24axwfzctrpmhzb2rxkq4dvmyohvvqzcq4kledplliy632kjbhvy6qd.onion/ (besucht am 21. 12. 2023).

[123] „AccMarket“. (2023), Adresse: http://55niksbd22qqaedkw36qw4cpofmbxdtbwonxam7ov2ga62zqbhgty3yd.onion/ (besucht am 21. 12. 2023).

[124] „Dark Web Wolf Street“. (2023), Adresse: http://streetgg2yqlii5ls3bro5ue3fhdaew4grl5xiduyyp22q7aachdfpad.onion/ (besucht am 21. 12. 2023).

[125] „The Notes King - Buy Pre-Shred Cash Online“. (2023), Adresse: https://thenotesking.com/ (besucht am 20. 12. 2023).

[126] „Mike's Grand Store“. (2023), Adresse: http://4yx2akutmkhwfgzlpdxiah7cknurw6vlddlq24fxa3r3ebophwgpvhyd.onion/ (besucht am 21. 12. 2023).

[127] „Counterfeit USD“. (2023), Adresse: http://qazkxav4zzmt5xwfw6my362jdwhzrcafz7qpd5kugfgx7z7il5lyb6ad.onion/ (besucht am 21. 12. 2023).

[128] „HQER“. (2023), Adresse: http://odahix2ysdtqp4lgak4h2rsnd35dmkdx3ndzjbdhk3jiviqkljfjmnqd.onion/ (besucht am 21. 12. 2023).

[129] „USJUD“. (2023), Adresse: http://usjud6j75mkut5w6fxbv7xnowzt7x3ostgcb2zdgusgt3sntfualg2yd.onion/ (besucht am 21. 12. 2023).

[130] „Dresdner zu Haftstrafe verurteilt : Suche nach Mörder im Darknet“. (2022), Adresse: https://www.mdr.de/nachrichten/sachsen/dresden/urteil-mord-darknet-auftragskiller100.html (besucht am 21. 12. 2023).

[131] „Russia police probe 'dark net' murder case“. (2019), Adresse: https://www.bbc.com/news/technology-47747357 (besucht am 21. 12. 2023).

[132] G. M. Volpicelli. „The unbelievable tale of a fake hitman, a kill list, a darknet vigilante... and a murder“. (2018), Adresse: https://www.wired.co.uk/article/kill-list-dark-web-hitmen (besucht am 21. 12. 2023).

[133] „TorZon Market“. (2023), Adresse: http://torzon4kv5swfazrziqvel2imhxcckc4otcvopiv5lnxzpqu4v4m5iyd.onion/index.php (besucht am 21. 12. 2023).

[134] „420prime“. (2023), Adresse: http://ajlu6mrc7lwulwakojrgvvtarotvkvxqosb4psxljgobjhureve4kdqd.onion/ (besucht am 20. 12. 2023).

[135] „Smokerland Marihuana Onlineshop“. (2023), Adresse: https://smokerland.net/de/ (besucht am 20. 12. 2023).

[136] „Weed nach Hause“. (2023), Adresse: https://weed-nach-hause.com/ (besucht am 20. 12. 2023).

[137] „DrChronic“. (2023), Adresse: http://iwggpyxn6qv3b2twpwtyhi2sfvgnby2albbcotcysd5f7obrlwbdbkyd.onion/ (besucht am 20. 12. 2023).

[138] „Smokeables - Finest Organic Cannabis“. (2023), Adresse: http://kl4gp72mdxp3uelicjjslqnpomqfr5cbdd3wzo5klo3rjlqjtzhaymqd.onion/ (besucht am 20. 12. 2023).

[139] „DeDope German Weed Store“. (2023), Adresse: http://dumlq77rikgevyimsj6e2cwfsueo7ooynno2rrvwmppngmntboe2hbyd.onion/ (besucht am 20. 12. 2023).

[140] „EuCanna First Class Cannabis Healthcare“. (2023), Adresse: http://wges3aohuplu6he5tv4pn7sg2qaummlokimim6oaauqo2l7lbx4ufyyd.onion/ (besucht am 20. 12. 2023).

[141] „Euro Guns“. (2023), Adresse: http://hyjgsnkanan2wsrksd53na4xigtxhlz57estwqtptzhpa53rxz53pqad.onion/index.php (besucht am 21. 12. 2023).

[142] „Deep Market“. (2023), Adresse: http://deepmar4ai3iff7akeuos3u3727lvuutm4l5takh3dmo3pziznl5ywqd.onion/ (besucht am 21. 12. 2023).

[143] „Nemesis Market“. (2023), Adresse: http://nemesis555nchzn2dogee6mlc7xxgeeshqirmh3yzn4lo5cnd4s5a4yd.onion/items/fraud/cards-cvvs-fullz/ (besucht am 21. 12. 2023).

[144] „Based Cooking“. (2023), Adresse: http://wpzzhvw6q32pneau3rzsa5h7tzl7fgswya3cgtmu5rpesd725bii3cad.onion/ (besucht am 21. 12. 2023).

[145] „The Cavern“. (2023), Adresse: http://vpocsdxjwaodp73xm65pscydeidt3uap2lftcuuhxpznjigtuzx5pqad.onion/index.php (besucht am 21. 12. 2023).

[146] „Carne Human Meat“. (2023), Adresse: http://vihnyh2wifmtfoa72xpufv4qjuf7xhlazot467jjlx657gwzazsr5byd.onion/enindex.html (besucht am 21. 12. 2023).

[147] „SpyGame“. (2023), Adresse: http://spygame5awoookfmfhda7jfqimwyfxicjkn3wc4v3oozyno7sqv2axid.onion/ (besucht am 21. 12. 2023).

[148] „Beyond the Styx“. (2023), Adresse: http://o455kwz35ukwqp5zpqa3fs4vi44mhyeliiadpgjb4ele2qlyucjxtrid.onion/index_de.html (besucht am 21. 12. 2023).

Eidesstattliche Erklärung

Hiermit versichere ich – Oscar Trepte – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 20. Februar 2024	
Ort, Datum	Oscar Trepte