FB 5

Bachelorarbeit

„Anonymität im Darknet: Nutzer und Usability im Vergleich der drei Hauptvertreter“

Julia Görmer

Anhalt University of Applied Sciences

Hochschule Anhalt

Fachbereich 5

Angewandte Informatik und Digitale Spieleentwicklung

Bachelorarbeit

Anonymität im Darknet

Nutzer und Usability im Vergleich der drei Hauptvertreter

Autor: **Julia Görmer** | Matrikelnummer: 4056018

Gutachter: Prof. Dr. Alexander Carôt | Zweitgutachter: Herr Karsten Zischner

Kurzfassung

Die vorliegende Bachelorarbeit gibt einen Überblick über die Funktion und Hintergründe des Darknets mit einem konkreten Schwerpunkt auf das Problem der Anonymität. Zu diesem Zweck wurden die drei Netzwerk-Lösungen „The Onion Routing Network“, „Freenet“ und „The Invisible Internet Project“, vorgestellt und anhand ihrer Usability und technischen Kriterien untersucht. Die Ergebnisse des Vergleichs dieser Darknets liefern Aufschlüsse zu zukünftigen Entwicklungen und ermöglichen einen Einstieg in eine Betrachtung des Themas aus anderen Fachrichtungen.

Abstract

The present work is meant to give an overview about functionality and historical background of darknets. In that context it focuses on the anonymity-aspect. To accomplish an all-around insight into the topic, I compared three solutions - The Onion Routing Network, Freenet and the invisible internet project – focused on usability and technical solutions. The results of this comparison lead to valuable conclusions of future developments and delivers an approach to explore the topic related to other departments.

Keywords: Darknet, Freenet, TOR, I2P, Netzwerk, Anonymität

Inhaltsverzeichnis

1 Einleitung

„Zwei Darknet-Marktplätze ausgehoben: Ermittler schließen Plattform für Drogen und Waffenhandel“[1], „Darknet: Waffen, Drogen & Co. – die dunkle Seite des Internets!“ [2], „Festnahmen in Bedburg: Drogen im großen Stil übers Darknet verkauft“[3], „Ex-Dealer packt aus: So funktioniert der Drogenhandel im Darknet“[4], „Marktplätze im Darknet: Ich kauf mir einen Hackerangriff“[5]

Erschreckende Schlagzeilen der letzten Monate und oft die einzigen Informationen, die viele Menschen über das Thema Darknet erhalten. Während das Darknet vor einigen Jahren für einen Großteil der deutschen Bevölkerung völlig unbekannt oder gar ein Mythos war, so beherrscht es nun doch immer häufiger Nachrichten und Schlagzeilen. Doch verschwindend selten kommt es dabei zu einer Erwähnung ohne geringschätzende oder ablehnende Tendenzen. Dabei erzeugen die Medien auch mit Negativ-Headlinern wie diesen ein rätselhaftes und geradezu mythisches Bild des Darknets.

Dies gilt es zu ergründen. Was hat es mit dem Darknet auf sich? Weshalb wird etwas, das augenscheinlich so vor Kriminalität strotzt, gebilligt? Wer nutzt es wie und weshalb? Fragen, auf die oft Antworten fehlen, obwohl das Thema Darknet und die Anonymität, die es bietet, so brisant ist, wie noch nie.

Besonders in der heutigen Zeit, in der etwa 80% der Deutschen das Internet für alltägliche Aufgaben nutzen [6] und nahezu jeder ein Smartphone, Tablet oder anderes mobiles Endgerät hat, haben viele die Idee von Anonymität aufgegeben oder verlassen sich auf Standardeinstellungen. Wir befinden uns in einer modernen Informationsgesellschaft, und die Analyse des Onlineverhaltens eines jeden sind für Viele zur Normalität geworden. Doch es gibt Personengruppen, für die ein anonymes Surfen geradezu überlebenswichtig ist und für die das Darknet trotz all der schaurigen Medienpräsenz die einzige Möglichkeit ist, diese Anonymität zu gewährleisten.

In meiner Arbeit möchte ich auf die aktuelle Medienpräsenz des Darknets eingehen und anderen Nutzen als Drogen- und Waffenhandel aufzeigen, der deutlich seltener von deutschen Medien aufgegriffen wird [7]. Ich möchte die verschiedenen Nutzergruppen der Darknets analysieren und speziell auf jene Nutzer eingehen, die eine gesellschaftlich erwünschte Nutzung der Netzwerke anstreben. Für diese Personengruppen soll die Bedeutung der Anonymität hervorgehoben werden. Da diese Arbeit jedoch keiner Lobeshymne gleichkommen soll, möchte ich einen neutralen, wenn auch kritischen Blickwinkel auf das Dilemma der Anonymität im Darknet beibehalten.

1.1 Hintergrund & Kontext

Bereits vor einigen Jahren bin ich durch Gespräche mit Kommilitonen auf das Thema rund um das Darknet aufmerksam geworden. Tiefergehendes Interesse wurde erst geweckt, als das Darknet erneut im Zusammenspiel mit der Online-Rätselreihe der Cicada 3301 [8] in den Medien auftauchte. In diesem Zusammenhang verdichtete sich ebenfalls das Interesse für Online-Anonymität und die Gründe, die dahinterstehen könnten. Durch den Autor Stefan Mey, der sich in mehreren kleinen Artikeln, sowie einem eigenen Buch mit dem Problem befasste, und der Aufklärungsarbeit der Enigma Group zu diesem Thema war es mir möglich, mich umfassender in die Thematik einzuarbeiten. Dabei fiel mir auf, dass es viele unterschiedliche Sichtweisen auf die Darknets gibt und wie oft deren Nutzung von Personen, die sich mit der Materie befassen, völlig gegensätzlich begründet wird. In Gesprächen mit weniger Computer-affinen Personen folgt nahezu immer die Frage „Was ist das eigentlich genau, dieses Darknet? Wie funktioniert das?“. Zusammengefasst erschienen mir diese Gründe ausschlaggebend dafür, diese Fragen im Rahmen meiner Bachelorarbeit zu beantworten.

Dabei werden verschiedene Themenbereiche des Studiums aufgegriffen - allem voran Datenschutz und Datensicherheit, da sich ein Großteil der Ideen, die hinter den Darknets stehen, auf Kryptografie stützen und deren Ziel fast immer die verschlüsselte Übermittlung von Informationen ist - ein Problem, mit dem sich die Menschen schon lang vor der Erfindung des Computers befassten und dessen Faszination nicht nachlässt. Auch das Online- und Medienrecht wird dabei tangiert. Oft bewegen sich Nutzer hier in Grauzonen, und vielen Personen ist die Rechtslage unbekannt. Wissen über Netzwerke, über Datenverbindungen und über die Geschichte der Kommunikation sind erforderlich, um zu verstehen, wie die Darknets überhaupt entstehen konnten. Auch Gebiete, die auf den ersten Blick weit abseits des eigentlichen Themas wirken, sind relevant, wie zum Beispiel Usability und die Interaktion zwischen Mensch und Computer, sowohl im Hinblick auf Hardware, als auch Software. Dies spielt vor allem dann eine Rolle, wenn es um die Frage der Anonymität geht.

Dabei gibt es kaum genaue Zielgruppen, auf die die Idee der Darknets abzielt. Jeder soll sie nutzen können, um anonym mit der Außenwelt in Kontakt zu treten. Jedoch haben sich aus geschichtlichen Hintergründen und den Gegebenheiten, welche die Anonymität mit sich bringt, einige Nutzergruppen besonders stark herauskristallisiert. Dabei werden

unterschiedlichste Absichten verfolgt. „Wie zu erwarten, wird die dort gebotene Anonymität auf gesellschaftlich erwünschte, wie ethisch unerwünschte Weise genutzt.“ [9] Doch gerade diesen „gesellschaftlich erwünschten“ Nutzern sollte verständlich gemacht werden, wie das Darknet funktioniert und wie sie anonym bleiben können. Oftmals scheitert die Kommunikation über diese Plattformen an fehlendem Know-How, falschen Informationen über das System oder Fehlern in der Nutzung, welche die Anonymität gefährden.

Zu diesen erwünschten Nutzern zählen unter anderem Reporter und Journalisten aus Ländern, in denen die Freiheit der Medien nicht gewährleistet ist oder in denen kritische Berichterstattung bestraft wird. Doch auch Menschen die nicht für die Medienbranche arbeiten und Informationen teilen wollen, ohne sich selbst dabei in Gefahr zu begeben. Darunter zählen auch die sogenannten Whistleblower, die spätestens seit Edward Snowden, den meisten ein Begriff sein sollten. Auch Medien-Konzerne zählen zu den „erwünschten Nutzern“. So haben zum Beispiel die britische Zeitung „Guardian“, die „New York Times“ und „Heise Online“ im TOR-Darknet anonyme Postfächer [10] eingerichtet, um Informanten Sicherheit zu bieten. Auch einige bekannte Socialmedia Dienste bieten Darknet-Zugänge zu ihren Portalen an, um Nutzern auch in Ländern, in denen diese Funktionen gesperrt sind, die Möglichkeit zu bieten, über deren Dienste zu kommunizieren. So ist zum Beispiel Facebook unter der Adresse „https://facebookcorewwwi.onion“ [12], anonym über den TOR-Browser erreichbar und kann so beispielsweise auch in China verwendet werden. Ebenfalls für Angehörige von Flüchtlingen soll die Darknet-kommunikation von „gesellschaftlich erwünschtem Nutzen“ sein. Diese können so mit ihren Angehörigen in Kriegs- und Krisengebieten kommunizieren ohne deren Standort oder Identität preiszugeben. Diese Arten der Nutzung, machen das Thema wichtig und verlangen nach einer besseren Aufklärung der Verwendung und technischen Hintergründe.

1.2 Probleme & Fragen

Es ergeben sich zwei Arten von Problemen Probleme- auf die ich in meiner Arbeit eingehen möchte und solche, die sich bei der Erarbeitung des Themas ergeben.

1.2.1 Probleme, die sich ergeben:

Die größte Schwierigkeit besteht hierbei darin, eine objektive Haltung zu dem Thema zu wahren- insbesondere, da ich mich vorwiegend auf den erwünschten Nutzen der Darknets konzentrieren möchte. Ein zweites Problem, bei der Erarbeitung könnte darin bestehen, dem Leser ein übersichtliches Gesamtbild der Hauptvertreter der Darknets zu liefern, da hierbei eine beachtliche Menge an Informationen ergibt. Hinzu kommt, dass die komplexen Funktionsweisen der Netzwerke auch für Leser ohne besonderes Vorwissen zu diesem Thema anschaulich erläutert werden müssen. Am Ende der Arbeit soll ein stimmiges Gesamtbild stehen, das einen Vergleich von TOR, I2P[1] und Freenet im Hinblick auf Nutzer und Anonymität bietet und den Leser aufklärt.

1.2.2 Probleme, auf die ich eingehen möchte:

Um dem Leser einen umfassenden Eindruck zu verschaffen und über Anonymität, Nutzer und Verwendungszweck der Darknets aufzuklären, müssen mehrere Fragen innerhalb der Arbeit beantwortet werden.

- Was ist das Darknet und wie ist es einzuordnen?
- Wie funktioniert die Software hinter dem Phänomen?
- Wer nutzt es und weshalb?
- Ist die Anonymität im Darknet undurchdringbar oder gibt es Schwächen?
- Lassen sich die Anonymität und der Sicherheitswunsch des Staates vereinbaren?
- Welche Hindernisse ergeben sich für Nutzer?
- Worin bestehen die Unterschiede der Darknets?

Um auf diese Probleme für den Leser der Arbeit verständlich eingehen zu können, muss zuerst eine Wissensbasis über das Thema Darknet geschaffen werden. Dazu gehört eine

[1] Kurz für „Invisible Internet Project“

geschichtliche, gesellschaftliche und technische Einordnung sowie eine umfassende Begriffsklärung. Da es mehrere Darknets gibt, soll dies vor allem am Beispiel der drei bekanntesten Vertreter geschehen, welche sich in der Öffentlichkeit unter verschiedenen Nutzergruppen, durchgesetzt haben. „The Onion Routing“-Project, Freenet und dem „invisible Internet Project“.

1.3 Ziel der Arbeit

Das oberste Ziel dieser Arbeit ist es, Aufklärungsarbeit bezüglich des Darknet und der dort gebotenen Anonymität zu leisten. Sie soll ein Bewusstsein dafür schaffen, worum genau es sich bei einem Darknet handelt und wie bekannte Vertreter funktionieren. Es soll einen Einblick darin geliefert werden, weshalb die dort gebotene Anonymität sowohl wichtig als auch gefährlich ist und die Barrieren in der Handhabung dieser Vertreter beleuchtet werden. Konkret gehe ich dafür auf die Darknet-Lösungen des TOR-Projekts, der Freenet-Gruppe und des I2P-Projektes ein. Leser dieser Arbeit sollen im Anschluss ein besseres Verständnis für die Thematik entwickeln, sowie einen klaren Zusammenhang der Begrifflichkeiten, um Nachrichten und Artikel zu der Thematik in Zukunft kritisch bewerten zu können.

2 Vorbereitende Arbeiten und Stand der Entwicklung

Ein Schwerpunkt dieser Arbeit soll es sein, sich mit den Nutzern und der Usability des Aspekts der Darknets zu befassen. Dies soll vor allem in Hinblick auf die Anonymität der Nutzer geschehen. Um eine Untersuchung dieser Aspekte zu gewährleisten, muss jedoch zunächst eine vorbereitende Wissensbasis geschaffen werden. Aus diesem Grund wird im Folgenden eine klare Abgrenzung relevanter Begrifflichkeiten erfolgen, sowie eine spezifizierte Definition von Usability-Kriterien für Darknets im Allgemeinen. Außerdem soll der Begriff der Anonymität im Rahmen des Themas eingegrenzt und definiert werden, um sich in der folgenden Arbeit darauf beziehen zu können. Für einen fließenden Kontext soll ein Einblick in den aktuellen Stand der Entwicklung und eine historische Einordnung sorgen.

2.1 Surface Web, Deep Web, Darknet – Begriffsklärung

Clearnet, Internet, Surface Web, Visible Web, Deep web, Dark Web, Darknet. Es gibt einen wahren Begriffsdschungel rund um das Thema des Darknets. Dabei haben nicht alle diese Namen etwas mit den eigentlichen Darknets zu tun, werden jedoch häufig in Online-, sowie Zeitungsartikeln falsch verwendet. Sogar in einigen FAQ-Sektionen befassen sich themenspezifische Webseiten speziell mit dieser Problematik. Aus diesem Grund soll auch hier zunächst eine Abgrenzung der genannten Begriffe erfolgen.

2.1.1 Internet

Das Internet sollte in der heutigen Zeit jedem Bürger unserer Informationsgesellschaft bekannt sein. Doch oftmals wird der Begriff zu grob verwendet. Vielen Menschen ist nicht bewusst, dass man das Internet in zwei separate Sektionen untergliedert. Den Teil, den wir mit Suchmaschinen erfassen und finden können und den Teil, der von Suchmaschinen nicht erfasst wird. Nicht nur beim Standardnutzer kommt es dabei zu Verwirrungen, auch bei Spezialisten wie dem Bundeskriminalamt (BKA) herrscht durchaus Zwiespalt, wie die Abgrenzungen der einzelnen Begrifflichkeiten zu bewerten ist. So präsentierten die Beamten des BKAs bei einer Bundeskonferenz im Juli 2016 an einem Tag den Begriff des „Clearnet“ und zwei Tage später den Begriff des „Visible Web“. Wobei die jeweiligen Vortragenden der Meinung waren, sie würden unterschiedliche Konzepte präsentieren. Inhaltlich war letztendlich jedoch kaum ein Unterschied erkennbar [13]. Das

Problem des sogenannten „Wordings[2]“, also der Verwendung dieser verschiedenen Namen für ein und dieselbe Sache, entstand vor allem dadurch, dass sich diese Bezeichnungen aus dem Nutzen heraus gebildet haben und lange Zeit parallel ohne konkrete Definition existieren konnten. Dieses Problem besteht nicht ausschließlich in dieser Thematik, sondern ist fachübergreifend in vielen Bereichen der Wirtschaft vertreten. Üblicherweise löst sich das Problem dadurch, dass Fachliteratur und Fachkräfte sich über einen gewissen Zeitraum automatisch auf den gängigsten Begriff einigen. Da das Thema der Abgrenzungen von Darknet und Internet jedoch noch relativ neu ist, gibt es noch keine favorisierten Bezeichnungen.

Wenn wir im Alltagsgebrauch von „dem Internet“ sprechen, meinen wir häufig jedoch nur den Teil des Internets, welcher von Suchmaschinen wie Google, Yahoo oder Bing erfasst wird. Eine Frage, die man sich stellen könnte, wäre, wieso trotzdem beide Teile unter dem Begriff des Internets gezählt werden können oder worin ihre Gemeinsamkeiten bestehen. Das Internet als Ganzes lässt sich vom Darknet konkret dadurch abgrenzen, dass sich die Überwachung von Userprofilen, besuchten Seiten und Verhaltensmustern relativ einfach umsetzen lässt. Sei es durch bestimmte Accounts, mit denen wir uns anmelden, unsere IP-Adresse oder die Informationen die wir auf den Servern unserer Internetprovider hinterlassen.

2.1.2 Clearnet, Surface Web, Visible Web

Der Teil des Internets, durch den wir uns mit Suchmaschinen navigieren können, wird Clearnet[3], Surface Web, [4]oder auch Visible Web, [5]genannt. Webadressen, die in diesen Bereich des Internets fallen, werden indizierte Webseiten [14] genannt. Das bedeutet, sie wurden in den Datenbestand von diversen Suchmaschinen aufgenommen, befinden sich also im Index. Dies ist Grundvoraussetzung dafür, dass die Adresse überhaupt von einer Suchmaschine gefunden werden kann. Die Inhalte des Surface Web lassen sich mit gängigen Internet-Browsern, wie zum Beispiel Google Chrome, Firefox oder Microsoft Edge aufrufen. Webseiten haben hier gängige Endungen wie Beispielsweise „.de“ oder „.com“.

[2] Deutsch: Wortfindung, Wird in der IT verwendet um die Zuordnung von Namen und Begrifflichkeiten zu bestimmten Sachverhalten zu beschreiben

[3] Deutsch: klares Netz

[4] Deutsch: Oberflächen Web

[5] Deutsch: Sichtbares Web

2.1.3 Deep Web

Der Begriff „Deep Web“ bezeichnet die Inhalte des Internets, die von Suchmaschinen nicht erfasst werden, da sie nicht in deren Datenbestand aufgenommen wurden. Dies kann verschiedene Gründe haben. Zum einen sind das Intranets[6], die bewusst vom öffentlichen Internet abgegrenzt werden, zum Beispiel von Unternehmen oder Organisationen. Ein weiterer Grund kann sein, dass Seiten gar nicht oder nur sehr rudimentär mit dem restlichen Netz verlinkt sind. Auch Bezahlschranken und Nutzerkonten können eine Aufnahme in den Index der Suchmaschinen verhindern. Dadurch können diese Seiten von Nutzern nur dann gefunden werden, wenn diese die Adresse kennen oder sie sich durch die Navigation einer bestimmten Webseite klicken, die mit der Zielseite verlinkt ist. Nach Sherman & Price [15] kann das Deep Web in fünf unterschiedliche Teile gegliedert werden: Opaque Web, Private Web, Proprietary Web, Invisible Web und Truly Invisible Web. Eine detailliertere Erklärung dazu findet sich in Tabelle 1: Arten des Deep Web.

Art des Deep Web	*Deutsche bezeichnung*	*Erklärung*
Opaque Web	Undurchsichtiges Netz	Könnten indiziert werden, technische Leistungsfähigkeit und Nutzen-Aufwand-Relation sorgen jedoch dafür, dass dies nicht getan wird.
Private Web	Privates Netz	Könnten indiziert werden, jedoch wird dies durch Zugangsbeschränkungen abgelehnt. ZUM BEISPIEL Intrantes oder Passwortgeschützte Seiten.
Proprietary Web	Gesetzlich geschütztes Netz	Sind nur nach Annerkennung von Nutzerbedingungen oder Eingabe von Passwörtern zugänglich
Invisible Web	Unsichtbares Netz	Diese Seiten können aus technischer Sicht zwar indiziert werden, jedoch wird dies aus kaufmännischen oder strategischen Gründen vermieden. ZUM BEISPIEL Datenbanken mit Webformular
Truly Invisible Web	Tatsächlich unsichtbares Netz	Webseiten die aus technischen gründen (noch) nicht indiziert werden können.

Tabelle 1: Arten des Deep Web

Quelle: Sherman & Price (2001)

[6] Kann unabhängig vom öffentlichen Netz benutzt werden

In verschiedenen Publikationen und Artikeln wird dabei oft das berühmte Sinnbild des Eisbergs benutzt, um eine Grenze zwischen Surface Web und Deep Web zu veranschaulichen, zu sehen im Abbildungsverzeichnis, Abbildung 1: Die Tiefen des Internets.

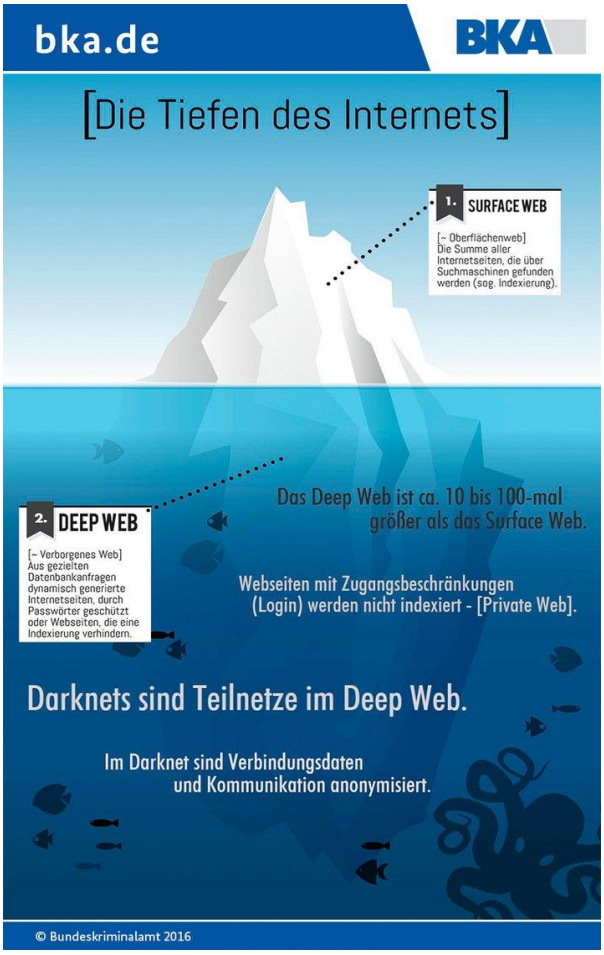

Abbildung 1: Die Tiefen des Internets
Quelle: https://cdn.netzpolitik.org/wp-upload/2016/07/CoXFpatXgAARzAM.jpg (abgerufen am 13.04.2018)

Dabei gibt es verschiedene Ausführungen dieser Grafik aus den unterschiedlichsten Quellen. Diese Versinnbildlichung ist daher so beliebt, da man nur „die Spitze des Eisberges“ sehen kann, während der ungeahnt größere Teil unter Wasser vor Blicken verborgen bleibt. Ähnlich wie bei „der Spitze des Eisberges“ wird davon ausgegangen, dass die Größe des indizierten Surface Webs deutlich kleiner ist als der „verborgene“ Teil des Internets, das Deep Web. So wird ein Eindruck von ungeahnten, verborgenen Tiefen des Deep Webs, die es zu entdecken gibt, erzeugt. Mit Hilfe dieser Grafik sollte vom Bundeskriminalamt, im Oktober 2016 der Eindruck erweckt werden, dass es sich beim Deep Web um eine 10- bis 100-mal größere Menge an Daten handeln soll, als das Surface Web

umfasst [Abbildung 1]. Dabei handelt es sich jedoch um falsche Zahlen. Der Eisberg-Vergleich im Zusammenhang mit der Problematik des Deep Web stammte ursprünglich aus einem Whitepaper[7] der amerikanischen Firma BrightPlanet [9]. Dabei handelt es sich um ein Unternehmen für Datenanalyse, welches 2001 auf der Grundlage einiger Hochrechnungen davon ausging, dass das Deep Web ungefähr 400- bis 550-mal so groß sein muss wie das Surface Web. Diese Annahme erschien deshalb glaubwürdig, da sie zu einer Zeit aufgestellt wurde, als Suchmaschinen weniger fortschrittlich waren, als sie es heute sind. Damals hatten Suchanfragen weit weniger Tiefgang, als es beim heutigen Stand der Entwicklung möglich ist [9]. Dennoch hat die Eisberg-Metapher immer noch großen Anklang und wird trotz falscher Zahlen immer wieder verwendet. Obwohl daher davon auszugehen ist, dass die Datenmenge des Deep Webs deutlich geringer ist, als in der Schätzung von BrightPlanet angegeben, kann trotzdem angenommen werden, dass sie deutlich größer ist als das Surface Web [16].

2.1.4 Dark Web, Darknet

Oftmals wird der Begriff „Deep Web“ fälschlicherweise als Synonym für das Darknet verwendet [18]. Während Darknets zwar einen Teil des Deep Webs darstellen, grenzt die Definition eines Darknets dieses jedoch klar vom Deep Web ab. Stefan Mey formulierte die Definition eines Darknets wie folgt: „Ein Darknet ist ein digitales Netz, das sich vom sonstigen Internet abschirmt und mit technologischen Mitteln die Anonymität seiner Nutzer herstellt. Wer Inhalte anbietet, wer mit wem kommuniziert und worüber, das alles wird mithilfe von Verschlüsselungstechnologien verschleiert“ [9]. Somit sind die Adressen innerhalb der Darknets nicht nur nicht indiziert, sondern ohne spezielle technische Maßnahmen auch dann nicht erreichbar, wenn man die Adresse kennt. Aus diesem Grund wird von einer Abschirmung vom restlichen Internet gesprochen. Diese Einteilung wird grafisch verdeutlicht in Abbildung 2: The Internet, the Deep Web, and the Dark Web, sowie in Tabelle 2: The Internet, the Deep Web, and the Dark Web.

[7] eine Übersicht über Leistungen, Standards und Technik vor allem zu IT-Themen

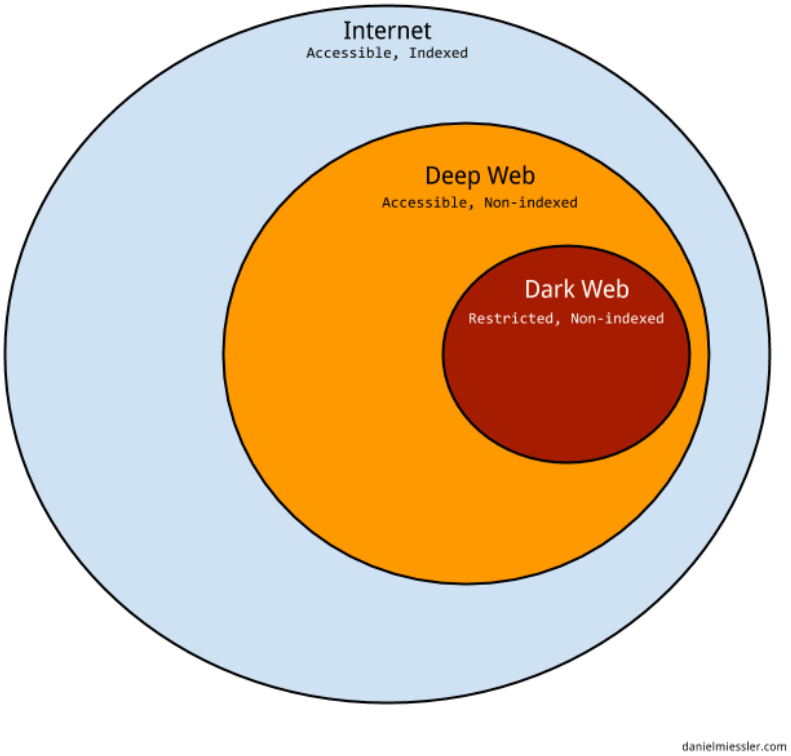

Abbildung 2: The Internet, the Deep Web, and the Dark Web
Quelle: https://danielmiessler.com/study/internet-deep-dark-web/ (abgerufen am 16.04.2018)

Internet Deep Web Dark Web	**Indexed**	**Non-indexed**
Restricted	--	Dark Web
Accessible	Internet	Deep Web

danielmiessler.com

Tabelle 2: The Internet, the Deep Web, and the Dark Web
Quelle: https://danielmiessler.com/study/internet-deep-dark-web/ (abgerufen am 16.04.2018)

Zugrunde liegt dieser Abschirmung in der Regeln eine VPN-Variante[8], welche um zusätzliche Maßnahmen erweitert wird [17]. Um welche Maßnahmen es sich dabei konkret handelt, variiert je nach Darknet. Auf diese Weise soll das Netzwerk an sich, sowie die IP-Adressen dessen Mitglieder verschleiert werden. Im Idealfall sollen Informationen ab-

[8] Virtual Private Networks

solut unerkannt ausgetauscht werden. Durch diese Vorkehrungen, wird jedoch die Geschwindigkeit, mit der Daten gesendet und empfangen werden können, deutlich verringert. Die wohl bekannteste Nutzung dieser Entwicklung ist das illegale Filesharing[9] von urheberrechtlich geschützten Inhalten, Raubkopien, Schadsoftware oder illegalen Inhalten. Jedoch ist dies nicht der Hauptzweck der Netzwerke. Ursprünglich waren die Darknets dazu gedacht, Raum für private Kommunikation zu schaffen, wenn öffentliche Kommunikation ein Risiko für das eigene Leben darstellt. Ein in der Öffentlichkeit bekanntgewordener Fall für diese Art der Nutzung war, als das Mubarak-Regime in Ägypten, 2011 das Internet im Land unzugänglich machte und Dissidenten das Darknet TOR verwendeten, um weiterhin mit der Außenwelt kommunizieren zu können [17]. In jüngerer Zeit werden Darknets ebenfalls genutzt, um Netzwerksicherheitstests durchzuführen. Dabei wird sich die Tatsache zu Nutze gemacht, das Darknets prinzipiell geroutete Zuweisungen eines IP-Adressraums sind. Administratoren reservieren sich einen ungenutzten Teil dieses IP-Adress-Segments und konfigurieren einen entsprechenden Dienst zu Überwachung des Datenverkehrs einer bestimmten IP-Adresse innerhalb dieses Netzwerkbereiches [17]. Der Begriff Darknet wird dabei sowohl als Sammelbegriff für die Gesamtheit aller Darknets verwendet, als auch als Bezeichnung für jedes Einzelne. Nimmt man diese Definition als Grundlage, kann folglich jeder mit entsprechenden technischen Ressourcen und Wissen ein eigenes Darknet aufbauen. Aus diesem Grund ist es unmöglich, genau zu sagen, wie viele Darknets es gibt, jedoch haben drei größerer Vertreter Bekanntheit erlangt. TOR als größtes bekanntes Darknet ist vor allem durch Medien vielen Menschen ein Begriff - wobei es oftmals als „Das Darknet“ bezeichnet wird. Trotz, oder gerade durch weniger Medienpräsenz haben sich jedoch auch Freenet und I2P als gängige Darknets durchgesetzt. Auf diese drei Hauptvertreter werde ich in dieser Arbeit besonders eingehen und Vergleiche bezüglich derer Nutzergruppen, Usability-Kriterien und Anonymisierungstechnologie ziehen.

2.2 Historische Einordnung

Ein gemeinsamer historischer Hintergrund für die Entstehung der Darknets lässt sich nur schwer finden, da sie sich sehr unabhängig voneinander entwickeln. Es lässt sich auch nicht mit genauer Sicherheit sagen, welches per Definition das erste Darknet war. Jedoch lassen sich alle Darknets auf den gemeinsamen Ursprung in der klassischen Kryptografie

[9] Deu.: Datenfreigabe, Datenaustausch

zurückführen. Kryptografie befasst sich mit der Verschlüsselung von Informationen, wird heutzutage jedoch oft allgemein als Bezeichnung für Informationssicherheit verwendet [18]. In „Eine kurze Geschichte der Kryptografie“ benennt Albrecht Beutelspacher das Hauptziel der Kryptografie als den Schutz der Kommunikation zwischen mehreren Personen vor Außenstehenden [19]. Dies deckt sich im Wesentlichen mit den Zielen der Darknets, wobei diese noch einen Schritt weitergehen, indem sie nicht nur Informationen verschlüsseln wollen, sondern versuchen, Nutzer zu anonymisieren. Viele frühe Verfahren der Verschlüsselungen entwickelten sich vor allem im militärischen und politischen Bereich. Dabei versucht man meist die Menge der zu verschlüsselnden Daten zu reduzieren, indem man so genannte Schlüssel einsetzt. Es gab jedoch auch früher schon Versuche, sich mit Hilfe der Kryptografie vor der Überwachung von Staaten zu schützen. Dieses Ziel spiegelt sich im Prinzip der anonymisierten Netzwerke besonders stark wieder. Innerhalb der Darknets kommt moderne Kryptografie vor allem bei der Verschlüsselung von Datenpaketen innerhalb des Netzwerkes zu tragen. Aber auch anonymisierte Bezahlverfahren innerhalb eines solchen Netzwerkes wie zum Beispiel die Bitcoin Zahlung über eine dritte Partei, wie es vor allem innerhalb des TOR-Netzwerks üblich ist, sind moderne Formen von Kryptografie. Ganz im Widerspruch zum Entzug aus staatlicher Aufsicht, verbindet jedoch auch der militärische Hintergrund die Kryptografie mit den Darknets. Insbesondere im Fall von TOR, da dieses Projekt seine Ursprünge im US-Verteidigungsministerium hat [20]. Neue Entwicklungen der Kryptografie werden vermutlich auch in Zukunft zu einer Weiterentwicklung der Darknet-Technologie führen, sowie Anwendungsprobleme der Darknets im Austausch zu neuen Errungenschaften der Kryptografie führen könnten.

2.3 Stand der Entwicklung

Wo die Entwicklung der Darknet-Technologie aktuell steht, ist nicht eindeutig festellbar, da es nicht nur ein großes Darknet gibt, sondern viele kleine. Diese sind komplett in sich geschlossen, voneinander getrennt und entwickeln sich komplett unabhängig voneinander- nicht nur Inhaltlich, sondern auch bei der Art von Verschlüsselungen und der Technik, die sie nutzen. Betrachtet man den aktuellen Entwicklungsstand der Darknets im Allgemeinen, soweit ersichtlich, so fällt zunächst eines besonders auf: In jedem Fall muss für deren Nutzung eine technische Grundlage geschaffen werden. Dies kann entweder ein spezieller Browser sein oder eine Veränderung des Standard-Internetbrowsers durch spezielle Software. Nur so kann die charakteristische Abschirmung gewährleistet werden.

Auch das grundlegende Verfahren zur Verschleierung von Identitäten und Informationen ist im Prinzip ähnlich. Informationen werden vom Absender in das Darknet geschickt, verschlüsselt und über mehrere, unabhängige Teilnehmer Knoten weitergeleitet, beim Zielknoten angekommen, werden sie wieder entschlüsselt und sind nun lesbar. Dabei ist zu bemerken, dsas die Informationen nur während der Weiterleitung durch das Darknet verschlüsselt sind, beim Empfänger und Sender jedoch im Klartext vorliegen. Besonders gut erkennbar ist dieses Prinzip bei der Dokumentations-Grafik von TOR, zu sehen im Abbildungsverzeichnis, Abbildung 5: How TOR works.

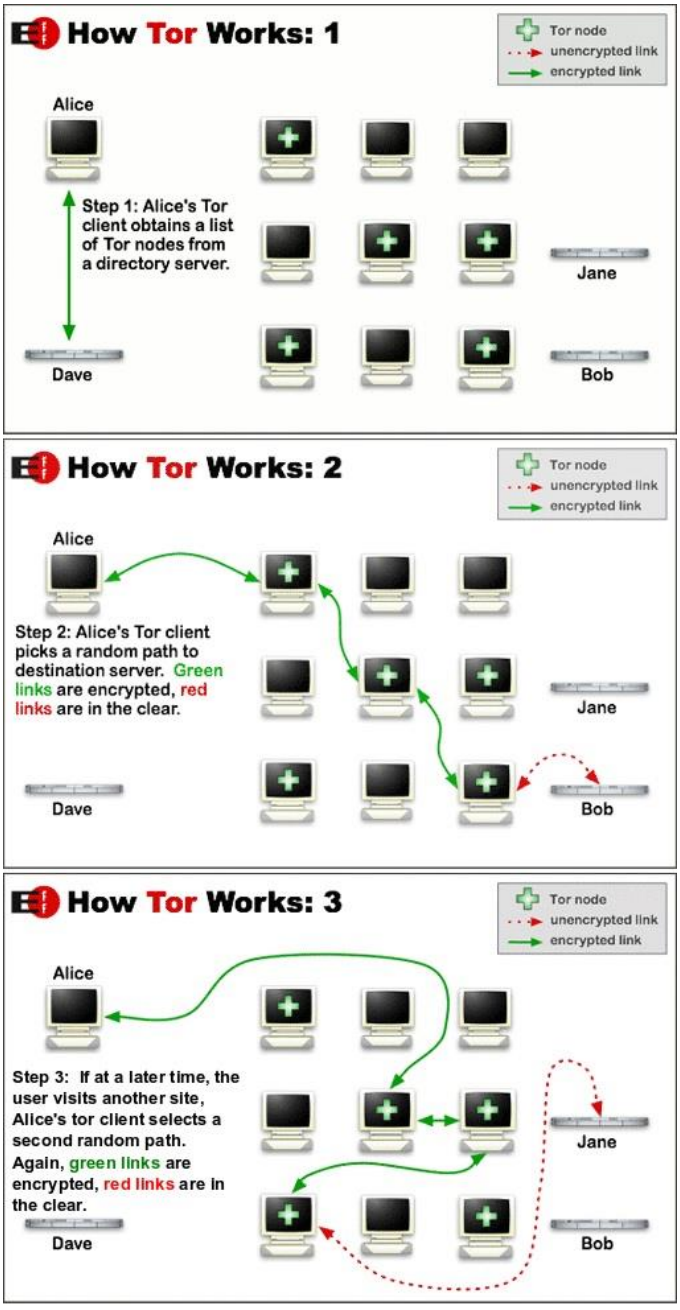

Abbildung 3: How TOR works

Quelle: https://www.torproject.org/images/htw1.png
https://www.torproject.org/images/htw2.png
https://www.torproject.org/images/htw3.png (abgerufen am 22.03.2018)

Ein weiterer großer Angriffspunkt der über Darknets verschlüsselten Kommunikation ist das Abfangen der Informationen, bevor oder nachdem sie verschlüsselt wurden [21]. Doch auch die Verschlüsselung innerhalb der Darknets ist nicht unantastbar. Zum aktuellen Zeitpunkt gibt es zwei bekannte Verfahren, mit denen sich die Anonymität des Darknets angreifen lässt. Beide Methoden wurden in Deutschland entwickelt und getestet. Die erste Variante basiert auf der Idee einer flächendeckenden Überwachung und ist vor allem dann nützlich, wenn es weniger um die verschlüsselten Inhalte an sich, als vielmehr um die Metadaten, also welcher Sender mit welchem Empfänger wann und wie oft kommunizierte. Es wird vorgesehen, dass alle Knotenpunkte eines Darknets überwacht werden. Dadurch wird sichtbar, wie die verschlüsselten Datenpakete durch das Netzwerk wandern. Auf diese Weise wird nicht nur die verschlüsselte Information aufgedeckt, sondern der komplette Verschleierungsprozess überwacht [22]. Diese Technik wird deshalb nicht dauerhaft verwendet, da der Aufwand und die Kosten in keinem Verhältnis zum erzielten Nutzen stehen. Um ein Netzwerk mit ähnlichen Ausmaßen wie TOR, ca. 7000 Server, auf diese Weise überwachen zu können, werden enorme Ressourcen verlangt [22]. Dennoch veröffentlichte das Portal netzpolitik.org einen Artikel, der auf zukünftige, praktische Anwendungen des Verfahrens hinweist. Demnach habe der Bundesnachrichtendienst schon im Jahr 2008, Geheimdienste anderer Länder über die Methode unterrichtet und Pläne zur Anwendung auf das Darknet TOR verfasst. Im Zuge dieser Recherche wurde außerdem davon berichtet, dass mehrere TOR-Server von Geheimdiensten betrieben und somit eine solche Überwachung vereinfachen würden [23]. Der zweite Ansatz zur Überwachung der Darknet-Kommunikation beruht auf der bereits zuvor genannten Schwachstelle, dass eine Verschlüsselung nur innerhalb des Netzwerks erfolgt. Dabei soll das Gerät des Nutzers direkt, durch Schadsoftware angegriffen werden. Dieses Verfahren nennt sich „Quellen-Telekommunikationsüberwachung“ Dabei wird ein Trojaner auf das Endgerät vermeintlicher Nutzer geschleust, um Informationen noch vor der Verschlüsselung abzufangen. Dadurch können zum Beispiel Screenshots vom Bildschirm des Nutzers gemacht werden oder komplette Tastenanschläge übermittelt werden ohne Wissen des Nutzers. Diese Methode stößt innerhalb Deutschlands jedoch deshalb an Grenzen, da sie Menschenrechte verletzt [24]. Jedoch greift dieses Argument längst nicht überall auf der

Welt. Mithilfe dieser Technik wurde 2012 eine Gruppe Dissidenten[10] in Marokko überführt und verfolgt, da sie einen regierungskritischen Blog namens „Mamfakinch“[11] betrieben [25]. Diese Beispiele zeigen, dass auch die Darknets beim heutigen Stand der Technik keine hundertprozentige Anonymität bieten können. Außerdem zeigen solche Fälle gut auf, wie es um den aktuellen Stand der Entwicklung aus politischer Sichtweise steht. Es entsteht ein Interessenkampf zwischen Sicherheit und persönlichem Freiraum. Matthias Schulze benennt dieses Problem sehr treffend in seinem Artikel „Going Dark?“. „Entweder fördert man eine starke Verschlüsselung, die Schutz vor Hackern bietet aber auch die Nutzung durch Terroristen ermöglicht; oder man nutzt schwächere Verschlüsselungstechnologien, um Terroristen überwachen zu können mit der Folge eines geringeren Sicherheitsniveaus gegen Hacker und Cyberangriffe“ [26].

2.4 Usability-Kriterien bezüglich Darknets

Um sich mit dem Usability-Faktor der einzelnen Darknets genauer befassen zu können, muss zunächst definiert werden, was genau unter Usability zu verstehen ist und welche Kriterien für diesen speziellen Anwendungsfall relevant sind. Usability befasst sich im Wesentlichen mit der Nutzungsfreundlichkeit bestimmter Anwendungen, Portale oder Produkte [27]. Dementsprechend müssen die Kriterien von Fall zu Fall angepasst und abgewogen werden. Im besonderen Fall der Darknets handelt es sich um eine Kombination aus Software und Verfahren. Dies setzt sich aus den speziellen Browser-Konfigurationen eines Darknets zusammen, sowie der Nutzung dieser, um Anonymität zu wahren, denn auch hier können Fehler gemacht werden. Wirft man einen Blick auf den Usability-Katalog[12] einer Webseite zum Beispiel, so findet man vorwiegend Punkte, die sich mit der Navigation innerhalb der Seite beschäftigen [28]. Dieses Prinzip kann teilweise auch für Darknets übernommen werden, da ein Großteil der Anwendung darin besteht, durch die Inhalte des Netzwerks, mit Hilfe des konfigurierten Browsers zu navigieren. Skoposnova beschäftigen sich auf ihrer Webseite mit Usability Kriterien für Webseiten, Produkte und Apps und stellen für jeden Fall einen Plan zur Ermittlung relevanter Kriterien bereit [29]. Bei genauerer Betrachtung fällt auf, dass Kriterien dann als relevant eingestuft wer-

[10] Von lat. Dissidere, auseinander sitzen, nicht übereinstimmen, in Widerspruch stehen

[11] Zu Deutsch: „Wir geben nicht auf“

[12] Liste gültiger Usability-Kriterien für einen bestimmten Anwendungsfall

den, wenn sie potentiell bekannte Nutzerprobleme ansprechen. Wendet man diese Vorgehensweise auf das Problem der Darknets an, ergeben sich folgende Usability-Kriterien, die es zu untersuchen gilt:

- Wie schwierig ist die technische Vorbereitung?
    - Lässt sich die Software einfach beschaffen?
    - Installation der Software
    - Einstellungen zur korrekten Nutzung
    - Navigation innerhalb der Optionen
- Nutzung der Darknets
    - Ist das Netzwerk sofort zugänglich?
    - Navigation innerhalb des Netzwerks
    - Anonymität
    - Rechtliche Risiken durch die Nutzung
- Deinstallation bzw. Abschalten der Software

Diese Qualitätsmerkmale werden bei den Vertretern The TOR Project, Invisible Internet Project und Freenet untersucht, um einen Vergleich der Nutzerfreundlichkeit ziehen zu können.

2.5 Anonymität und Online-Anonymität

„Anonymität bedeutet, dass eine Person oder eine Gruppe nicht identifiziert werden kann“ [30]. Sucht man im Duden nach dem Wort, so findet man die Definition: das Nichtbekanntsein, Nichtgenanntsein; Namenlosigkeit. Diese Eigenschaften sind es, die Anonymität auszeichnen. Dabei kommt sie bewusst, unbewusst, gewollt oder auch ungewollt in allen möglichen Bereichen unseres Lebens zum Tragen. Dabei ist Anonymität nicht immer absolut. Manchmal wird nur eine der Definitionen erfüllt, dennoch ist dadurch eine gewisse Anonymisierung gegeben. Ein Beispiel für solch eine abgeschwächte Anonymität wäre ein Einkauf im Supermarkt mit Barzahlung. Der Betroffene wählt seine Ware, geht an die Kasse und zahlt in bar. Dabei ist weder dem Kassierer, dem Ladenbesitzer

oder dem Hersteller des Produktes der Name des Käufers bekannt. Somit ist dieser namenslos, eine Form der Anonymität. Dennoch ist der Käufer nicht unerkannt, somit nicht absolut anonym [31]. Daran ist zu erkennen, dass es mehrere Stufen der Anonymität gibt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht diese Abstufungen ganz konkret in den drei Definitionen des Dudens [31]. Eine andere Definition für Anonymität ist das Fehlen einer Identität. Hierfür führt das BSI eine auf Marx gestützte Liste von Kriterien auf, die erfüllt sein müssen, damit eine Identität als nicht vorhanden zählt und somit Anonymität gewährleistet. Demnach müssen gesetzlicher Name, Adresse, alphanumerische Nummer wie zum Beispiel eine Ausweiß-ID, Pseudonyme, Verhaltensmuster, soziale Kategorisierung und Zertifikate zur Bestätigung einer Identität unbekannt sein, um als anonym zu gelten [31]. Es treten jedoch auch Szenarien auf, in denen die Identität einer Person nur vor bestimmten Menschen anonym gehalten werden soll, jedoch nicht vor allen Personen. Ein Beispiel hierfür sind Kundenkontos bei Online-Shops. Shop-Mitarbeiter dürfen den Namen eines Kunden zum Beispiel durchaus kennen, während dieser für andere Kunden des Online-Shops anonym bleibt. Dieses Beispiel fällt in den Bereich Online-Anonymität. Dieser Teilabschnitt ist es, der für die Thematik der Darknets eine wichtige Rolle spielt und eine Anpassung der Definition verlangt, da online Faktoren wie IP-Adresse, Nicknames[13], E-mai-Adressen und Verhaltensmuster eine größere Rolle spielen als die klassischen Kriterien der Anonymität. Dabei hinterlassen die meisten Nutzer unbewusst Spuren, durch die ihre Identität im Internet preisgegeben wird. Gleichzeitig gibt es eine Reihe technischer Hilfsmittel um Internet-Identitäten konkret aufzudecken. Dazu gehört zum Beispiel das Abhören von Datenverkehr - wobei es sich selbstverständlich nicht um das Abhören im wörtlichen Sinne handelt. Dabei lesen beispielsweise Internetprovider oder auch Firmennetzwerkbetreiber den Datenverkehr unverschlüsselt mit. Eine weitere Methode wäre das Cookie-Tracking. Viele Internetseiten weisen die Nutzer darauf hin, dass sie Cookies verwenden. Diese können verwendet werden, um den Nutzer zu markieren und später wieder zu erkennen. Wurden auf der entsprechenden Webseite personenbezogene Daten in Form von Kundendaten oder ähnliches hinterlegt, ist unsere Identität damit sofort bekannt, wenn wir die Seite erneut betreten [32] - folglich ist Anonymität nicht mehr gewährleistet. Dabei ist es für Laien nahezu unmöglich, Anonymität im Surface Web zu wahren. Deutlich leichter ist dies im Darknet. Hier erleichtern die internen Verschlüsselungen und die spezielle Form der Datenweiterleitung die Anonymisierung. Jedoch können sich Nutzer immer noch durch ihr Verhalten

[13] Nutzernamen, die als pseudonyme online verwendet werden

oder Nutzerkonten enttarnen. Online-Anonymität ist also nicht ausschließlich durch technische Hilfsmittel zu erlangen, sondern verlangt nach einer Kombination aus technischen Vorkehrungen und überlegtem Verhalten.

3 Grundlagen und Methodik

Nachdem alle relevanten Definitionen und Begriffe geklärt sind, kann im nächsten Schritt der konkrete Vergleich der Darknets TOR, I2P und Freenet erfolgen. Hier werden alle drei Vertreter, hinsichtlich der gleichen Kriterien, nacheinander betrachtet. Aufbauend auf diesen Informationen kann schließlich eine Kurzfassung inklusive Nutzeranleitung erstellt werden. Dabei werden die Applikationen für mobile Endgeräte unter IOS und Android außer Acht gelassen, da diese keine direkten Darknet-Zugänge anbieten, sondern den Nutzern lediglich einige Anonymisierungswerkzeuge bieten.

3.1 TOR

„The Onion Routing Project“, kurz TOR ist das wohl bekannteste und medienstärkste Darknet der heutigen Zeit. Oftmals wird es als „das Darknet“ bezeichnet. Dabei handelt es sich um einen Zusammenschluss aus freiwillig betriebenen Servern. Dieser Zusammenschluss wird durch Einzelpersonen erweitert, indem diese sich über virtuelle Tunnel mit dem Netzwerk verbinden. Auf diese Weise lebt das Netzwerk von seinen Nutzern. Das Projekt ist in der heutigen Zeit vor allem dazu gedacht, Nutzern und Organisationen die Möglichkeit zu geben, Informationen ohne Zensur und anonym austauschen zu können. Es soll eine Möglichkeit bieten, Blockaden im Internet zu umgehen und als Entwicklungsbaustein für anonyme Kommunikationssoftware genutzt werden. Dies sind die Ziele der Mitwirkenden des TOR-Projekts [33]. Jedoch ist das TOR-Darknet wesentlich kleiner, als der Medientrubel darum vermuten lässt. Jedoch ist es mit geschätzten 50.000 Adressen[14] noch größer als seine beiden Konkurrenten. Dies sind Adressen mit dem Anhang „.onion“, welche sie als Darknetseiten innerhalb von TOR ausweisen. Allerdings haben Studien ergeben, dass weniger als 10.000 dieser Seiten tatsächlich vom Browser ansteuerbare Inhalte enthalten [34]. Laut TOR-Project nutzen ca. 2,5 Millionen Menschen täglich das Netzwerk, wobei etwa acht Prozent aus Deutschland stammen [35]. Nicht verfolgen lässt sich allerdings, wie viele dieser Nutzer tatsächlich „.onion“-Adressen besuchen und wie viele nur anonym im Surface-Web unterwegs sind. Zieht man jedoch alle Schätzungen des TOR-Projekts in Betracht, gibt es zusammengefasst deutlich weniger als 100.000 TOR-Nutzer, also Nutzer die tatsächlich „.onion“-Adressen ansteuern, innerhalb des Netzwerks [34]. Inhaltliche Vielfalt findet sich innerhalb des TOR-Darknets vor

[14] Stand Oktober 2017

allem auf der illegalen Seite des Netzwerks. Besonders nennenswert ist hierbei die Vielzahl an illegalen, jedoch professionell betriebenen Marktplätzen. Ähnlich wie bei dem Darknet-Vertreter Freenet, finden sich auch hier eine beachtliche Anzahl an Diskussionsforen und Blogs. Ein zweiter, verbreiteter Verwendungszweck der TOR Software ist der Einsatz als Programmbaustein. Die Programme, die dabei entstehen, sind vorwiegend speziell für den TOR-Browser. Ein bekanntes Beispiel hierfür ist Onion-Share [36] - ein File-Sharing Programm, welches kurzzeitig eine „.onion"-Adresse erstellt, von der aus Nutzer eine Datei herunterladen können, anschließend wird die Seite wieder gelöscht. Eine weitaus legalere Nutzung bietet die dritte Kategorie der TOR-Anwendungen als alternativer Zugang. Wie zuvor bereits erwähnt, nutzen Anbieter wie Facebook, Heise-Online oder auch der Chaos Computer Club das Darknet als anonymen Zugang zu ihren Portalen. Dies ist besonders dann interessant, wenn es darum geht, Zensur oder Überwachung von Kommunikationsmedien zu umgehen. Diese Funktion wird sich für verschiedenste Zwecke von den unterschiedlichsten Gruppierungen zu Nutze gemacht.

3.1.1 Geschichtliche Hintergründe

Der Name „The Onion Router" oder auch „The Onion Routing Project" stammt von einem Vergleich dieser Technologie mit einer Zwiebel. Dieser zunächst befremdlich wirkende Vergleich wurde gezogen, da sich die Identität des Nutzers unter mehreren Anonymisierungsschichten versteckt [37]. Die Entstehungsgeschichte von TOR steht dabei in einem besonderen Kontrast zu der heutigen Nutzung und den Zielen des Projekts. Die Technologie, die TOR zugrunde liegt, wurde 1995 von Paul Syverson, einem Mathematiker und Urheber des Zwiebel-Vergleiches, entwickelt. Er forschte während der Entstehungszeit dieser Technologie für eine Forschungsabteilung des US-Verteidigungsministeriums [20]. Später zum Projekt hinzu kam Roger Dingledine, welcher dazu beitrug, dass die Technologie einem weiteren Personenkreis zur Verfügung gestellt wurde und zur heutigen Zeit das öffentliche Gesicht von TOR ist. Die Begründung für diesen Schritt lag nah, da die Technologie als Anonymisierungsmaßnahme nicht funktioniert hätte, würde sie nur von einer Personengruppe genutzt werden. Sobald eine Verbindung aufgebaut wird, wäre offensichtlich gewesen, dass es sich um einen CIA-Agenten handelte. Durch die Nutzung der Software in mehreren Bevölkerungsschichten wurde ein so genannter „Cover Traffic[15]" erzielt. Das bedeutet: die Masse an unterschiedlichsten Nutzern komplettiert die Anonymisierung erst [20]. Im Jahr 2000 wurde aus der technologischen

[15] Deutsch: Verschleiernder Datenverkehr

Grundlage das eigentliche TOR-Projekt. Jedoch waren die ersten Ansätze rein theoretischer Natur, bis 2002 die ersten Umsetzungen erfolgten. Dies geschah an der Universität Cambridge durch Matej Pfajfar [43]. Bereits 2003 wurde das TOR-Netzwerk daraufhin für externe Knoten freigegeben und der Quellcode der Software unter einer Open-Source-Lizenz freigegeben [20]. Bis 2004 lief die Entwicklung weiter unter Paul Syverson und wurde unterstützt durch die ONR[16] und die DARPA[17]. Letzten Endes wurde das TOR-Projekt 2006 als formal unabhängige, nicht profitorientere Organisation gegründet. Aktuell ist TOR in erster Linie ein großes Open-Source-Projekt, an dem sich viele Menschen aus unterschiedlichen sozialen Schichten und Gründen beteiligen. Dabei wird jedoch unterschieden, zwischen „Core Tor People", also den Kernmitgliedern des Projekts und freiwilligen Helfern. Die Kernmitglieder sind auf der Internetseite des TOR-Projektes aufgelistet und haben jeweils eine feste Position inne, während freiwillige Helfer selbst entscheiden, was und wie viel sie beisteuern möchten. Freiwillige, die besonders hilfreiche Beträge beigesteuert haben, werden ebenfalls auf der Projekt-Seite aufgelistet und entweder mit ihrem echten Namen oder aber einem gewählten Pseudonym genannt.

3.1.2 Finanzierung & Organisation

Ein Blick auf die Onlinepräsenz des TOR-Projekts[18] verrät bereits, dass ein Teil der Finanzierungsgelder durch Spenden zusammengetragen wird. Unter den Navigationspunkten „About Tor" und „Sponsors", steht öffentlich einsehbar eine Liste von früheren und aktuellen Sponsoren bereit [38]. Doch trotz aller formaler Abgrenzung des Tor-Projekts von seinen Ursprüngen, wird es zu einem großen Teil nach wie vor mit Forschungsgeldern der US-Regierung finanziert [20]. Dem Finanzbericht des Projekts aus dem Jahr 2015 ist zu entnehmen, dass in diesem Jahr ein Budget von 3,3 Millionen Dollar zur Verfügung stand [39]. Dabei setzt diese Summe sich auch weitaus weniger aus Spenden als aus Regierungsgeldern zusammen. Die Aufschlüsselung dieser Finanzen ist veranschaulicht zu sehen im Abbildungsverzeichnis, Abbildung 6: Budget-Zusammensetzung TOR 2015.

[16] Office of Naval Research (deu.: Büro der Marineforschung)

[17] Defense Advanced Research Projects Agency (deu.: Agentur für Forschung im Bereich der Verteidigung)

[18] www.torproject.org

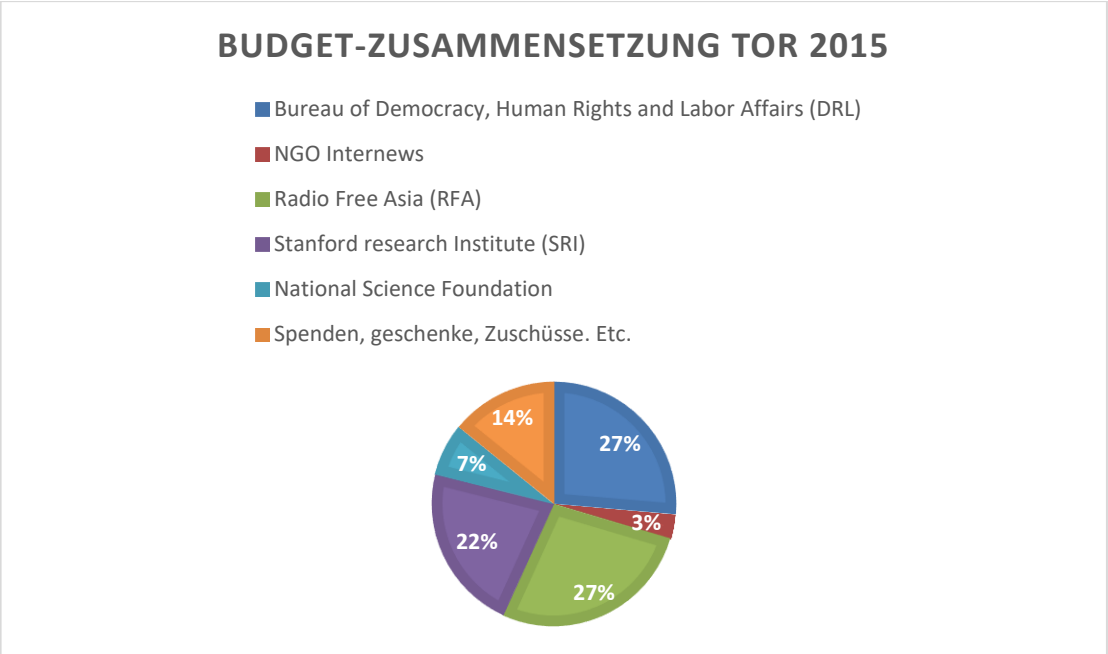

Abbildung 4: Budget-Zusammensetzung TOR 2015

Mit Hilfe des Diagramms dargestellt, ist zu sehen, dass 29% der Gelder vom US-Außenministerium stammen, Zusammengesetzt durch 857.515 Dollar vom DRL[19] und 104.540 Dollar der NGO Internews, wobei es sich hierbei ebenfalls um weitergeleitete Zuschüsse des DRL handelt. Von einem staatlichen Auslandssender, dem Radio Free Asia (RFA) erhielt TOR 886.724 Dollar. RFA wurde ursprünglich von der CIA gegründet und im kalten Krieg verwendet, bevor er auf eine eigenständige Rundfunkbehörde überging. Weitere 719.500 Dollar stammten aus dem Stanford Research Institute, welches zwar eine unabhängige Forschungseinrichtung ist, aber zwei Drittel seiner Gelder vom US-Verteidigungsministerium bezieht. Die restlichen 460.298 Dollar stammten aus anderen Quellen [40]. Roger Dingledine selbst schätzt den Teil von staatlichen Geldern innerhalb des Tor-Budgets auf 80-90% [20]. Diese regierungsstarke Förderung bringt sowohl Vor- als auch Nachteile für das Projekt mit sich. Durch diese starke Unterstützung, steht TOR genug Budget zur Verfügung, um sich feste Angestellte zu leisten. 2015 hatte das Tor-Projekt zehn Festangestellte, die teilweise Gehälter bis 135.000 Dollar im Jahr erhielten [20]. Durch diese vollberufliche Unterstützung und die gute finanzielle Lage ist es TOR möglich, sich stetig weiter zu entwickeln und zu wachsen. Zusätzlich zu gutem Budget

[19] Bureau of Democracy, Human Rights and Labor Affairs (Deutsch.: Büro für Demokratie, Menschenrechte und Arbeitsangelegenheiten)

und festen Mitarbeitern kommen die zahlreichen freiwilligen Helfer sowie Organisationen und Gruppen, die in eigenem Interesse Werbung für das Projekt betreiben. Zum aktuellen Zeitpunkt wirken an Tor 62 Kernmitglieder mit [41]. Die Zahl der sonstigen Freiwilligen ist ungewiss. Besonderen Stellenwert nehmen dabei Personen ein, die nicht nur an Tors Infrastruktur und konstruktiven Inhalten mitwirken, sondern auch Tor-spezifische Anwendungen entwickeln und zur Verfügung stellen. Jeder Nutzer von TOR kann potenziell zum Ausbau des Netzwerks beitragen, indem er Datenverkehr für Dritte weiterleitet, also als Datentransfer-Knoten im Netz dient. Jedoch ist diese Funktion nicht automatisch Pflicht und kann abgestellt werden. Die Schattenseite dieser Art der Regierungsförderung und Tors Entstehungsgeschichte ist, dass regierungsnahe Einrichtungen tiefgehendes Wissen über die Funktionsweise der Anonymisierungstechnologie haben und man sich so fragen muss, wie sicher diese wirklich sind.

3.1.3 Funktionsweise

Um TOR nutzen zu können, müssen zunächst einmal die technischen Grundbedingungen geschaffen werden. In diesem Fall bedeutet das mindestens, den TOR-Browser herunterzuladen und zu installieren. Ein Alleinstellungsmerkmal dieses Darknets ist, dass es einen komplett eigenständigen Browser zur Verfügung stellt, während üblicherweise lediglich eine Software verwendet wird, die den bereits vorhandenen Internetbrowser so modifiziert, dass er Zugang zum jeweiligen Darknet erhält. In einigen Anleitungen wird dazu geraten, sich neben dem Browser auch noch ein angepasstes Betriebssystem zu installieren, dies ist jedoch nicht notwendig. Es handelt sich dabei lediglich um eine weitere, persönliche Schutzmaßnahme vor Schadsoftware.

Der TOR-Browser beruht auf dem Firefox-Browser und ist in seiner Menüführung und Handhabung dem Original sehr ähnlich. Dadurch fällt es vielen Nutzern leicht, einen Einstieg in dessen Nutzung zu finden. Mit Hilfe des Browser lassen sich nicht nur die TOR-spezifischen Webseiten mit der Endung „.onion“ aufrufen, sondern es ist dem Nutzer auch möglich, anonym auf Seiten des normalen Internets zu surfen.

Um diese Anonymisierung zu gewährleisten, soll zum einen verhindert werden, dass eine Analyse des Datenverkehrs erfolgen kann. Das bedeutet, es darf nicht ersichtlich sein, wer mit wem kommuniziert und wie häufig. Um dieses Ziel zu erreichen, wird jede Verbindung auf mehrere Punkte, sogenannte Knoten, im Netzwerk verteilt, sodass niemals eine einzelne Verbindung zum Ziel führen kann. Im Vergleich dazu wird im herkömmli-

chen Internet stets eine direkte Verbindung zum Ziel aufgebaut, um eine schnelle Kommunikation zu ermöglichen. Gut sichtbar wird diese Gegenüberstellung in Abbildung 7: Wie funktioniert Tor?, im Abbildungsverzeichnis.

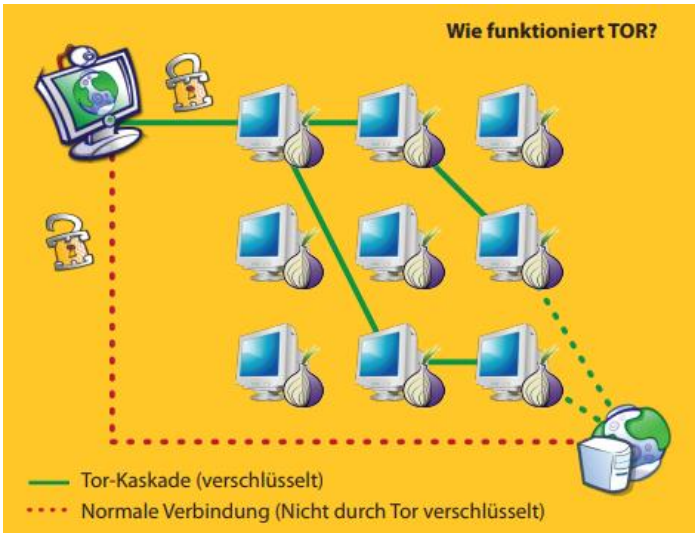

Abbildung 5: Wie funktioniert TOR?
Quelle: Anonymität im Netz mit Tor, Flyer des Chaos Computer Clubs, August 2010

Die Pfade, also über welche Knoten die Verbindungen gelenkt werden, werden zufällig immer wieder neu gebildet. Zusätzlich werden Hinweise darüber, von welchem Knoten ein Datenpaket kam und zu welchem Knoten es weitergeleitet wurde, verschleiert. Besonders wichtig für diesen Vorgang ist, dass der Pfad immer nur um einen Schritt erweitert wird. Jeder Knoten kann nachvollziehen, von welchem anderen Knoten im Netzwerk ein Datenpaket ankommt und an welchen es weitergegeben wird, jedoch kann kein Knoten die Schritte, die davor oder anschließend geschehen, rekonstruieren. Somit kennt jeder Knoten nur seinen direkten nächsten Nachbarn während eines Datentransfers und niemals den ganzen Pfad eines Datenpakets. Um sicherzustellen, dass die Verbindungen von keinem Knoten nachvollzogen werden kann, werden bei jedem Schritt, also jedem Datentransfer von einem Knoten zum nächsten, separate Verschlüsselungs-Schlüssel ausgegeben [42]. Charakteristisch für TOR ist hierbei, dass Jede Verbindung über drei verschiedene Knoten geleitet wird. Somit ist jedes Datenpaket dreimal verschlüsselt. Hier greift der berühmte Vergleich mit der Zwiebel. Dabei stellt den Kern der Zwiebel die eigentliche Nachricht dar und die Schichten sind die jeweils verschleierten Knoten-Adressen auf dem Pfad der Nachricht [43].

Sobald eine dieser zufälligen Verbindungspfade erstellt wurde, kann er für 10 Minuten genutzt werden, bevor TOR eine neue Verbindungsstrecke festlegt [42]. Die reine TOR-

Technologie, also das Verfahren ohne die speziellen Eigenschaften des TOR-Browsers, fokussiert sich dabei ausschließlich auf sicheren Datenverkehr. Der Browser selbst ist es, der Software zum Beispiel in Form von Verbindungsprotokollen einsetzt, um persönliche Informationen zu verschleiern [44].

Der Nutzer selbst muss letzten Endes jedoch dafür sorgen, dass er seine Identität nicht verrät indem er Daten wie Name oder Adresse preisgibt.

3.1.4 Wer nutzt TOR?

Prinzipiell ist TOR für jeden Menschen mit einem Computer und Internetzugang frei nutzbar. Im Grundgedanken soll das Netzwerk jeden Nutzer vor Missbrauch persönlicher Daten, Überwachung und Zensur schützen, sowie es ermöglichen, sich anonym im Netz zu bewegen und unter Wahrung der Privatsphäre zu kommunizieren. Allerdings haben sich einige Nutzergruppen besonders herauskristallisiert und werden, sofern sie sich zu erkennen geben, durch die TOR-Metrics statistisch festgehalten.

Journalisten bilden eine dieser besonderen Nutzergruppen, da die Freiheit der Medien nicht überall auf der Welt gegeben ist. Das Netzwerk soll Journalisten ermöglichen, ohne Angst vor Konsequenzen Bericht erstatten und mit der Außenwelt kommunizieren zu können. Das bringt mit sich, dass auch jene, die an diesen Berichten interessiert sind, TOR nutzen [45]. Hier fällt es oft schwer, noch eine Grenze zwischen Journalisten, Dissidenten und Whistleblowern[20] zu ziehen. Oftmals verschwimmen diese Nutzergruppen für Leser, insbesondere, da all diese Gruppen im TOR-Darknet stark vertreten sind. Aus ganz ähnlichen Gründen verwenden viele Blogger TOR, und auch Aktivisten nutzen das Netzwerk, um sich eine Online-Präsenz aufzubauen. Da TOR das mit Abstand größte Darknet ist und viele Nutzer erreicht, zieht es gerade diese auf Publikum angewiesenen Nutzergruppen zu speziell dem TOR-Darknet. Eine Nutzergruppe, die eher selten mit dem Darknet in Verbindung gebracht wird, sind Polizisten und Sicherheitskräfte. Diese nutzen TOR verstärkt, um während Undercover Aktionen ihre falsche Identität zu wahren und um illegale Geschäfte aushebeln zu können [46]. TOR wird daher benutzt, da sich besonders hier eine starke Vielfalt illegaler Marktplätze und Tauschbörsen errichtet hat. Händler illegaler Waren und Substanzen sind ebenfalls eine besonders große Partei des TOR-Netzwerks, da die hier gebotene Anonymität eine Strafverfolgung oder Aufdeckung

[20] eine Person, die für die Allgemeinheit wichtige Informationen aus einem geheimen oder geschützten Zusammenhang an die Öffentlichkeit bringt. (Deutsch: Hinweisgeber oder Enthüller)

ihrer Identität erschwert. Da TOR im Gegensatz zu anderen Darknets bessere Möglichkeiten der multimedialen Kommunikation bietet, zieht es auch diese Nutzergruppe stärker an. Doch ebenfalls Militärs und Menschen aus Kriegs- oder Krisengebieten nutzen TOR um eine Kommunikation mit der Außenwelt aufrecht zu erhalten, wenn das Internet keine sicheren Kanäle bietet.

Im Vergleich zu anderen Vertretern, bietet TOR die größte Nutzervielfalt, was nicht zuletzt daran liegt, dass es durch Medien, gute Finanzierung und Unterstützung den größten Bekanntheitsgrad errungen hat.

3.1.5 Usability-Einschätzung

Ebenfalls der großen Bekanntheit TORs zuzuschreiben ist die Tatsache, dass die Software sehr leicht zu finden ist. Neben dem Download auf der Seite des Projektes selbst bieten zahlreiche andere Downloadseiten wie zum Beispiel Chip, Heise oder Computerbild den TOR-Browser an. Somit sollte jeder Interessant ein Downloadportal seines Vertrauens finden können.

Auch die Installation des Browsers gestaltet sich relativ simpel. Der Download enthält eine Anwendung, welche das Installationsprogramm öffnet. Daraufhin wird der Nutzer gebeten, eine Sprache und ein Zielverzeichnis auszuwählen. Sobald der Installationsprozess abgeschlossen ist, kann der Browser gestartet werden. Beim ersten Start wird der Nutzer gefragt, ob eine direkte Verbindung aufgebaut werden soll oder ob zuvor Konfigurationen vorgenommen werden sollen [Abbildung 8: Erste Verbindung mit TOR].

Abbildung 6: Erste Verbindung mit TOR

Dabei leitet die Anwendung den Nutzer mit kurzen Erklärungstexten an, so dass auch Personen ohne großes Vorwissen Konfigurationen durchführen können. Entscheidet man sich für eine Konfiguration, so erhält man die Möglichkeit, eine alternative Verbindung zu wählen, falls TOR im eigenen Land blockiert wird, oder einen Proxy[21] einzustellen, falls dies benötigt wird. Wählt der Nutzer direkt die Option „Verbinden“ aus, so baut die Anwendung binnen weniger Sekunden eine Verbindung zum TOR-Netzwerk auf und öffnet den eigentlichen Browser. Damit ist der Installationsprozess bereits abgeschlossen. Einen Blick auf die Startseite des Browsers und dessen Interface [Abbildung 9: Startseite TOR-Browser] zeigt bereits deutliche Ähnlichkeiten zum aktuellen Firefox-Browser [Abbildung 10].

Abbildung 9: **Startseite TOR-Browser**

[21] ein Vermittler in Computernetzwerken (deu.: Stellvertreter)

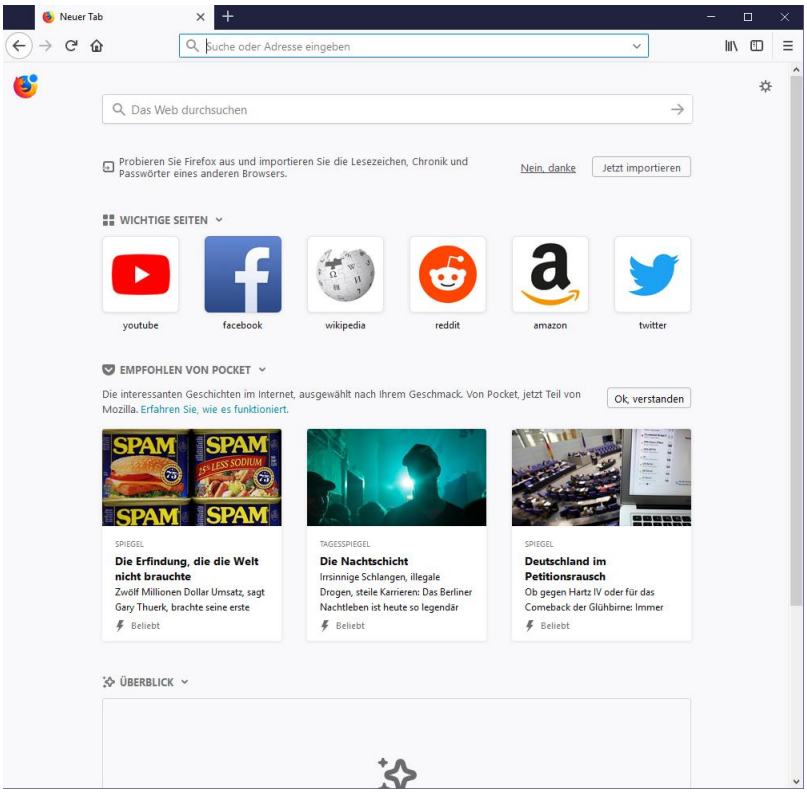

Abbildung 10: Startseite Firefox-Browser

Die Lage der Menü-Buttons und die generelle Anordnung des Interfaces ist nahezu identisch. Dies ermöglicht einer großen Anzahl von Nutzern den Einstieg in den Umgang mit der Software. Insbesondere was die Einstellungsoptionen angeht, hilft die Orientierung an der bekannten Vorlage. Neue Menü-Optionen finden sich lediglich im Bereich der Identitäts- und Kanalverwaltung TORs, welche unter dem Zwiebelsymbol in der linken oberen Ecke zu finden sind. Der normale Nutzer muss jedoch kaum von den vordefinierten Einstellungen abweichen.

Nach der Installation und gegebenenfalls der Anpassung einiger Einstellungen ist das TOR-Darknet jederzeit über den Browser zugänglich und erreichbar. Dank der TOR-Spezifischen Endung „.onion“, ist dem Nutzer zu jeder Zeit klar verdeutlicht, ob er sich anonym auf einer frei zugänglichen Webseite aufhält oder eine Darknet-Seite besucht. Sofern man sich durch das offene Internet mit Hilfe der Anonymisierungsverfahren des Tor-Browsers navigieren möchte, so ist dies kaum anders, als das Surfen im normalen Internetbrowser. Lediglich die Geschwindigkeit, mit der diese Seiten aufgerufen werden, ist etwas ist langsamer als üblich. Die Navigation im eigentlichen Sinne, stellt jedoch kein Problem dar. Anders verhält es sich bei der Navigation durch die Darknet-Seiten. Zwar

gibt es im TOR-Netzwerk einige Ansätze für Suchmaschinen, so zum Beispiel „Duck-DuckGo“, jedoch liefern diese nur mäßige Erfolge, da viele „.onion“-Seiten inaktiv sind und nicht mehr gepflegt werden. Der Hauptteil der Navigation findet hier über Link-Listen statt, also online einsehbare Listen, die Links zu Webseiten enthalten und kategorisch untergliedert sind. Der Überblick und die Ordnung sind hier deutlich geringer, als es bei Freenet der Fall ist. Viele Seiten sind nicht erfasst und können nur von denen gefunden werden, die die Adresse bereits kennen. Andere Links führen zu toten Seiten. Jene Listen, die relativ gut gepflegt werden, enthalten zumeist illegale Inhalte und führen zu Marktplätzen innerhalb des TOR-Netzes.

Anonymität lässt sich aus rein technischer Sicht relativ leicht wahren, nutzt man den TOR-Browser. Die meisten Prozesse zur Verschleierung der Kommunikation passieren automatisch im Hintergrund und die Voreinstellungen des Browsers sind für das Surfen durch verschiedene Webseiten und Darknet-Seiten bereits gut ausgerichtet. Die größte Gefahr, seine Identität selbst aufzudecken, liegt in unachtsamen Verhalten, dem preisgeben eines Namens oder einer Adresse bzw. Emailadresse oder Nutzung von Cookies. Doch auch hier bietet der Browser Hinweise und Pop-Ups, die den Nutzer informieren und warnen sollen, bevor einer solchen Funktion zugestimmt wird. Doch trotz all der vereinfachten Bedienung der Software und Automatismen ist die eigene Anonymität im TOR-Darknet potentiell größer gefährdet als in anderen Darknets, da speziell dieser Vertreter einen solch großen, negativen Medienfokus auf sich zieht. TOR ist inzwischen ein beliebtes Angriffsziel für Strafermittler und Regierungsbehörden und, wie zuvor bereits geschildert, gibt es im Arsenal dieser Institutionen Möglichkeiten, TOR anzugreifen und zu durchleuchten.

Rechtlich gesehen ist es grundsätzlich nicht illegal, TOR zu nutzen, wie oftmals fälschlicherweise angenommen. Entscheidend ist die Frage, was ein Nutzer im Darknet tut. Konkret strafbar macht man sich in TOR erst dann, wenn man sich an illegalen Aktivitäten oder Geschäften beteiligt. Doch da dies nicht immer eindeutig nachzuweisen ist, gibt es gewisse Risikoquellen, die es besonders im Falle von TOR zu beachten gilt. Das Kaufen von Gegenständen über das Darknet, sofern diese nicht illegaler Natur sind, ist zunächst kein strafbares Verhalten. Aufgrund der hohen Kriminalitätsdichte innerhalb TORs, ist jedoch nie ganz auszuschließen, dass es sich bei einem harmlos erscheinenden Gegenstand um Diebesgut handelt. Deshalb ist prinzipiell davon abzuraten, Einkäufe über TOR zu tätigen, um nicht unbewusst in kriminelle Handlungen verwickelt zu werden [47]. Ein weiterer wichtiger Punkt ist die Funktion als sogenannter Exit-Node. Dabei handelt es

sich um den letzten Knoten innerhalb einer Verbindung, der direkten Kontakt zu deren Ziel hat. Die Adresse dieses letzten Knotens lässt sich nachvollziehen, sofern das Ziel überwacht wird. Sollten die abgefragten Inhalte des Zielknoten strafbarerer Natur sein, so besteht für den Exit-Node ein Verdachtsfall, auch wenn dieser die Anfrage nicht gesendet hat und den eigentlichen Anfragesteller auch nicht kennt [43]. Nutzer sind jedoch nicht gezwungen als Exit zu fungieren, außerdem ist in der aktuellen Version des TOR-Browsers diese Funktion standardmäßig deaktiviert. Zu empfehlen ist es, diese Funktion nur dann zu aktivieren, wenn man umfassende Kenntnisse über die Rechtslage auf diesem Gebiet hat. Einige Knoten des Chaos-Computer-Clubs, denen ein juristisches Team beisteht, dienen zum Beispiel als Ausgangsknoten. Für Nutzer, die rechtlich vollkommen abgesichert sein wollen, auch wenn sie zufällig auf Onion-Seiten mit illegalem Inhalt stoßen, bleibt die Möglichkeit, diese Adresse direkt der Polizei oder einer zuständigen Behörde zu melden.

Auch das Entfernen der Software ist ähnlich nutzerfreundlich, wie die Installation. Möchte der Nutzer keinen Zugang mehr zu TOR haben, reicht es, den Browser vom eigenen Gerät zu löschen.

Zusammenfassend lässt sich also die Schlussfolgerung ziehen, das die Darknet-Lösung des TOR-Projekts sowohl in der Beschaffung als auch in der Anwendung als sehr nutzungsfreundlich einzustufen ist. Das Wahren der Anonymität, die damit verbundenen rechtlichen Risiken und die Navigation innerhalb des Netzes hingegen halten für einige Nutzer erhebliche Hürden bereit.

3.1.6 Zukunftsausblick

Das TOR-Projekt ist ein besonderer Fall, wenn es um einen Ausblick in die Zukunft geht, da es nicht nur im Fokus von Sicherheits- und Regierungsbehörden steht, sondern auch starke Unterstützung aus diesen Reihen erhält. Somit lässt sich schwer sagen, in welche Richtung sich das Netzwerk entwickeln wird. Es lässt sich jedoch sagen, dass das Netzwerk weiterhin wachsen und an Bekanntheit gewinnen wird, sowohl im positiven als auch im negativen Sinne. Die Projektseite macht sofort klar, dass jene, die hinter dem Projekt stehen, viel Arbeit und Zeit in dessen Entwicklung stecken. Doch damit wächst auch der Missbrauch durch kriminelle Nutzung. Durch den Erfolg des Bitcoins als anonyme Zahlungsmethode, hat sich TOR bereits jetzt als sicherer Handelsmarkt etabliert, und wie frühere Fälle beweisen, stören strafrechtliche Verfolgungen und Eingreifen in diese an

Macht gewinnende Wirtschaft keinesfalls das Wachstum dieser Märkte. Es bleibt zu hoffen, dass auch der positive Nutzen der Software Wachstum und einen Platz in den modernen Medien findet.

3.2 Freenet

Freenet ermöglicht es dem Nutzer, auf anonymer Basis Dateien auf so genannten „Freesites“ [22] auszutauschen. Es handelt sich dabei also um Webseiten, die ausschließlich durch Freenet erreichbar sind. Der User kann sich an der Kommunikation zu beteiligen, ohne Zensur fürchten zu müssen. Dabei kommen die für Darknets charakteristischen Verschlüsselungs- und Tunnelmechanismen zum Einsatz, um zu verschleiern, wer mit wem über was kommuniziert. Ähnlich wie TOR lebt auch dieses Netzwerk vom Mitwirken seiner Nutzer. Indem diese Bandbreite und Speicherplatz zur Verfügung stellen, wird das Netzwerk erst voll funktionstüchtig. Dabei hat Freenet den „Darknet-Modus“ direkt als Funktion implementiert. Die Besonderheit an diesem Modus ist, dass Nutzer nicht mit irgendeinem Knoten im Netzwerk verbunden werden, sondern nur mit so genannten Freunden und auch von diesen eingeladen werden müssen. Durch die Freunde von Freunden von Freunden ist es dem Nutzer so trotzdem möglich mit dem kompletten Netzwerk in Kontakt zu stehen, jedoch direkt nur mit Knoten verbunden zu sein, denen er vertraut [48]. Anders als bei TOR oder I2P gibt es hier keine typische Endung für die Darknet-Adressen. Stattdessen beginnt jede Adresse mit dem Vorsatz „localhost:8888“ und endet mit einer langen, zufällig wirkenden Zeichenfolge, an die sich der Titel der Seite anschließt. Nutzer gehen davon aus, dass die inhaltliche Vielfalt von Freenet größer ist als die der beiden anderen Vertreter, wobei ein großer Teil von Blogs und Diskussionsforen zu unterschiedlichsten Themen besteht. Laut den Betreibern handelt es sich dabei um ein Drittel des kompletten Netzwerks [49].

3.2.1 Geschichtliche Hintergründe

Die ersten Überlegungen für die Freenet Software kamen 1999 auf. Der damalige Student Ian Clarke schrieb an einer Abhandlung zu einem „verteilten dezentralisierten Informationsspeicher- und Abrufsystem“ [50], welches er kurze Zeit später mit einigen Freiwilligen praktisch umsetzte und im Jahr 2000 veröffentlichte. Die Folge war ein erhöhtes Vor-

[22] Zu deu.: freie Seiten

kommen in den Medien, vorwiegend mit der Fragestellung um das Problem von Copyrights, da das System in erster Linie zum Austausch von Daten konzipiert wurde. Die weitere Entwicklung der Freenet-Software erfolgte dezentralisiert über das Internet und wurde als gemeinnütziges Projekt definiert, „The Freenet Project Inc.“. Neben den freiwilligen Mitarbeitern, konnte 2002 dank Spendeneinnahmen und Einnahmen aus anderen Quellen ein Programmierer fest eingestellt werden. Mathew Toseland programmierte nun Vollzeit an Freenet. Der nächste Entwicklungsschritt erfolgte 2005, als Freenet 0.7 geplant wurde. Die bedeutendste Erneuerung bei dieser Version war der neue „Darknet-Modus“, den man nur auf Einladung eines Freundes betreten kann. Diese Version wurde 2006 veröffentlicht [51] und ist noch bis zur heutigen Zeit aktuell. Zwar gab es weitere Entwicklungen und Versionen, jedoch keine vergleichbar tiefgreifenden Veränderungen mehr.

3.2.2 Finanzierung & Organisation

Hinter dem Freenet-Projekt steht eine Organisation aus Austin, Texas. Präsident dieser Organisation ist der Erfinder von Freenet, Ian Clarke. Clarke schätzte 2017, dass sich etwa 15.000 User im Netz befinden, jedoch kann er selbst nicht feststellen, wie viele Seiten in Freenet betrieben werden. Auch die Zahl der ehrenamtlich mitarbeitenden Community kennt selbst er nicht genau, vermutet aber zwischen fünf und 20 Personen [49].

Finanziert wird das Projekt zum einen aus Spenden. Diese kommen sowohl von Privatpersonen, als auch von Unternehmen, Organisationen und Gruppierungen. Eine Liste besonders hohe Spendeneingänge ist auf der Projekt-Webseite[23] unter dem Menüpunkt „Donate“ aufgelistet. Dabei handelt es sich nicht ausschließlich um Geldspenden, sondern auch um Software Lizenzen oder Arbeitsmaterialien. Zum anderen kommen dem Projekt Gelder aus dem Verkauf eigener Produkte ihres Online-Shops[24] zu Gute.

3.2.3 Funktionsweise

Freenet bietet nicht wie TOR einen eigenen Browser an, sondern stellt eine Software, die den eigenen Browser modifiziert und Einstellung so ändert, dass auf das Freenet-Netzwerk zugegriffen werden kann. Das Netzwerk funktioniert über zwei verschiedene Funktions-Modi. Standard ist der sogenannte „Unsichere Modus“. Dieser bietet die Verbindung zu jedem Knoten im Netzwerk, der mit diesem Modus verbunden ist. Zwar ist die

[23] www.freenetproject.org

[24] www.zazzle.com/freenetproject

Verbindung hier verschlüsselt, jedoch können die IP-Adressen der Teilnehmer hier recht leicht erfasst werden. Der „Darknet Modus“ bietet die eigentliche Darknet-Technologie. Verbindung ist die „Verbindung zu Freunden“. Bei dieser Variante verbindet man sich nicht mit dem gesamten Freenet-Netzwerk, sondern nur mit ausgewählten Nutzern, die man kennt und denen man vertraut. Abbildung 4 veranschaulicht diese Verbindung.

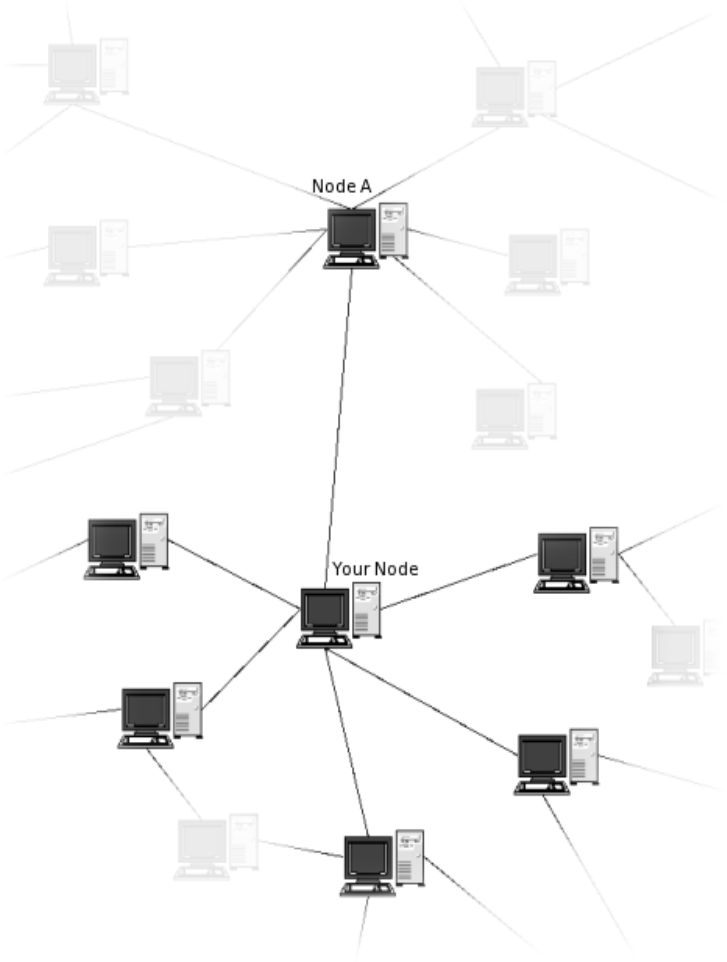

Abbildung 7: Connection to Friends - Freenet (Secure Mode)

Quelle: https://freenetproject.org/assets/img/Freenet-architecture-small.png (abgerufen am 19.03.2018)

Um diese Art der Verbindung überhaupt sinnvoll nutzen zu können, sollten dabei jedoch mindestens drei, besser noch fünf bis sieben Nutzer dauerhaft verbunden sein. Dabei sind alle Knoten des Netzwerks mit dem eigenen Rechner verbunden, allerdings unsichtbar in beide Richtungen. Datenverkehr wird daher nur über die Knoten geleitet, die dem Nutzer bekannt sind, also „Freunde“ sind. In der Grafik ist der befreundete Teilnehmer als „Node A“ bezeichnet, während die fremden Teilnehmer keine Namen haben. In diesem Beispiel

wird der Datenverkehr folglich nur über „Node A“ geleitet. Um sich mit Freenet verbinden zu können, wird die IP-Adresse eines anderen Teilnehmers benötigt. Im Unsicheren Modus stehen Listen mit solchen IP-Adressen, sogenannten Seednodes, freizugänglich zur Verfügung. Im Darknet Modus muss eine Einladung erfolgen. Durch diese Art der Verbindung mit Freunden formen sich vielmehr mehrere kleinere Netzwerke als ein gesamtes. Freenet arbeitet wie ein großer Datenspeicher, bei dem die Daten in kleinere Pakete zerlegt und auf verschiedenen Rechnern verteilt werden. Statt Inhalte auf Servern abzulegen, werden sie bei dieser Lösung somit in Einzelteile zerlegt, verschlüsselt und anschließend zufällig auf verschiedenen Rechnern abgelegt. Aus diesem Grund stellt jeder Rechner, der Teil des Netzwerks ist, einen Teil seines Speicherplatzes zur Verfügung. Dies geschieht automatisch bei Installation der Freenet-Software. Dies erfolgt, indem jedem Datenteil einen Content Hash Key (CHK) hinzugefügt bekommt. Mittels dieses Schlüssel kann die Datei wieder zusammengesetzt werden. Zur Verwaltung des Lageortes der jeweiligen Dateipakete innerhalb Freenets dient der Signed Subspace Key (SSK). Dieser hat einen Verweis auf die CHK gespeichert. In Zusammenarbeit der ID des jeweiligen als Speicherort dienenden Knotens und der SSK kann so eine Zuordnung zum Knoten erfolgen und die Datei wieder zusammengeführt werden.

3.2.4 Wer nutzt Freenet?

Da sich Freenet konkreter auf den Austausch von Daten spezialisiert als auf ein breites multimediales Spektrum, findet sich hier eine weniger gemischte Community, obwohl die inhaltliche Vielfalt größer vermutet wird, als es bei TOR der Fall ist. In Freenet finden sich zum Beispiel Gruppierungen, die sich anonym austauschen wollen, Blogger zu allerlei Themen, sowie Menschen die sich ohne Zensur an Diskussionen in den zahlreichen Diskussionsforen beteiligen. Doch auch in Freenet bleibt ein kriminelle Klientel nicht aus, besonders wenn es um Filmmaterial mit umgangenen Copyrights oder illegalem Inhalt geht. Jedoch setzt die Freenet-Community eine klare Abgrenzung zu dieser Nutzung ihres Darknets, indem Seiten mit entsprechendem Inhalt auf einer Liste mit dem Titel „Unerwünschte Inhalte“ vermerkt werden.

3.2.5 Usability-Einschätzung

Die Beschaffung der Software ist unkompliziert, da es sich um Freeware handelt. Genau wie bei TOR findet sich ein entsprechender Download auf der Projektseite oder über

zahlreiche Downloadportale. Die Installation gestaltet sich jedoch etwas schwieriger. Voraussetzung, um Freenet überhaupt installieren zu können, ist Java. Sobald der Installationsassistent startet, wird der Nutzer aufgefordert, eine Sprache für den Prozess auszuwählen. Sofern Java fehlt oder nicht auf dem benötigten Stand ist, folgt an dieser Stelle ein Hinweis, dass es mit installiert werden muss. Dies kann durch den Freenet-Installationsassistenten erfolgen [Abbildung 11].

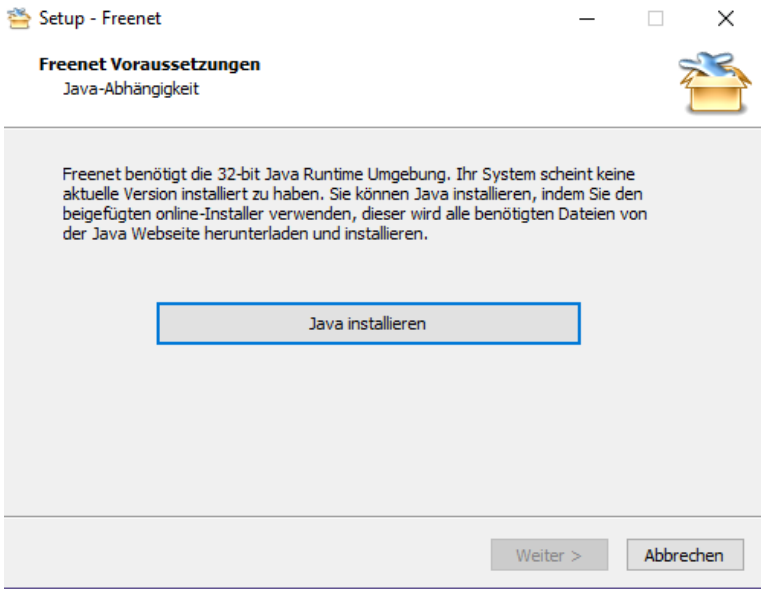

Abbildung 11: Freenet – Java Installation

Gegebenenfalls startet der Installationsprozess für Java. Ist dieses vorhanden, fordert der Assistent den Nutzer auf, einen Zielort für die Installation und anschließend einen Namen für den neu erstellten Ordner auszuwählen. Im Anschluss wird der Installationsprozess durchlaufen und nach dessen Abschluss kann Freenet gestartet werden. Die zusätzliche Java Installation könnte für ungeübte Nutzer ein Problem darstellen. Wenn man die Software startet, öffnet sich nicht direkt ein Browserfenster. Stattdessen taucht das Freenet-Symbol auf. Bei Windows zum Beispiel erscheint es im Bereich der „Ausgeblendeten Symbole“. Dies könnte für einen Anwender irritierend wirken, da ihnen optische Rückmeldung fehlt. Ein Klick auf das Symbol öffnet den Standardbrowser mit einer Freenet-Startseite. Beim erstmaligen Starten der Software erscheint hier ein Einrichtungs-Assistent, der dabei helfen soll, den richtigen Modus zu wählen [Abbildung 12].

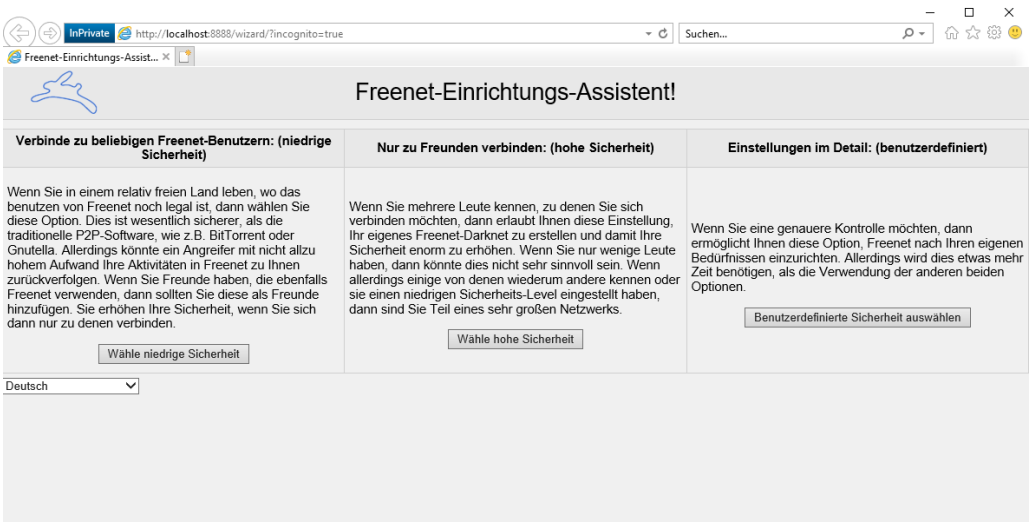

Abbildung 12: Freenet-Einrichtungs-Assistent

Hierzu steht zu den jeweiligen Optionen Unsicherer Modus, Freund-zu-Freund Verbindung und Benutzerdefinierter Modus ein erklärender Text. Wählt man den Darknet Modus, also die Freund-zu-Freund Verbindung, wird man auf bestimmte Browsereigenarten hingewiesen und wird schließlich aufgefordert, die IP mindestens eines Freundes zu bestätigen, um Zugang zum Netzwerk zu erhalten. Dies ist die Einladung, die benötigt wird. Wählt man den Unsicheren Modus oder kann eine befreundete IP nennen, so wird man aufgefordert, eine Reihe von Fragen zur eigenen Internetverbindung zu beantworten, um Freenet individuell zu konfigurieren. Abschließend verbindet sich die Software mit einem Knoten. Dies dauert unter Umständen einige Minuten und die volle Leistung des Netzwerks ist erst nach mehreren Stunden erreicht. Dieser Vorgang wiederholt sich jedes Mal, wenn Freenet für mehrere Minuten, abgeschaltet wurde, was eine spontane Nutzung der Software erschwert. Die Einstellungen für die Software sind damit abgeschlossen, könnten aber einige Neueinsteiger aufgrund der Art der Fragen trotz Anleitung verwirren. Es gibt außerdem kein browserinternes Interface wie bei TOR. Einstellungen können anschließend nur noch über einen Rechtsklick auf das Freenet-Symbol erfolgen.

Um einen Einstieg in die Navigation innerhalb des Netzwerks zu finden, öffnet Freenet dem Nutzer als Startseite eine Liste mit Verzeichnissen und Link-Listen, relevanten Dokumenten, Freenet-bezogenen Anwendungen und den Blogs einiger Mitwirkender. Die Navigation innerhalb des Freenet-Netzwerks, unabhängig vom Verbindungsmodus, erfolgt vorwiegend über Link-Listen, welche im Gegensatz zu denen von TOR und I2P äußerst gut dokumentiert und gepflegt sind.

Die Anonymität zu wahren ist bei Freenet deutlich fehleranfälliger als bei TOR. Da der Standardbrowser verwendet wird, ist die Gefahr groß, dass Nutzer auf bestimmten Webseiten noch mit Nutzerkonten eingeloggt sind und Cookies verwenden, und so seine Identität preisgeben. Außerdem bietet der Unsichere Modus keine wirklich starke Verschleierung der IP-Adresse.

Das Risiko, rechtlich belangt zu werden, ist hier äußerst gering, sofern man sich nicht an illegalen Aktivitäten beteiligt. Durch die Aufteilung und Verschlüsselung der Datenpakete kann kein Nutzer rechtlich belangt werden, sogar dann, wenn sich fremde, kriminelle Inhalte auf seinem Rechner befinden. Da ohne die entsprechenden Schlüssel niemand sagen kann, was sich innerhalb der gelagerten Datenpakete befindet, ist schwer nachzuvollziehen, auf welchen Geräten sich diese kriminellen Inhalte befinden und der Besitzer des Gerätes ist in der Regel nicht der Urheber dieser Inhalte. Somit sind Nutzer hier abgesichert, wenn es um inhaltliche Probleme geht. Jedoch gab es auch innerhalb der Freenet-Community bereits Festnahmen, denn wer illegale Inhalte bewusst verteilt, macht sich auch hier strafbar.

Die Deinstallation von Freenet ist nicht anders als die anderer Programme. Jedoch lassen sich nicht alle Komponenten der Software automatisch deinstallieren. Einige Dateien müssen manuell gesucht und gelöscht werden.

Es wird damit also deutlich, dass die Freenet-Lösung sowohl in der Beschaffung als auch im Rahmen der rechtlichen Gefahren für Nutzer eine angenehme Handhabung verspricht. Auch Konfiguration, Navigation und Verfügbarkeit bewegen sich in einem akzeptablen Maß. Jedoch kristallisieren sich große Problemquellen im Bereich der Sicherheit von Anonymität heraus.

3.2.6 Zukunftsausblick

Es ist zu erwarten, dass Freenet zwar weniger rasant wächst als TOR, da die finanzielle Lage sich in anderen Dimensionen bewegt, aber das Engagement, das hinter dem Projekt steht, nicht minder stark ist. Inhaltlich betrachtet hat Freenet einen geringeren kriminellen Anteil als der größere Vertreter und eine positiver behaftete, wenn auch kleinere Medienpräsenz. Dies könnte sich in Zukunft durchaus als Vorteil erweisen. Stefan Mey bezeichnet die Freenet-Software als fortschrittlichste Darknet-Technologie [52]. Aus diesem Gesichtspunkt betrachtet wäre es durchaus möglich, dass sich auf dieser technischen Grundlage in der Zukunft noch weitere Ansätze entwickeln. Dem Freenet-Wiki ist zu

entnehmen, dass es klare Ziele für die Weiterentwicklung von Freenet gibt - so zum Beispiel eine Anpassung verwendeter Protokolle, die Einführung von Stenographie oder der Unterstützung freier, virtueller Java Maschinen [53]. Fest steht also, dass Freenet sich auf technischer Ebene noch viel vorgenommen hat.

3.3 I2P

„The invisible Internet Project“ ist ein anonymes Netzwerk, welches sich sehr auf Kommunikation spezialisiert hat. Jede Kommunikation über I2P ist dabei End-To-End-verschlüsselt[25]. Charakteristisch für Inhalte dieses Darknets ist die Adressendung „.i2p“. Jeder am Netzwerk angeschlossene Rechner sendet und empfängt Daten der eigenen Kommunikation sowie den Datenverkehr anderer, welcher weitergeleitet wird. Das bedeutet, dass die Infrastruktur des Netzwerks von den Teilnehmern automatisch aufgebaut wird [10]. Die I2P-Nutzer stellen die Infrastruktur, da jeder Nutzer auch gleichzeitig Knoten im Netzwerk ist. Folglich sendet und empfängt jeder angeschlossene Rechner Daten auf demselben Auslastungsniveau. Anonymität kommt vor allem dadurch zustande, dass Daten über sich ständig neu formende Tunnel verschickt werden[26]. Damit ein Rechner I2P nutzen kann und Teil des Systems wird, ist eine spezielle Software erforderlich. Diese modifiziert den üblichen Internetbrowser so, dass dieser anschließend auch die entsprechenden „.i2p“-Adressen des Darknets aufrufen kann. Die am häufigsten vertretenen Inhalte des Darknets bestehen nach Schätzungen der Betreiber insbesondere aus Tauschbörsen für Mediendateien wie Filmen und Musik, Diskussionsforen, größtenteils zu politischen Themen und I2P-basierenden Softwareangeboten. Die Größe des Netzwerks wurde 2017 auf 400 aktive i2p.-Adressen geschätzt und ist damit deutlich kleiner als von vielen angenommen.

3.3.1 Geschichtliche Hintergründe

Trotz des errungenen Status als einer der Topvertreter der Darknets gilt das I2P Projekt seit seiner Veröffentlichung im Jahr 2003 als Beta-Version. Grund dafür ist, dass den Betreibern Nutzerrückmeldungen fehlen und noch längst nicht alle erdachten Konzepte ausgebaut wurden [54]. Seitdem wurde das Projekt jedoch stetig weiterentwickelt und ausgebaut. Besonders erwähnenswert sind hier die Einführung einer Android-Version im

[25] Bezeichnet die Verschlüsselung von Daten über alle Kommunikationsebene, nur die jeweiligen Endpunkte, also Sender und Empfänger, können diese entschlüsseln.

[26] https://geti2p.net/de/docs/how/intro

Jahr 2014, sowie die Gründung einer Organisation zur Pflege von I2P-spezifischen Anwendungen im selben Jahr.

3.3.2 Finanzierung & Organisation

Betrieben wird das I2P-Netzwerk von einem losen Zusammenschluss von Personen, welche auch die Technik hinter dem System warten [52]. Nach eigenen Angaben der Betreiber besteht das Kern-Team aus gerade mal 15 Personen [52]. Eine Liste von Mitwirkenden ist auf der Projekt-Webseite[27] einzusehen. Auf den ersten Blick könnte man meinen, dass es sich dabei um weit mehr Personen handelt, bei genauerem Hinsehen jedoch fällt auf, dass mehrere Positionen von je einer Person besetzt werden. Auch einige freie Stellen fallen auf, dies unterstützt die Schätzungen. Trotz der verteilten und rein freiwilligen Organisation von Mitarbeitern, sind Aufgaben und Positionen klar strukturiert und verteilt. Ähnlich Freene, finanziert sich auch I2P über Spenden. Diese können in den unterschiedlichsten Währungen und Kryptowährungen überreicht werden. Für einen besonders hohen Anonymitätsfaktor bietet I2P sogar die Möglichkeit, per Bargeld und Brief zu spenden. Für jene Spender, die etwas Anerkennung wünschen, ist unter dem Menüpunkt „Ruhmeshalle“ eine Liste von Spendern bereitgestellt.

3.3.3 Funktionsweise

Die grundlegende Technik zur Anonymisierung unter I2P ist das Versenden der Daten über sich ständig neu formende Inbound-[28] und Outbound-Tunnel[29] [64] [Abbildung 16]. Im Anhang, Abbildung 3, wird das Verfahren beispielhaft dargestellt.

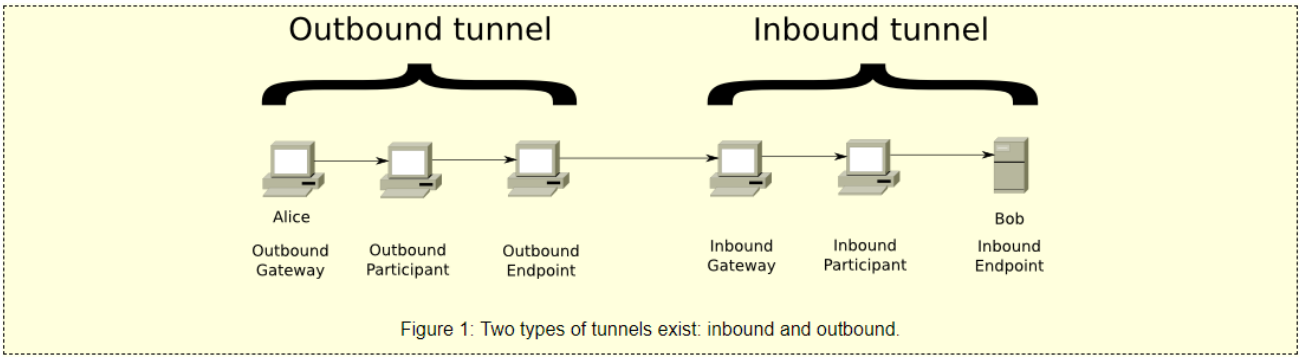

Abbildung 16: I2P Tunnelarten
Quelle: https://geti2p.net/de/docs/how/tech-intro (abgerufen am 03.05.2018)

[27] www.geti2p.net/de/about/team
[28] Deutsch: Eingehend
[29] Deutsch: Ausgehend

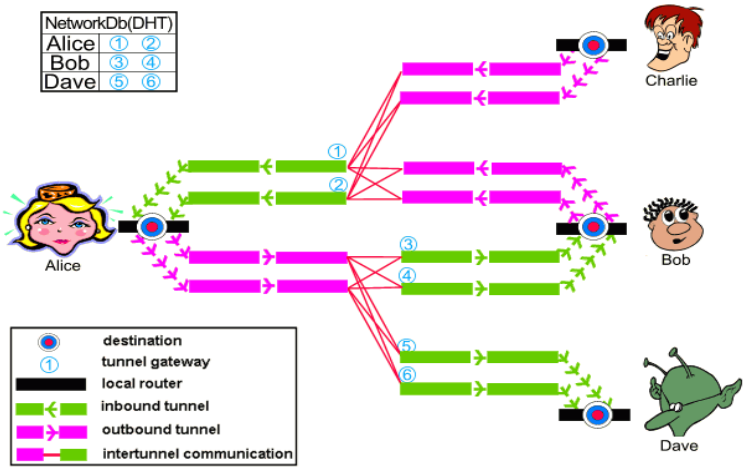

Abbildung 8: "Tunnel"- Kommunikation von I2P
Quelle: https://geti2p.net/_static/images/net.png (abgerufen am 20.03.2018)

Bei diesem handelt es sich um eine Modifikation des Kademlia-Algorithmus [55], welcher von Petar Maymounkov und David Mazières entwickelt wurde und üblicherweise bei Filesharing-Software zum Einsatz kommt [63]. Im Gegensatz zu TOR und Freenet ist es nicht das primäre Ziel der Software, Teile der Kommunikation zu verstecken. Stattdessen sollen Empfänger und Sender füreinander und für Dritte anonym sein. I2P ist, im Gegensatz zu TOR, ein geschlossenes Netzwerk. Das bedeutet konkret, dass Daten nicht über schwer nachvollziehbare Wege an öffentliche Server weitergereicht werden, sondern ausschließlich an Adressen innerhalb des I2P-Netzwerkes gesendet werden. Diese Adressen sind sogenannte „Eepsites“, anonym gehostete Seiten wie zum Beispiel ein anonymer Blog [56]. Ähnlich wie es bei Freenet der Fall ist, wurde I2P in Java geschrieben, weshalb eine Java-Laufzeitumgebung erforderlich ist, um die Software nutzen zu können. Ein Herzstück der Funktionsweise von I2P sind Web-Dienste und -Anwendungen, die unter I2P laufen. So lassen sich zum Beispiel mit Hilfe von „Jetty“, „Ngnix“ oder „Apache“ speziell für i2P konfigurierte Webserver aufsetzen. „El Dorade“ und „JAMWiki“ erlauben es, anonyme Blogs für das Netzwerk aufzusetzen, und für anonyme Foren bieten sich „Pebble“, „phpBB“ und „Syndie“ an. I2P unterstützt außerdem eine breite Auswahl an Kommunikationsprotokollen wie beispielsweise HTTP, XMPP oder IRC. Zum Austausch von Daten unter I2P gibt es vorkonfigurierte Anwendungen wie zum Beispiel „I2PSnark“ oder „Transmission for I2P“. Es gibt ebenfalls entsprechende Email-Dienste, zum Beispiel „I2P-Bote“, sowie Chat-Programme, die speziell für das Netzwerk ausgelegt sind [57]. Diese Anwendungen und Dienste sind für das Netzwerk wichtig, da

sie einen großen Teil des Zugangs zum Netzwerk darstellen. Andere Dienste fungieren teilweise als Proxy, die sich gegenüber dem Client wie normale Server verhalten und so auf normale Programme wie einen als Standard festgelegten Internet-Browser angewendet werden können. Diese werden einfach über eine Port-Nummer auf einen I2P-Server konfiguriert [59].

Um Daten durch das Netzwerk zu leiten, sendet das jeweilige für I2P eingestellte Programm diese an den angegeben I2P-Router, wo die Verschlüsslung vorgenommen wird. Im nächsten Schritt wird vom Router ein Tunnel über mehrere fremde I2P-Router festgelegt, welcher bis zu einem vordefinierten Übergabeknoten des Ziel-Routers führt [Abbildung 17 – 18].

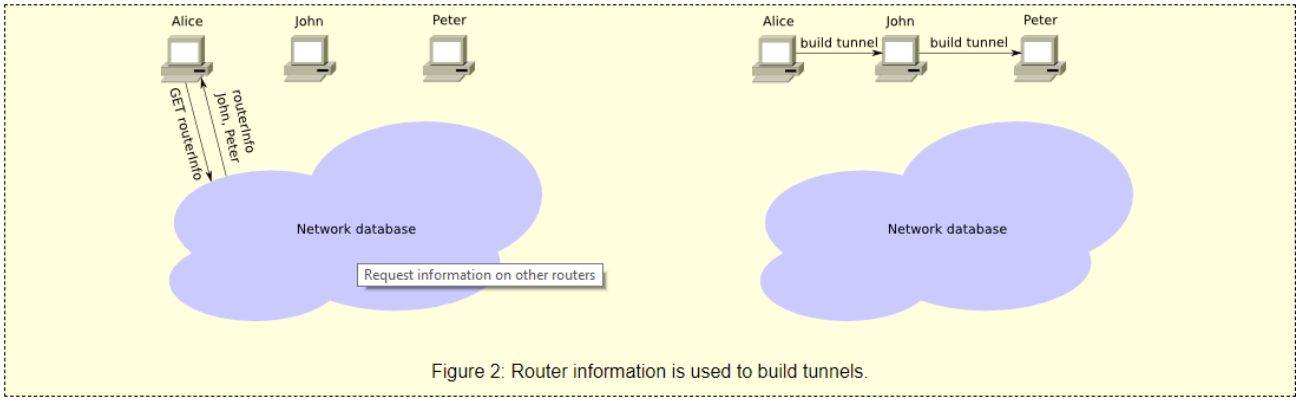

Abbildung 17: I2P Routerinformationen zum Erzeugen von Tunneln1
Quelle: https://geti2p.net/de/docs/how/tech-intro (abgerufen am 03.05.2018)

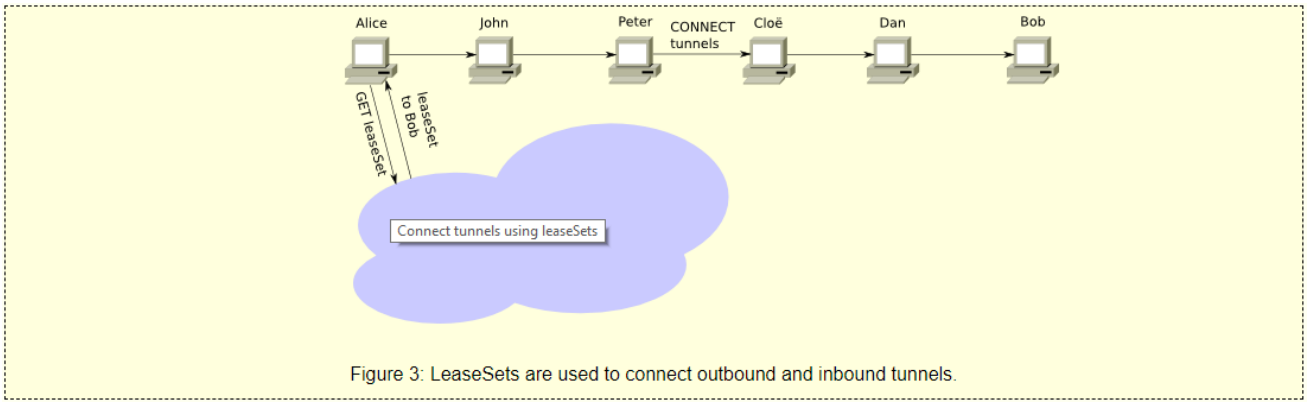

Abbildung 18: I2P Routerinformationen zum Erzeugen von Tunneln 2
Quelle: https://geti2p.net/de/docs/how/tech-intro (abgerufen am 03.05.2018)

Dort werden die Daten übergeben und wieder durch einen Tunnel aus mehreren I2P-Routern zum eigentlichen Ziel geleitet. Diese Tunnel führen stets über mindestens drei fremde

I2P-Router, um einen gewissen Grad an Sicherheit zu gewährleisten [Abbildung 19]. Damit es beim Ausfall eines Routers und somit des kompletten Tunnels nicht zu Datenverlusten kommt, werden stets zwei Routen aufgebaut. War die Übertragung durch einen der Tunnel erfolgreich, wird vom Ziel-Router eine Empfangsbestätigung durch einen komplett anderen Tunnel zurückgesendet. Um klar zu definieren, wo sich Übergabepunkte im Netz befinden, bzw. welche Tunnel gerade belegt sind, werden Abfragen an die sogenannte I2P-Netzdatenbank gesendet. An dieser Stelle wird der bereits erwähnte Kademlia-Algorithmus angewandt, denn diese Datenbank enthält eine darauf basierende Hashtabelle [59], in der die entsprechenden Informationen vorliegen. Nach jeweils 11 Minuten werden die aufgebauten Tunnel wieder verworfen und neu belegt.

3.3.4 Wer nutzt I2P?

Da das Netzwerk in seiner Grundstruktur und Handhabung kaum Ähnlichkeiten zu TOR oder Freenet aufweist, sind die Nutzergruppen deutlich konzentrierter. I2P wird vor allem von Personen benutzt, die das Konzept der anonymen Kommunikation fasziniert, an dem Projekt in irgendeiner Form mitwirken oder selbst „Eepsites“ betreiben. Da die meisten „Eepsites“ jedoch nicht mehr erreichbar sind und stetig neue hinzukommen [58], ist anzunehmen, dass es sich außerdem um eine sich stetig verändernde Nutzerbasis handelt. Personen, die an einem sicheren Austausch von Dateien interessiert sind, werden sich vor allem mit Anwendungen wie „I2PSnark“ beschäftigen [58]. Durch die Vielzahl an Diensten und Applikationen, die I2P als Grundlage dienen, ist es ein sehr vielseitiges Netzwerk. Jedoch schreckt es Nutzer, die zum Beispiel TOR bevorzugen, durch seine Komplexität ab.

3.3.5 Usability-Einschätzung

Der Download der Software ist nicht schwierig, dennoch sind die entsprechenden Downloadmöglichkeiten nicht so zahlreich wie es bei den beiden anderen Vertretern der Fall war. Der Download ist auch hier über die Projekt-Webseite für Windows, Android, Mac, Ubuntu und Linux, auffindbar. Wird jedoch ein anderer Downloadhost verwendet, so kann es passieren, dass durchaus etwas Falsches heruntergeladen wird, da es noch andere Projekte und Programme mit gleichem bzw. ähnlichem Namen gibt. Sobald sich die Software auf dem Gerät des Nutzers befindet und gestartet wurde, öffnet sich ein kleiner Begrüßungsbildschirm, der auf die Projektseite verweist, gefolgt von einigen Informationen

zum Projekt und der Software. Danach soll der Benutzer die ersten Konfigurationen für die Installation vornehmen [Abbildung 13], sowie ein Installationsverzeichnis wählen.

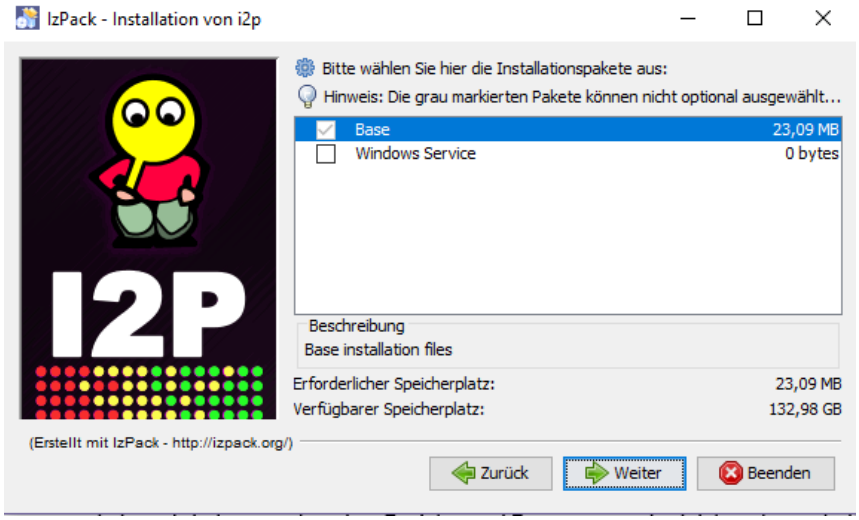

Abbildung 13: Installation i2p

Es muss eine Programmgruppe gewählt werden [Abbildung 14], bevor der Installationsprozess startet.

Abbildung 14: Installation von i2p – Programmgruppe

Diese doch recht umfangreichen Einstellungsoptionen während der Installation sind ohne konkretere Beschreibung oder Hintergrundwissen schwer zu bewältigen. Nach Fertigstellung muss das Programm händisch gestartet werden. Ist dies erfolgt, öffnet sich im Standard-Browser die sogenannte I2P-Routerkonsole [Abbildung 15].

Abbildung 15: I2P-Routerkonsole

Diese bildet die Startseite und das Hauptnavigationspanel. Für Neueinsteiger kann die Menge an Optionen, die hier zur Verfügung stehen, überfordernd sein. Dies wird jedoch durch eine klare Gliederung und gute optische Aufbereitung wieder ausgeglichen. Am linken Rand befinden sich Einstellungsmöglichkeiten und Informationen bezüglich der Verbindung zum Netzwerk. Im Fokus der Seite findet sich ein Infoboard, eine Sprachauswahl, Anwendungen, Konfigurationsmöglichkeiten und Dienste des Darknets. Doch um diese nutzen zu können, muss der entsprechende Browser noch für I2P angepasst werden. Hierzu muss das Einstellungsmenü des jeweiligen Browsers geöffnet werden und eine IP-Adresse, ein Port und eine Localhost-Adresse angegeben werden. Für Nutzer, die nicht wissen was genau hier eingetragen werden muss, gibt es hierfür einige Hinweise auf der Projektseite. Diese Anpassung des Browsers macht es recht unhandlich, I2P spontan zu nutzen, da die Einstellung bei jeder Nutzung bzw. Abschaltung wieder geändert werden müssen. Abhilfe hierfür können zumindest bei Firefox einige Plug-Ins schaffen, die sich solche Einstellungen merken und mit einem Klick ändern. Jedoch kann dies die Anonymität gefährden. Als weitaus schwieriger erweist sich die Navigation innerhalb des Netzwerks. Zwar liefert die Routerkonsole ein I2P-Adressbuch, dieses ist jedoch zunächst leer und muss erst noch vom Nutzer mit Adressen gefüllt werden. Für diesen Zweck wird ein sogenannter „Jump Service“ benötigt. Einige dieser Services finden sich bereits in der Routerkonsole, wobei nicht jeder dieser Links funktionstüchtig ist. Sobald ein funktionierender Service gefunden wurde, wird dieser zum Adressbuch hinzugefügt und gestartet. Nachdem eine Verbindung aufgebaut wurde, kann durch diese angefangen werden, dass I2P-Darknet zu durchsuchen und Adressen im Adressbuch gespeichert werden [60].

Die Gefahr, die eigene Anonymität zu lüften, ist in diesem Fall recht gering. Zwar besteht auch hier die Chance, mit Nutzerkonten durch den Browser verbunden zu sein bzw. aktive Cookies gespeichert zu haben, doch I2P blockiert die meisten Dienste und Protokolle, die eine Gefahr für die eigene Anonymität darstellen. Natürlich ist dieser Schutz nicht zu 100% fehlerfrei, deckt jedoch die meisten Bedrohungen gut ab. Da es sich um ein recht kleines Netzwerk handelt, ist auch das Risiko von Angriffen weniger gering, als es bei TOR der Fall ist. Die größte Hürde besteht darin, sich selbst durch Weitergabe von persönlichen Daten zu entlarven. Aus rechtlicher Sicht betrachtet, ist die Gefahr sich selbst strafbar zu machen somit auch gering, sofern man keine kriminellen Inhalte anbietet oder illegalen Aktivitäten nachgeht.

Die Deinstallation der Software muss durch eine Deinstallationsanwendung erfolgen, die sich im Installationsordner der Anwendung befindet, da bei einer herkömmlichen Deinstallation die Gefahr besteht, dass nicht der komplette Speicherplatz wieder freigegeben wird. Der Nutzer wird während der Installation jedoch darauf hingewiesen.

Es wird deutlich, dass I2P eine der nutzerfreundlichsten Lösungen bietet, wenn es um rechtliche Risiken und Anonymität geht. Im Bereich der Beschaffung, Konfiguration und Zugänglichkeit bietet die Software ebenfalls eine solide Umsetzung, jedoch treten für unsichere Nutzer bereits Hürden bei der Installation und der anfänglichen Navigation innerhalb des Netzwerks auf.

3.3.6 Zukunftsausblick

Das i2P-Projekt hat noch viel Potential, um ausgebaut und weiterentwickelt zu werden. Dies ist nicht verwunderlich, da es sich nach wie vor in einer Beta-Entwicklungsphase befindet. Besonders auffällig wird dieser Umstand auf der Projektseite. Diese wechselt sporadisch zwischen Sprachen und ist auf Hinblick der Dokumentation noch verbesserungswürdig. Trotzdem ist das Projekt auf einem interessanten Weg, wenn es um Technologie geht und hat genau wie die beiden anderen Vertreter ein treues Team an seiner Seite. Daher lässt sich sagen, dass die Entwicklung mit Sicherheit weitergehen wird, wenn auch mit langsamen Schritten. Da es das jüngste der drei Projekte ist und einen gänzlich anderen Ansatz verfolgt, kann damit gerechnet werden, dass noch grundlegende Änderungen und Wendepunkte auftreten könnten.

I2P selbst stellt auf seiner Webseite klar, dass es noch viele ausbaufähige Punkte gibt, sowie Probleme, auf die noch Antworten gefunden werden müssen [61].

Es ist ebenfalls zu erwarten, das I2P als Komponente in andere Darknet-Lösungen integriert wird. Dies ist durch den Aufbau des Netzwerks möglich, da es sich um eine separate eigene Kommunikationsschicht handelt. Entsprechende Überlegungen sind bereits aus dem Freenet-Wiki zu entnehmen [62].

3.4 Methodische Vorgehensweise

Es sollen zwei konkrete Aussagen getroffen werden. Zum einen soll aus der Gegenüberstellung der drei Darknet-Vertreter ein klares Fazit bezüglich Usability und Anonymität gezogen werden. Zum anderen muss geklärt werden, ob diese Arbeit ihren Zweck der Aufklärungsarbeit zu diesem Thema erfüllt. Um diese Ziele zu erreichen, erfolgt eine abschließende Auswertung und Analyse der Untersuchungen zu TOR, Freenet und I2P, sowie eine Leserumfrage, die klären soll ob die Leser sich nun besser mit der Thematik der Darknets und ihrer Anonymität zurechtfinden.

3.4.1 Leserumfrage

Die Leserumfrage soll überprüfen, ob diese Arbeit ihrem Aufklärungsanspruch gerecht wird. Um eine konkrete Aussage darüber treffen zu können, für welche Zielgruppe die Arbeit den größten Nutzen erzielt, werden je drei Personen, mit unterschiedlichem Vorwissen befragt. Die erste Kategorie von Befragten sollte sich noch nie aktiv mit dem Thema befasst haben. Eine weitere Gruppe sollte sich schon oberflächlich mit der Thematik auskennen, durch zum Beispiel Medien oder eigene Recherche, und die dritte Kategorie von Testpersonen sollte einige Kenntnisse über Netzwerke besitzen, da diese Grundlage der Darknets bilden. Die Testpersonen bekommen eine Kurzfassung der Arbeit zu lesen. Diese besteht grundlegend aus der Begriffsklärung des Darknets sowie die geschichtlichen Hintergründe und Funktionsweisen der drei Vertreter. Der Fragebogen [Anhang 1] ist zu diesem Zweck gegliedert in Teil A, welcher vor dem lesen der Kurzfassung ausgefüllt werden soll, und Teil B, der nach dem Lesen ausgefüllt wird. Durch den Vergleich der Teile lässt sich anschließend eine Aussage über den Wissens- und Verständnisgewinn treffen.

4 Analyse und Interpretation

Der erste Teil der Auswertung in diesem Kapitel befasst sich damit, die Untersuchungsergebnisse der Analyse von TOR, Freenet und I2P in Relation zu bringen. Unter der Teilüberschrift „4.2 Interpretation der Umfrageergebnisse“, wird die Auswertung der Fragebögen interpretiert werden um eine Qualitätsbewertung treffen zu können.

4.1 Analyse des Vergleichs von TOR, Freenet und I2P

In Tabelle 3, wurden die Usability-Kriterien für jedes des drei Darknets, in einem Benotungssystem von eins bis fünf, gegenübergestellt. Dies geschah basierend auf den Untersuchen in Kapitel 3.

Usability-Kriterien	**TOR**	**Freenet**	**I2P**
Beschaffung	1	1	2
Installation	2	3	4
Einstellungen	2	3	3
Navigation: Optionen	3	4	2
Zugänglichkeit	1	4	3
Navigation: Netzwerk	5	3	4
Anonymität	2	5	2
Rechtliche Risiken	4	2	1
Deinstallation / Abschaltung	1	3	3

Tabelle 3: Usability-Auswertung auf Grundlage des Vergleiches der Vertreter
(1 = leichte Handhabung – 5 = schwierige Handhabung)

Unter den drei betrachteten Vertretern stellt sich das TOR-Projekt klar als die bekannteste und nutzerstärkste Lösung heraus. Insbesondere das Alleinstellungsmerkmal des eigenen Browsers bildet einen Grund für diese Entwicklung, da es den Zugang und die Verfügbarkeit des Netzwerks erleichtert. Während Freenet einige Stunden Vorlaufzeit braucht, um nach dem Starten seine volle Geschwindigkeit zu erreichen und man unter I2P erst den eigenen Browser konfigurieren muss, kann der TOR-Browser beliebig gestartet und geschlossen werden. Dadurch entsteht für den Nutzer eine bequeme Flexibilität. Ein Begleitphänomen der großen Nutzerbasis ist ständig wachsender Inhalt, wodurch eine Suche

schneller zum Erfolg führt. Obwohl Freenet und I2P hinsichtlich Anonymität und rechtlichen Risiken die besseren Alternativen sind, beschränkt sich die Community auf Mitwirkende, Entwickler und besonders an diesem Projekt interessierte Personen. Dies lässt die Annahme zu, das Bequemlichkeitskriterien für den Nutzer stärker gewichtet sind als Sicherheitskriterien.

Betrachtet man den finanziellen Hintergrund, so scheint Freenet die sicherste Position einzunehmen. Zwar erhält das TOR-Projekt wesentlich höhere Geldzahlungen, diese stammen jedoch zu einem Großteil aus staatlichen Quellen. In Anbetracht des Negativimages, das TOR aufbaut, ist kritisch zu bewerten, ob diese Geldquellen eine langfristige Lösung darstellen. Freenet hingegen erhält neben Geldspenden auch noch Sachspenden, die für die Entwicklung des Projekts einen großen Nutzen erzielen. Außerdem ist es in der Lage, sich durch den eigenen Shop teilweiße selbst zu tragen und gewinnt somit eine gewisse Unabhängigkeit. I2P schneidet in dieser Kategorie am schlechtesten ab, da das Projekt trotz seines Erfolges noch relativ klein ist und somit deutlich weniger Geld zur Verfügung gestellt bekommt.

Auch wenn die Art und Weise, wie Anonymität innerhalb der drei Vertreter auf technischer Ebene aufgebaut wird in ihrer Grundsubstanz sehr ähnlich wirkt, stellt sich bei näherer Betrachtung jedoch heraus, dass die Ansätze sehr verschiedene Richtungen einschlagen. Das bietet einen interessanten Spielraum für zukünftige Entwicklungen auf diesem Themenfeld. Die unterschiedlichen Ansätze haben ebenfalls zur Folge, dass eine konkrete Vorstellung davon, wie ein Darknet eigentlich aussehen sollte, nur schwer zu formen ist und so zum mysteriösen Ruf der Netzwerke beiträgt. I2P scheint hier jedoch die größte Sicherheit zu bieten, da TOR durch verstärkte Überwachung ein Ziel für professionelle und teure Überwachung darstellt und Freenet nur im eigentlichen Darknet-Modus eine verlässliche Verschleierung bietet, da für Neueinsteiger der Unterschied zwischen den Modi jedoch nicht klar ersichtlich ist, können hier leicht Fehler entstehen.

Was zukünftige Entwicklungen betrifft, bildet TOR das Schlusslicht. Zwar bieten Finanzlage und Community viel Raum zur Weiterentwicklung, doch durch seine Größe und den großen medialen Druck, der auf dem Projekt lastet, entwickelt es sich deutlich langsamer und schwerfälliger als die kleineren, verwandten Projekte. Das größte Potential bietet hier I2P. Durch den einzigartigen Aufbau über Dienste und Anwendungen ist es in andere Projekte integrierbar und hat daher das größte Potential.

4.2 Interpretation der Umfrageergebnisse

Die Umfrageergebnisse zeigen deutlich, dass die Wahrnehmung des eigenen Vorwissens zum Thema der anonymen Nutzung des Darknets, innerhalb der drei Kategorien, stark auseinander gehen. Dies kann dadurch begründet werden, dass jeder der Befragten die Problematik aus einem anderen Blickwinkel wahrnimmt. Trotzdem ist ein klarer Unterschied zwischen den Befragten ohne Vorwissen und den beiden anderen Gruppen zu sehen. Während die Personen ohne Vorwissen einen sehr allgemeinen Blick auf das Thema haben, werden die Personen mit Netzwerkkenntnissen vor allem auf technischer Ebene darauf schauen, was die Betrachtung des Themas etwas einschränkt und übersichtlicher gestaltet. Bei der Frage nach bekannten Darknets antworteten sieben von neun Befragten mit TOR. Dies verdeutlicht den höheren Bekanntheitsgrad dieses Vertreters, der in der Arbeit bereits angesprochen wurde und lediglich Personen, die sich bereits mit Netzwerken beschäftigen, kennen mindestens einen der anderen Vertreter. Jedoch haben lediglich zwei Testpersonen das Darknet bisher genutzt, um nach Informationen zu suchen. Dabei wurden im Wesentlichen drei Gründe von allen Beteiligten genannt: Fehlende Notwendigkeit, Schwierigkeiten bei der Nutzung der jeweiligen Software und die Angst vor rechtlichen Problemen. Daran ist zu erkennen, dass die Angst davor, eventuell durch die Nutzung eines Darknets etwas Illegales zu tun oder darin verwickelt zu werden, die Angst vor Überwachung noch überwiegt. So das die Mühe der Nutzung von Darknet-Technologie, den Vorteilen die man daraus gewinnen könnte nicht gerecht wird. Dieses Ergebnis ist allerdings nicht überraschend, da in Deutschland, im Gegensatz zu einigen anderen Ländern, nur wenige Konsequenzen für kritische Meinungsäußerungen zu erwarten sind. Es wird weiterhin deutlich, dass in mindestens einem Fall grundsätzliches Interesse für die Thematik besteht, jedoch bestimmte Kriterien vor der Nutzung des Darknet-Zugangs abschrecken.

Teil A

Befragter	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Vorwissen	*Ohne Vorwissen*			*Mäßiges Vorwissen*			*Informiert*		
Frage 1	*2*	*3*	*1*	*6*	*7*	*6*	*4*	*6*	*7*
Frage 2	*Keines*	*TOR*	*Keines*	*TOR*	*TOR*	*TOR*	*TOR, I2P*	*TOR, I2P*	*TOR, Freenet, I2P,*
Frage 3	*Nein*	*Nein*	*Nein*	*Nein*	*Ja*	*Nein*	*Nein*	*Nein*	*Ja*

Tabelle 4: Auswertung der Leserumfrage Teil A

In der Auswertung von Teil B ist interessant zu beobachten, dass die Befragten mit mäßigem Vorwissen, also Vorwissen das aus eigenen Recherchen stammte, den größten Wissensgewinn vermerkten. Ein Grund dafür könnte das besondere persönliche Interesse an der Thematik sein, so dass der Wert der neu gewonnenen Informationen von dieser Person als besser gewertet wird als bei den beiden anderen befragten. Im Gegensatz dazu gaben die Personen, die mit Wissen über Netzwerktechnik an die Thematik herangehen, einen vergleichsweise geringen Zuwachs an Verständnis. Es ist zu vermuten, dass hier die Erwartung nach einer tiefergehenden technischen Aufklärung bestand, allerdings nur rudimentär erfüllt wurde. Trotz des schwankenden Ergebnisses der ersten Frage, nach der Quantität des neuerworbenen Verständnisses, gab jeder Befragte an, sich nun besser informiert zu fühlen. Dies spricht durchaus für den Aufklärungsaspekt der Arbeit, auch wenn der konkrete Wert je nach Leser variiert. Eine solche Variation ist unvermeidlich, da jeder Leser subjektiv an die Bewertung seines Vorwissens und des neuen Wissens herangeht. Jedoch ist anzunehmen, dass die befragte Person ohne Vorwissen, die neuerworbenen Informationen nicht in praktischen Nutzen umsetzen werden, da sie sich entweder nicht in der Lage fühlen eine solche Software zu nutzen oder die rechtlichen Risiken nicht einschätzen können. In den Kategorien mit mäßigen Vorwissen und informierten Befragten, besteht prinzipiell die Möglichkeit auf eine zukünftige Nutzung der Netzwerke. Lediglich eine dieser Testpersonen, gab an, Probleme bei der Einschätzung der rechtlichen Bedingungen zu haben.

Teil B

Befragter	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Vorwissen	*Ohne Vorwissen*			*Mäßiges Vorwissen*			*Informiert*		
Frage 1	*8*	*8*	*6*	*9*	*10*	*10*	*6*	*4*	*5*
Frage 2	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*
Frage 3	*Ja*	*Nein*	*Ja*	*Ja*	*Ja*	*Ja*	*Nein*	*Ja*	*Ja*
Frage 4	*Nein*	*Ja*	*Nein*	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*	*Ja*
Frage 5	*8*	*10*	*4*	*8*	*10*	*9*	*8*	*7*	*7*

Tabelle 5: Auswertung der Leserumfrage Teil B

Wenn es um die zukünftige kritische Bewertung von Artikeln und Medien zu diesem Thema geht, geben jedoch alle Befragten an, diese besser bewerten zu können, womit das Kernziel der Arbeit eindeutig erfüllt wurde.

5 Fazit & Zukunftsausblick

Zielsetzung der vorliegenden Arbeit war es, Aufklärungsarbeit über das umfangreiche Thema der Darknets und der dort gebotenen Anonymität zu leisten. Dazu wurden zunächst grundlegende Begrifflichkeiten definiert und eine Wissensbasis geschaffen. In einem zweiten Schritt wurden die drei größten Vertreter TOR, Freenet und I2P vorgestellt und hinsichtlich ihrer organisatorischen Struktur, Nutzergruppen, technischen Grundlagen und Usability-Kriterien untersucht.

Zusammenfassend spiegeln die Ergebnisse wieder, dass das TOR-Projekt wesentliche Vorteile aus seiner Bekanntheit und seinem geschichtlichen Hintergrund ziehen kann, allerdings in Sachen Sicherheit noch einiges von seinen kleineren Nebenvertretern lernen kann. Alle drei Lösungen bieten für verschiede Nutzergruppen attraktive Vorteile und sind noch ausbaufähig. Dabei stehen sehr unterschiedliche treibende Kräfte hinter den jeweiligen Projekten und beeinflussen die zukünftige Richtung derer Entwicklung maßgeblich.

Die Ergebnisse dieses Vergleichs können als Grundlage für zukünftige Vertiefungen der jeweiligen Netzwerkstrukturen dienen oder genutzt werden, um die Thematik aus einem rechtlichen oder sozialen Gesichtspunkt zu betrachten.

Abkürzungsverzeichnis

FAQ = frequently asked questions (Deutsch: häufig gestellte Fragen)

TOR = The Onion Routing (Beschreibt das Verfahren der Datenübertragung), wird jedoch oft als Abkürzung für das Darknet „The TOR-Project“, selbst verwendet

I2P = Invisible Internet Project (deutsch: Unsichtbares Internet Projekt)

NGO = Non-governmental organization (Deutsch: Nicht-Regierungsorganisation)

CIA = Central Intelligence Agency

DRL = Bureau of Democracy, Human Rights and Labor Affairs (deu.: Büro für Demokratie, Menschenrechte und Arbeitsangelegenheiten)

RFA = Radio Free Asia (Deutsch: Freies Radio Asien)

BKA = Bundeskriminalamt

BSI = Bundesamt für Sicherheit in der Informationstechnik

Quellenangaben

[1] RP-Online, 20.Juli 2017

[2] Computer Bild, 23.Mai 2017

[3] Kölner Stadt-Anzeiger, 26.Oktober 2017

[4] Spiegel Online, 14.Januar 2018

[5] Spiegel Online, 07.Januar 2018

[6] Statista, 2016

[7] Daniel Moßbrucker; Netz der Dissidenten: die Helle Seite im Darknet; **Aus Politik und Zeitgeschichte – Darknet,** November 2017; s. 16

[8] Motherboard.vice.com, "Wollte mich die NSA mit dem schwierigsten Rätsel von 4Chan rekrutieren?", Mai 2015

[9] Stefan Mey, „"Tor" in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets"; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 04

[10] Stefan Mey, „"Tor" in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets"; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 07

[12] Heise Online 31.Oktober 2014

[13] Netzpolitik.org, „Clearnet war gestern – BKA präsentiert das Surface Web", 27.07.2016

[14] Alexander Weikert, Die Entstehung von Darknets und der Zugang zu den anonymen Netzwerken, 2016, s.03

[15] „Deep Web – Arten des Deep Web", https://de.wikipedia.org/wiki/Deep_Web, (abgerufen am 18.04.2018)

[16] Alexander Weikert, Die Entstehung von Darknets und der Zugang zu den anonymen Netzwerken, 2016, s.5

[17] „Definition Darknet", https://www.searchsecurity.de/definition/Darknet (abgerufen am 15.04.2018)

[18] „Kryptographie", https://de.wikipedia.org/wiki/Kryptographie (abgerufen am 23.04.2018)

[19] Albrecht Beutelspacher, „Eine kurze Geschichte der Kryptografie"; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 35

[20] Stefan Mey, „"Tor" in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets"; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 09

[21] Matthias Schulze, „"Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten"; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 25

[22] Daniel Moßbrucker; „Netz der Dissidenten: die Helle Seite im Darknet“; **Aus Politik und Zeitgeschichte – Darknet,** November 2017; s. 20

[23] „Geheime Dokumente: Der BND hat das Anonymisierungs-Netzwerk Tor angegriffen und warnt vor dessen Nutzung“, https://netzpolitik.org/2017/geheime-dokumente-der-bnd-hat-das-anonymisierungs-netzwerk-tor-angegriffen-und-warnt-vor-dessen-nutzung/ (abgerufen am 22.04.2018)

[24] Daniel Moßbrucker; „Netz der Dissidenten: die Helle Seite im Darknet“; **Aus Politik und Zeitgeschichte – Darknet,** November 2017; s.21

[25] Daniel Moßbrucker; „Netz der Dissidenten: die Helle Seite im Darknet“; **Aus Politik und Zeitgeschichte – Darknet,** November 2017; s.16

[26] Matthias Schulze, „“Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten“; **Aus Politik und Zeitgeschichte – Darknet** , November 2017, S. 25

[27] „Usability“, https://de.wikipedia.org/wiki/Usability (abgerufen am 26.04.2018)

[28] „Qualitätscheck: 13 Usability-Kriterien für erfolgreiche Webseiten“, https://www.interactive-tools.de/Interactive-Insights/Qualitaetscheck-13-Usability-Kriterien-fuer-erfolgreiche-Webseiten (abgerufen am 27.04.2018)

[29] „Markieren Sie Ihre Ziele“, https://www.skopos-nova.de/usability.html (abgerufen am 27.04.2018)

[30] „Anonymität“, https://de.wikipedia.org/wiki/Anonymität (abgerufen am 22.04.2017)

[31] „Was ist Anonymität?“, https://www.bsi.bund.de/DE/Publikationen/Studien/Anonym/wasistanonymitaet.html (abgerufen am 22.04.2018)

[32] „Anonymität im Internet“, https://de.wikipedia.org/wiki/Anonymität_im_Internet#Maßnahmen_zum_Schutz_der_Anonymität (abgerufen am 26.04.2018)

[33] „TOR: Overview“, https://www.torproject.org/about/overview.html.en (abgerufen am 26.04.2018)

[34] Daniel Moore/ Thomas Rid, Cyrptopolitik and the Darknet, in: Survival 1/2016, S. 7.38

[35] “Tor metrics”, http://metrics.torproject.org (abgerufen am 13.03.2018)

[36] Stefan Mey, „“Tor“ in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets“; November 2017, S. 06

[37] Stefan Mey, „“Tor“ in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets“; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 05

[38] „Tor: Sponsors“, https://www.torproject.org/about/sponsors.html.en (abgerufen am 26.04.2018)

[39] „Tor: Financial Report“, https://www.torproject.org/about/findoc/2015-TorProject-combined-Form990_PC_Audit_Results.pdf (abgerufen am 27.04.2018)

[40] Stefan Mey, „“Tor“ in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets“; **Aus Politik und Zeitgeschichte – Darknet,** November 2017, S. 08

[41] „Tor: People“, https://www.torproject.org/about/corepeople.html.en (abgerufen am 27.04.2018)

[42] „The Solution: a distributed, anonymous netzwork“, https://www.torproject.org/about/overview.html.en#thesolution (abgerufen am 27.04.2018)

[43] Anonymität im Netz mit Tor, Flyer des Chaos Computer Clubs, August 2010

[44] „Staying anonymous“, https://www.torproject.org/about/overview.html.en#thesolution (abgerufen am 27.04.2018)

[45] “Journalists and their audience use tor”, https://www.torproject.org/about/torusers.html.en (abgerufen am 28.04.2018)

[46] „Law enforcement officers use tor”, https://www.torproject.org/about/torusers.html.en (abgerufen am 28.04.2018)

[47] „9 Darknet Fragen“, https://motherboard.vice.com/de/article/wj8a9q/9-darknet-fragen-die-sich-jeder-stellt-aber-niemand-traut-zu-fragen (abgerufen am 03.05.2018)

[48] „What is freenet?“, https://freenetproject.org/pages/about.html (abgerufen am 26.04.2018)

[49] Stefan Mey, „“Tor“ in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets“; November 2017, S. 08

[50] „Freenet: A Distributed Anonymous Information Storage and Retrieval System”, https://web.archive.org/web/20070927194127/https://freenetproject.org/papers/freenet.pdf (abgerufen am 04.05.2018)

[51] „Freenet (software)“, https://de.wikipedia.org/wiki/Freenet_(Software)#Geschichte (abgerufen am 02.2018)

[52] Stefan Mey, „“Tor“ in eine andere Welt? : begriffe, Technologie und Widersprüche des Darknets“; November 2017, S. 07

[53] „Freenet (Software)“. https://de.wikipedia.org/wiki/Freenet_(Software)#Zukunft (abgerufen am 04.05.2018)

[54] „I2P – The invisible internet project”, https://staas.home.xs4all.nl/t/swtr/documents/wt2015_i2p.pdf (abgerufen am 04-05.2018)

[55] „I2P: Wie?“ https://geti2p.net/de/docs/how/intro (abgerufen am 10.03.2018)

[56] Alexander Weikert, Die Entstehung von Darknets und der Zugang zu den anonymen Netzwerken, 2016, s.12

[57] Alexander Weikert, Die Entstehung von Darknets und der Zugang zu den anonymen Netzwerken, 2016, s.11-13

[58] „I2P: FAQ-Generell“, https://geti2p.net/de/faq#down (abgerufen am 03.05.2018)

[59] „I2P: Realisierung“, https://de.wikipedia.org/wiki/I2P#Funktionsweise (abgerufen am 05.05.2018)

[60] „How to use I2P“, https://www.bestvpn.com/use-i2p-idiots-starting-guide/ (abgerufen am 05.05.2018)

[61] „I2P: Zukunft“, https://geti2p.net/de/docs/how/tech-intro (abgerufen am 05.05.2018)

[62] „Freenet: Future, I2P“, https://de.wikipedia.org/wiki/Freenet_(Software)#Zukunft (abgerufen am 02.05.2018)

[63] https://de.wikipedia.org/wiki/Kademlia (abgerufen am 04.05.2018)

[64] https://geti2p.net/de/docs/how/intro (abgerufen am 04.05.2018)

Anhänge

Anhang 1: Leserumfragebogen

Leserumfrage zur Bachelorarbeit: Anonymität im Darknet

Teil A: Vor dem Lesen der Arbeit zu beantworten

1) *Auf einer Skala von 1 bis 10, wie hoch schätzen Sie ihr Vorwissen zu der Thematik „Anonymität im Darknet" ein? (1 = Gar kein Vorwissen, 10 = Umfangreiches Wissen)*

1	2	3	4	5	6	7	8	9	10

2) *Welchen der unten genannten Darknet-Vertreter kennen Sie bereits? (namentlich genügt, bitte ankreuzen)*

The Onion Routing Network (TOR)	
Freenet	
Invisible Internet Project (I2P)	

3) *Haben sie bereits im Darknet nach Inhalten gesucht?*

☐ Ja

☐ Nein

a. *Falls Ja: Wie erfolgreich war Ihre Suche? (1= Erfolglos, 10= Komplett zufriedenstellend)*

1	2	3	4	5	6	7	8	9	10

b. *Falls Nein: Nennen Sie einen Grund!*

Teil B: Nach dem Lesen der Arbeit zu beantworten

1) *Fühlen Sie sich allgemein besser informiert über die Anonymität im Darknet? (1 = weniger als zuvor, 10 = wesentlich besser)*

1	2	3	4	5	6	7	8	9	10

2) *Haben Sie ein besseres Verständnis über Angebot verschiedener Darknets?*

☐ Ja

☐ Nein

3) *Haben Sie das Gefühl, die Risiken und Vorteile der Darknet-Nutzung nun besser einschätzen zu können?*

☐ Ja

☐ Nein

4) *Fühlen Sie sich in der Lage selbstständig eines der Darknets zu nutzen? (Unabhängig von der Notwendigkeit)*

☐ Ja

☐ Nein

5) *Haben Sie das Gefühl, Nachrichten und Artikel zu diesem Thema nun besser einschätzen zu können? (1 am schlechtesten, 10 am besten)*

1	2	3	4	5	6	7	8	9	10

Vielen Dank, dass Sie sich die Zeit genommen haben meine Arbeit zu lesen und an dieser Umfrage teilzunehmen!
Ich hoffe Sie konnten dem Text ein wenig neues Wissen entnehmen und in Zukunft nutzen.

Julia Görmer | Hochschule Anhalt | Fachbereich 5

Eidesstattliche Versicherung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbständig, ohne fremde Hilfe angefertigt worden ist. Alle Inhalte, die aus fremden Quellen stammen und direkt bzw. indirekt übernommen wurden, wurden kenntlich gemacht. Keine außer der im Literaturverzeichnis angegebenen Literaturquellen und der im Abbildungsverzeichnis angegebenen Abbildungen wurden für diese Arbeit verwandt. Diese Arbeit wurde bislang noch nicht veröffentlicht.