Darknet und Politik

- *Handout zum Vortrag in der Rabryka am 29.09.2021, Görlitz*
- *Stefan Mey, Berlin, Journalist*innenbüro Schnittstelle, Autor eines Sachbuchs zum Darknet*

(1) Der Tor-Browser

Mit dem Tor-Browser kann man anonym und zensurfrei im „normalen“ Internet surfen und Darknet-Webseiten betreten (die stets mit .onion enden).

Der Tor-Browser auf PC

• downloadbar unter https://www.torproject.org
• "Benutzerhandbuch" des Tor Projects zum Tor-Browser: https://tb-manual.torproject.org/de/
• z. B. Erläuterung zu Bridge-Knoten (die kommen zum Einsatz, wenn Länder Tor generell blockieren): https://tb-manual.torproject.org/de/bridges/
• Tor-Seite zu Brücken-Knoten: https://bridges.torproject.org/

Der Tor-Browser auf dem Smartphone

• (Android) Tor Browser for Android: https://play.google.com/store/apps/details?id=org.torproject.torbrowser&hl=de
• (iOS) OnionBrowser von Mike Tigas: https://itunes.apple.com/de/app/onion-browser/id519296448?mt=8

Achtung: In den App-Stores werden viele Tor-Apps angeboten, bei denen nicht immer klar ist, wie seriös und sauber sie sind. Das Tor Project empfiehlt die beiden genannten Apps.

(2) Andere Darknet- und Tor-Programme

OnionShare: anonym Daten tauschen

• Download: https://OnionShare.org
• OnionShare erzeugt auf dem eigenen Rechner eine temporäre Darknet-Adresse. Aus der kann man (a) eine Download-Station machen, über das andere Leute freigegebene Dokumente vom eigenen Rechner herunterladen können, (b) ein Postfach machen, über das andere einem Dateien zukommen lassen und (c) einen Chatraum machen
• Die „andere Seite“ muss das OnionShare-Programm nicht installiert haben. Die jeweilige Person öffnet die von OnionShare erzeugte Darknet-Adresse einfach mit dem Tor-Browser.
• Vorstellung der Funktionen von OnionShare: https://docs.onionshare.org/2.3.2/de
• Achtung: Onionshare hat keinen eigenen Virenscanner eingebaut. Gebt die Postfach-Adresse deswegen am besten nur Leuten, die ihr kennt und denen ihr vertraut.

Ricochet Refresh: Darknet-PC-Chatprogramm

• https://www.ricochetrefresh.net
• Ricochet Refresh ist ein sehr simples Darknet-basiertes Text-Chatprogramm für PC. Beide Seiten der Kommunikation müssen Ricochet Refresh auf ihrem Rechner installiert haben.

Briar: Darknet-Chat-App für Smartphones (nur Android)

• https://briarproject.org
• Briar ist eine Messenger-App für Android. Man kommuniziert über Darknet-Adressen, direkt von Handy zu Handy, ohne eine Datenbank „dazwischen“. Das ist maximal datensparsam. Briar bringt allerdings einige Funktionseinschränkungen mit: Briar gibt es nur für Android und nicht für iOS. Es

sind nur Nachrichten möglich, aber keine Telefonie. Und beide Seite der Kommunikation müssen gleichzeitig online sein, da Nachrichten nirgendwo zwischengespeichert werden.
• verfügbar im Play-Store: https://play.google.com/store/apps/details?id=org.briarproject.briar.android und über F-Droid: https://briarproject.org/installing-briar-via-f-droid/
• Erklärartikel zu Briar (Sept 18): https://mobilsicher.de/kategorie/whatsapp-und-messenger/messenger-app-briar-kurz-vorgestellt

Orbot: Tor-VPN-App für Android

• Überblicksseite des Tor Projects zu Orbot: https://2019.www.torproject.org/docs/android.html.en
• Orbot im Play-Store: https://play.google.com/store/apps/details?id=org.torproject.android&hl=de&gl=US
• Orbot ist eine Art VPN-App, mit der sich jeglicher Datenverkehr eines Android-Smartphones über Tor leiten lässt.
• Erklärartikel zu Orbot: https://mobilsicher.de/ratgeber/beliebige-apps-ueber-tor-nutzen-android (Stand August 2018)

Tails: hyperanonymes Live-Betriebssystem

• https://tails.boum.org
• Tails ist ein Linux-basiertes Betriebssystem auf dem USB-Stick. Man kann den Rechner über den USB-Stick temporär über Tails laufen lassen. Es verbleiben bei korrekter Nutzung keinerlei Spuren auf den Rechner und auch nicht auf dem USB-Stick. Besonders ist, dass sämtlicher Datenverkehr standardmäßig über Tor läuft.
• Über Tails: https://tails.boum.org/about/index.de.html
• Für Tails gibt es eine sehr gute deutschsprachige Anleitung (PDF): https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2021/04/Tails-2021-04-12.pdf
• Achtung: Die Nutzung von Tails geschieht auf eigenes Risiko. Bitte, wie bei jeder Veränderung am Betriebssystem, vorher ein Backup des Geräts machen.

(3) Hintergrund: Tor, das Darknet und der Tor-Browser

Hintergründe Tor und Darknet
• Frühe Geschichte von Tor https://www.onion-router.net/History.html
• Artikel zur Tor-Geschichte https://www.heise.de/hintergrund/Missing-Link-25-Jahre-Anonymisierung-mit-Tor-eine-Geschichte-mit-Widerspruechen-4972675.html?seite=all
• Überblicksartikel in der APUZ (2017): https://www.bpb.de/apuz/259135/tor-in-eine-andere-welt?p=all

Zahlen und Daten zum Tor-Netzwerk und zum Darknet
(Nutzer*innen)
• Tor-User insgesamt https://metrics.torproject.org/userstats-relay-country.html
• Tor-User nach Ländern https://metrics.torproject.org/userstats-relay-table.html
• Tor-User Deutschland https://metrics.torproject.org/userstats-relay-country.html?graph=userstats-relay-country&country=de

(Tor-Knoten)
• Tor-Knoten aus Deutschland https://metrics.torproject.org/rs.html#search/country:de
• Die größten Tor-Knoten-Familien https://nusenu.github.io/OrNetStats/#relay-families-by-consensus-weight

• Die zehn „Hüter*innen des Tor-Netzwerks“, die Authority Directories, die einen Überblick über alle verfügbaren Tor-Knoten erstellen und die einzelne Knoten aus dem Netzwerk werfen können: https://metrics.torproject.org/rs.html#search/flag:Authority

(4) Das politische Darknet

→ Darknet-exklusive Inhalte

• Da gibt es kaum etwas.

→ das Darknet als Programmbaustein

• die Darknet-Programme Onionshare, Ricochet, Briar (siehe oben)

→ das Darknet als alternative Zugangstür

• **Linke Kollektive im Darknet**: Akteur*innen der linken Zivilgesellschaft haben Darknet-Parallelpräsenzen eingerichtet, z.B. ...

• IT-Kollektiv Riseup im Darknet:
http://vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion/de

• IT-Kollektiv Systemli im Darknet:
http://7sk2kov2xwx6cbc32phynrifegg6pklmzs7luwcggtzrnlsolxxuyfyd.onion/

• Systemli und Riseup sind eigentlich im „normalen Internet“ vertreten, unter www.systemli.org und https://riseup.net. Für ihre Hauptseite und für die einzelnen Kommunikationswerkzeuge haben sie aber auch parallele Darknet-Adressen eingerichtet.

• Liste der verschiedenen Darknet-Präsenzen von Systemli:
https://www.systemli.org/service/onion/
Liste der verschiedenen Darknet-Präsenzen von Riseup: https://www.riseup.net/en/tor

• die deutschsprachige Indymedia im Darknet:
http://gsxbcjvcrdl66ycimkwra2nxzwvy2idef4twi7elojuzm5ztt5abqyid.onion/

• Weitere Parallelpräsenzen im Darknet:

• die Meta-Suchmaschine Metager:
http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhlvdgsswvo6ii4akgyd.onion

• FragdenStaat.de (eine deutsche Webseite für Informationsfreiheitsanfragen):
http://fdstaat23zv6kdmntgkvdzkr7hipl5oqswwi3xawzkj2w2gwsbxmrwyd.onion

• Nuudel, ein (schlichtes) Umfrage- und Terminfindungs-Tool des deutschen Vereins Digital Courage: http://cca4yrsk4qza2jrg7maf2ltphqeqo6a7hrazacfgrvq427wgeakevfid.onion/

• Links bzw. Verweise zu weiteren Parallel-Webseiten im Darknet finden sich auf:
https://github.com/alecmuffett/real-world-onion-sites

• Außerdem würde ich die **Darknet-Whistleblower-Postfächer von Medien** zum politischen Darknet zählen, zum Beispiel:

• Postfach der SZ: http://udhauo3m3fh7v6yfiuornjzxn3fh6vlp4ooo3wogvghcnv5xik6mnayd.onion, Landing Page des Postfachs: https://www.sueddeutsche.de/projekte/kontakt/, Interview zum SZ-Postfach: http://get.torial.com/blog/2019/07/sz-postfach-securedrop-kann-eine-art-lebensversicherung-fuer-whistleblower-sein/

• Spiegel-Postfach: http://kxenegnp5vjtzfifupdaibxckguzitxyuqo2qoyj5riumorb54l3zdqd.onion, Landing Page: https://www.spiegel.de/extra/so-nehmen-informanten-sicheren-kontakt-zum-spiegel-auf-a-1030502.html

• Heise Tippgeber:
http://ayznmonmewb2tjvgf7ym4t2726muprjvwckzx2vhf2hbarbbzydm7oad.onion, Landing Page: https://www.heise.de/investigativ, Hinter den Kulissen des Postfachs:

https://www.heise.de/select/ct/2016/17/1471512410860907
- AfriLeaks (Gemeinschaftspostfach afrikanischer Medien)
http://f3mryj3e2uw2zrv3zv6up6maqosgzn27frz7xodvpl7pkestoyigtkad.onion/, Landing Page: https://afrileaks.org
- Sourcesûre (Gemeinschaftspostfach französischsprachiger Medien): Postfach: http://2xb4llzwxnmr2ccx4ospauepczqfrzhghe63rztik5pqkdbfzq3242yd.onion/, Landing Page: https://www.sourcesure.eu