



# 2017/43 dschungel

<https://jungle.world/artikel/2017/43/die-im-dunkeln-sieht-man-nicht>

**Im Darknet lebt das unregulierte Web der Neunziger fort**

## **Die im Dunkeln sieht man nicht**

Von **Enno Park**

**Wenn vom Darknet die Rede ist, geht es meistens um Drogen- oder Waffenhandel. Aber das Netzwerk ist für verfolgte Minderheiten und Dissidenten auch eine Möglichkeit, die staatliche Zensur zu unterlaufen.**

Immer wieder tauchten im Darknet Missbrauchsszenen eines kleinen Mädchens auf. Das Bundeskriminalamt ging Anfang Oktober mit den Bildern an die Öffentlichkeit und konnte inzwischen einen dringend Tatverdächtigen festnehmen. Im Juli 2016 tötete David S. vor einem Münchner Einkaufszentrum neun Menschen. Seine Waffe hatte er sich im Darknet beschafft.

Wer die Schlagzeilen verfolgt, verbindet mit dem Darknet vor allem Kriminalität der üblen Sorte. Eine Google-Suche nach dem Begriff »Darknet« ergibt eine lange Liste solcher Meldungen, die fast schon lustvoll den Sündenpfuhl des Internets beschreiben. Das Darknet scheint alles zu bieten, was der Verbrecher begehrt: Waffen, Drogen, Hacks und Zero Day Exploits, erbeutete Passwörter, Facebook-Likes im Tausenderbündel, Falschgeld, Pässe, Kinderpornographie und versklavte Menschen.

### **Ein digitaler Mythos**

Dazwischen tauchen vereinzelt Anleitungen in den Suchergebnissen auf, die erklären, wie man ins Darknet gelangt.

Das dunkle Netz ist ein digitaler Mythos. Es stellt sich die Frage: Warum wird das Darknet nicht geschlossen und wie ist es technisch möglich, dass es im gut überwachten Internet einen Raum der Anonymität überhaupt gibt? Um dies zu beantworten, muss man wissen, wie das Netz technisch funktioniert. Auch gilt es zu unterscheiden: Häufig wird das Darknet mit dem sogenannten Deep Web verwechselt. Das Deep Web ist jener Teil des Internets, der nicht ohne weiteres mit Suchmaschinen wie Google zugänglich ist. Seine Inhalte kann man erst sehen, wenn man sich auf einer Website mit Namen und Passwort angemeldet hat. Zum Deep Web gehören Datenbanken aller Art, wissenschaftliche Publikationen hinter Bezahlschranken, Bibliothekskataloge oder auch die Profile auf Dating-Seiten.

Das Darknet ist etwas völlig anderes. Es entstand zusammen mit dem Browser Tor und dem Netzwerk Onion kurz nach dem Jahr 2000. Ziel war, eine völlig anonyme Kommunikation im Internet herzustellen. Wer heutzutage eine Website besucht, hinterlässt dort seine IP-Adresse. Provider wie die Telekom wissen, welcher Anschluss zu welcher Zeit die jeweilige IP-Adresse hat. Ermittlungsbehörden können so die Quelle ausfindig machen, wenn sie im Netz illegale Aktivitäten registrieren. Das ist auch der Grund für die Einführung der Vorratsdatenspeicherung, die im Juni allerdings gerichtlich wieder unterbunden wurde: Die Provider sollen für einen bestimmten Zeitraum speichern, wer wann welche IP-Adresse hatte, damit Polizei und Staatsanwaltschaft darauf zugreifen können.

Um die eigene IP-Adresse zu verschleiern, kann man das Tor-Netzwerk benutzen. Der Computer verbindet sich beim Besuch einer Website nicht direkt mit dem Adressaten, sondern mit einem anderen Server des Tor-Netzwerks. Von dort wird das Datenpaket von einem Knotenpunkt zum nächsten geleitet, bevor es an den eigentlichen Adressaten ausgeliefert wird. Auf dem Weg dorthin wird es mehrfach verschlüsselt, bildlich gesehen wie die Schichten einer Zwiebel, die Stück für Stück entfernt werden müssen, um an den Kern zu gelangen. Daher der Name Onion-Routing. Der besuchte Webserver erkennt nicht, welche IP-Adresse der Besucher hat, sondern lediglich, dass die Anfrage aus dem Tor-Netzwerk stammt. Die Identität der Nutzer ist erfolgreich verschleiert. Die Tor-Knoten verteilen sich auf der ganzen Welt. Jeder technisch Versierte kann einen Knoten betreiben, was auch erklärt, warum das Darknet nicht einfach abgeschaltet oder gesperrt werden kann.

Der größte und wichtigste hidden service ist vermutlich Facebook, das im Darknet einen anonymen Zugang zum sozialen Netz und so die Möglichkeit anbietet, das Forum in Ländern zu nutzen, in denen es verboten ist.

Tor wird weltweit aus den unterschiedlichsten Gründen genutzt. Manche User wollen aus Prinzip nicht, dass ihre Aktivitäten im Internet nachvollziehbar sind. Andere haben handfeste Gründe, etwa weil sie wissen, dass sie von Geheimdiensten oder Ermittlungsbehörden überwacht werden. Andere leben in Ländern wie der Türkei, dem Iran oder China, in denen das Internet zensiert wird. Tor ist für diese Menschen eine Möglichkeit, auf Facebook oder Twitter zuzugreifen oder Nachrichten zu lesen, die in ihren Ländern unterdrückt werden. Außerdem wird Tor von Whistleblowern genutzt, die anonym Missstände auf Plattformen wie Wikileaks veröffentlichen wollen. Dieser anonymisierte Datenverkehr macht den Großteil des Datenaufkommens im Darknet aus. Jeder, der will, kann den Browser nutzen. Dazu muss er lediglich auf dem eigenen Rechner installiert werden.

Allerdings dient Tor nicht nur dazu, Kommunikation zu verschleiern. Hacker kamen auf die Idee, ganze Webserver im Tor-Netz zu verstecken. Sie sind von Google nicht auffindbar und können ohne Tor-Browser nicht aufgerufen werden. Um sie zu erreichen, muss man ihre Adresse kennen. Allerdings gibt es mittlerweile Verzeichnisse wie die Suchmaschine »Grams«, die helfen, sich im Darknet zu orientieren und solche hidden services zu finden. Diese Möglichkeit, versteckte Webserver zu betreiben, zieht auch Kriminelle an, die ihre

Dienste dort anbieten. Ein Problem war bislang die Bezahlung. Wer Kreditkartennummern angibt oder Banküberweisungen tätigt, hebt damit seine Anonymität auf. Richtig in Schwung kamen die illegalen Angebote erst, als es möglich wurde, mit Bitcoins auch anonym zu bezahlen.

### **Lebensversicherung für Whistleblower**

Einer Studie des britischen International Institute for Strategic Studies zufolge bieten 57 Prozent von 5 205 untersuchten Websites im Darknet illegale Dienste an. Der Rest besteht aus Foren und Websites aller Art. Zum Beispiel können Homosexuelle aus islamischen Ländern dort Kontakte knüpfen, ohne Entdeckung fürchten zu müssen. Der E-Mail-Provider Mailbox.org bietet eine Möglichkeit, über das Darknet anonym E-Mails zu lesen und zu versenden. Verlage bieten Briefkästen für Whistleblower im Darknet an. Das Magazin *The New Yorker* hat sogar eine ausführliche Anleitung zu deren Nutzung veröffentlicht. Ein bekannter Dienst ist »Dead Man Zero«. Whistleblower können dort ihr Material hochladen und müssen sich fortan täglich einmal am Dienst anmelden. Sobald sie das nicht mehr tun, geht der Dienst davon aus, dass der Person etwas zugestoßen ist und das Material wird automatisch veröffentlicht. Für Menschen, die brisante Daten besitzen, ist das eine Lebensversicherung.

Im Darknet lässt sich beobachten, ob und wie eine Gesellschaft ohne Regeln funktionieren könnte, wie Anarchisten und Libertäre sie sich bisweilen vorstellen. Das Ergebnis ist ein seltsames Nebeneinander von Freiheit und Hacker-Romantik auf der einen und Skrupellosigkeit auf der anderen Seite

Der größte und wichtigste hidden service ist vermutlich Facebook, das im Darknet einen anonymen Zugang zum sozialen Netz und so die Möglichkeit anbietet, das Forum in Ländern zu nutzen, in denen es verboten ist. Es ist eine Chance für Angehörige von unterdrückten Minderheiten, Dissidenten und Menschenrechtlern, sich international zu vernetzen. Deshalb verteidigen NGOs wie der Verein »Zwiebelfreunde« und »Reporter ohne Grenzen« das Darknet vor immer neuen Verbotsforderungen.

Tatsächlich ist das Darknet trotz der zweifellos dort stattfindenden kriminellen Aktivitäten etwas völlig anderes als ein Freihafen für Verbrecher. Vielmehr erinnert es an das unübersichtliche und unregulierte Web der neunziger Jahre. Dort lässt sich beobachten, ob und wie eine Gesellschaft ohne Regeln funktionieren könnte, wie Anarchisten und Libertäre sie sich bisweilen vorstellen. Das Ergebnis ist ein seltsames Nebeneinander von Freiheit und Hacker-Romantik auf der einen und Skrupellosigkeit auf der anderen Seite, was ein wenig an den wilden Westen erinnert. In jüngster Zeit gab es eine Reihe von erpresserischen DDoS-Attacken auf Online-Shops im Darknet. Die Idee der Angreifer: Wenn man einen illegalen Shop erpresst, wird der wahrscheinlich nicht zur Polizei gehen, sondern zahlen.

Insgesamt ist das Darknet längst nicht so sicher, wie allenthalben behauptet und geglaubt wird. Immer wieder melden Ermittlungsbehörden Fahndungserfolge im Darknet. Fast immer haben die Festgenommenen den Fehler gemacht, zwar anonym über Tor zu

kommunizieren, sich aber an anderer Stelle zu verraten, etwa indem sie E-Mail-Adressen angegeben haben, die zugeordnet werden konnten. Ermittlungsbehörden und Geheimdienste aus aller Welt haben ein großes Interesse daran, was im Darknet passiert, und wahrscheinlich gibt es kaum Server im Internet, die strenger bewacht werden als die exit nodes, die Ein- und Austrittsserver des Darknet. Eine Umkehrung des Anonymitätsversprechens: Wer das Darknet nutzt, sollte gute Gründe dafür haben und genau wissen, was er tut. Wer sich hier nicht sehr vorsichtig verhält, kann schnell enttarnt und verdächtigt werden. In Ländern wie Syrien kann allein die unvorsichtige Nutzung des Darknet oder das Vorhandensein des Tor-Browsers auf dem Laptop zur Verhaftung führen.