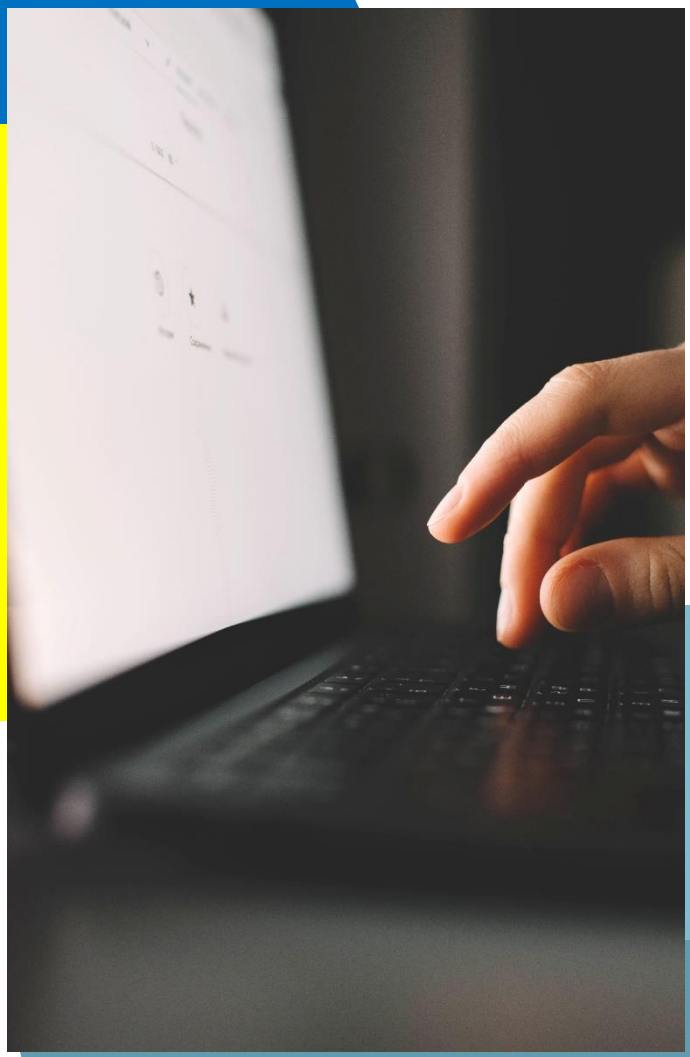
Leitfaden zur anonymen Kommunikation.



Anonymität kann entscheidend sein.

Wenn die eigene Welt auf dem Kopf steht und man sich auch Gedanken darüber machen muss, wer ggfs. mitliest, dann kann man eventuell durch die Kommunikation andere, wie Freunde und Familie, in Gefahr bringen.
Deshalb ist es in Krisen- und Kriegsgebieten wichtig, die Grundlagen der anonymen Kommunikation zu kennen.

Stand 2022

Anonyme Kommunikation bedeutet Sicherheit.

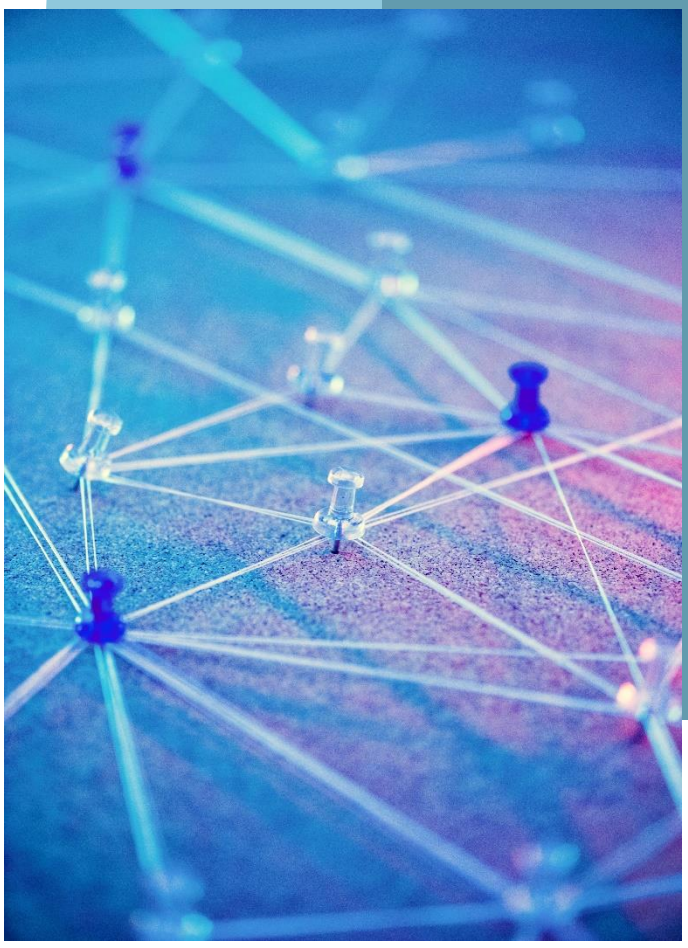
Nikolaus Stapels

Mit diesem Leitfaden möchte ich meinen Teil dazu beitragen, um Menschen in Krisen- und Kriegsgebieten zu unterstützen. Bereits in der Flüchtlingskrise konnte ich vielen helfen, eine anonyme Kommunikation in Kriegsgebieten einzurichten.

VPN Software bei staatlicher Zensur

Einige Länder beschränken den Zugriff auf freie Informationen im Netz.

Eine VPN-Software ist ein guter erster Schritt, denn über eine VPN-Software können Sie eine verschlüsselte Leitung aufbauen und so zum Beispiel sogenannte DNS-Sperren umgehen und auf gesperrte Webseiten zuzugreifen.



Über die VPN Verbindung wird auch Ihre Privatsphäre im Netz geschützt, indem die eigene IP-Adresse verändert wird, dadurch sind Sie schwerer identifizierbar.

Zudem kann Ihre Kommunikation nicht oder nur sehr schwer abgefangen und zum Beispiel verändert werden.

Über gängige Suchmaschinen können Sie Testsieger sowohl für Smartphones, Tablets oder Laptops finden.

Um noch sicherer und anonymer im Netz unterwegs zu sein, empfiehlt es sich, das TOR-Netzwerk zu nutzen.

Das TOR-Netzwerk

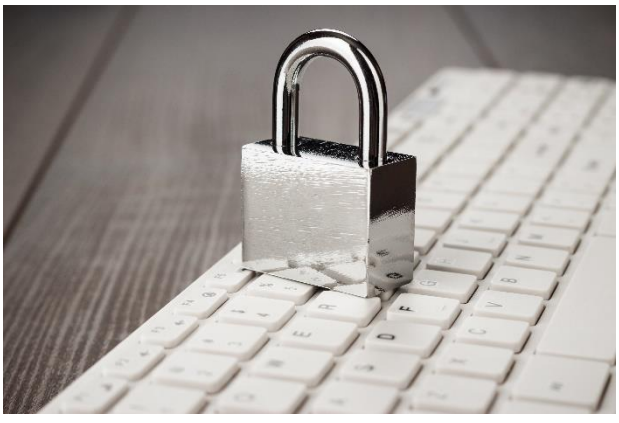
In einer Welt, die sich immer schneller digitalisiert, wachsen auch die Möglichkeiten der Überwachung von einzelnen Personen bis hin zu Personengruppen oder ganzen Bevölkerungen rasant an.

Nicht mehr nur Journalisten bei brisanten Recherchen und Menschenrechtsaktivisten in der Kommunkation untereinander wollen unerkannt bleiben.
Immer häufiger müssen auch „normale“ Nutzer Vorkehrungen treffen, um sich und ihre Liebsten zu schützen.

Eine gute und einfache Möglichkeit ist die Nutzung des TOR-Netzwerks, da hier die Datenpakete nicht direkt zu einem Webservice geschickt werden, sondern einen Umweg über verschiedene Server im Netzwerk gehen.

TOR-Netzwerk

Mithilfe zum Beispiel des TOR-Browsers können Sie vollautomatisiert eine anonyme Verbindung zu dem Netzwerk aufbauen und so Ihre Spuren verwischen.
Diese Anonymisierungstechnik nennt sich „Onion Routing“; dabei werden die Webseiten über die sogenannten „Knoten“ geleitet.
Diese Verbindung ist verschlüsselt und schützt somit die eigene Identität.
Zudem können so auch zum Beispiel Internetsperren von bestimmten Webseiten im Land umgangen werden.



Sichern Sie Ihre gesamte Kommunikation.

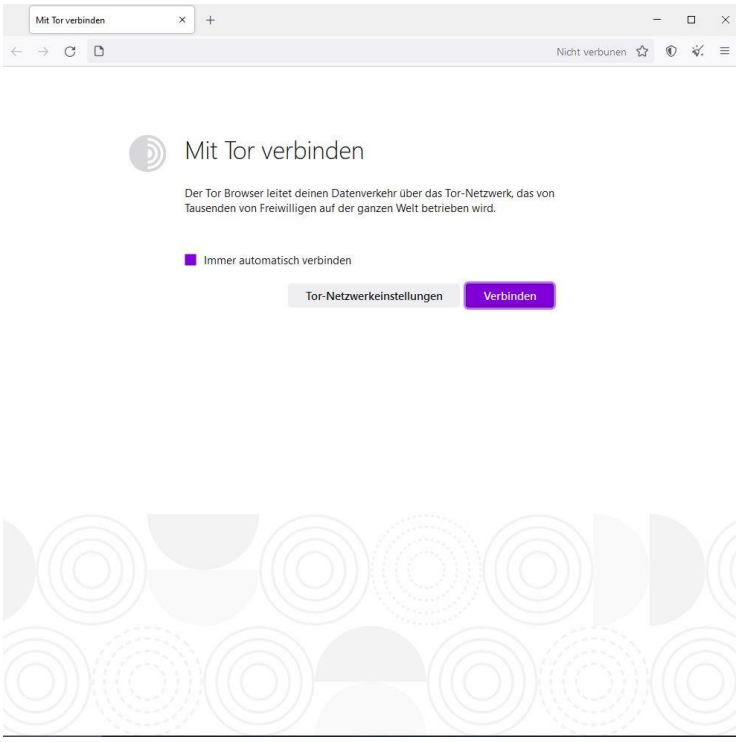
Die Nutzung des TOR-Netzwerks; starten wir…

Wenn das Internet keine sicheren Kanäle mehr bietet, wechseln viele Nutzer auf das TOR-Netzwerk. TOR ist aufgrund seiner großen Nutzervielfalt sehr bekannt und die Software ist leicht über gängige Suchmaschinen zu finden.
Achten Sie ggfs. darauf, dass Sie die Software über einen öffentlichen Hotspot auf z. B. Ihr Handy, Laptop oder Tablet laden und dann ggf. per USB-Stick verteilen, damit eventuelle Überwachungsorgane nicht direkt mitbekommen, dass Sie den TOR-Browser geladen haben.
Je mehr Leute in Ihrem Umfeld das TOR-Netzwerk nutzen, um so sicherer ist dies für alle.

Start

Nachdem Sie den Browser installiert und gestartet haben, können Sie direkt eine Verbindung zum TOR-Netzwerk aufbauen.
In die TOR-Netzwerkeinstellungen (linker Button) brauchen Sie nur gehen, wenn der TOR-Browser aufgrund von Beschränkungen im eigenen Land blockiert ist.

In diesem Falle muss man dann sogenannte Brücken einrichten; weitere Informationen finden Sie direkt unter : https://bridges.torproject.org/



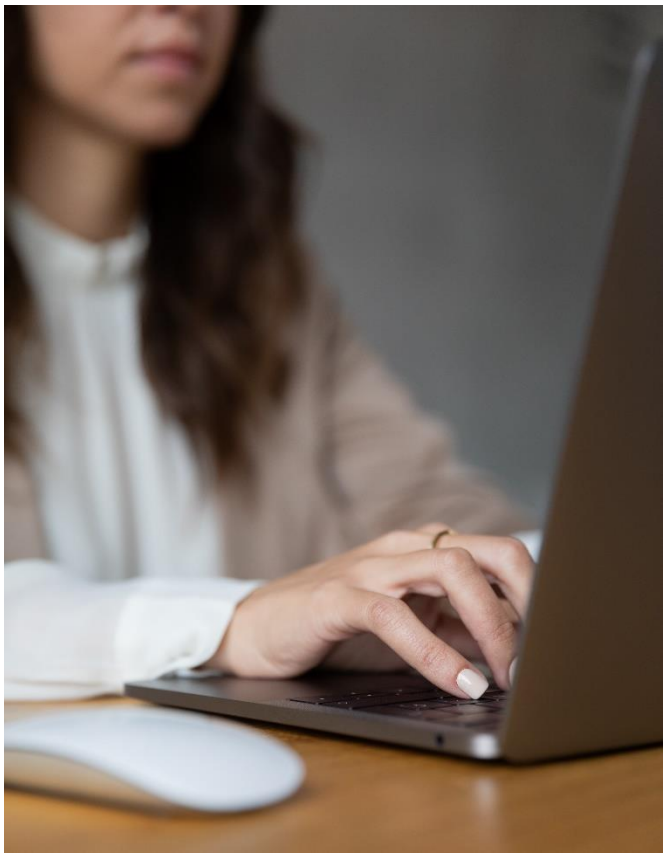
Startbildschirm TOR-Browser

Wichtige Hinweise bei der Nutzung.

Die Anonymität ist aus der technischen Sicht her sehr einfach umzusetzen, da das meiste vollautomatisch funktioniert.

Es gibt aber eine große Gefahr - einige Fehler, die viele Nutzer am Anfang begehen.
Beachten Sie deshalb die folgenden Punkte:

- Erstellen Sie neue (anonyme) Social Media Accounts; über den alten sind Sie identifizierbar..
- Nutzen Sie keine Echtnamen oder bereits vorhandene Pseudonyme (Nicknames) von anderen Seiten.
- Geben Sie keine echten Adressen oder vorhandene Mailadressen an.
- Nutzen Sie keine Cookies beim Surfen im TOR-Netzwerk, diese können Sie direkt im Browser ablehnen.
- Schützen Sie weiterhin Ihre Rechner mit Antivirensoftware. und Firewalls.

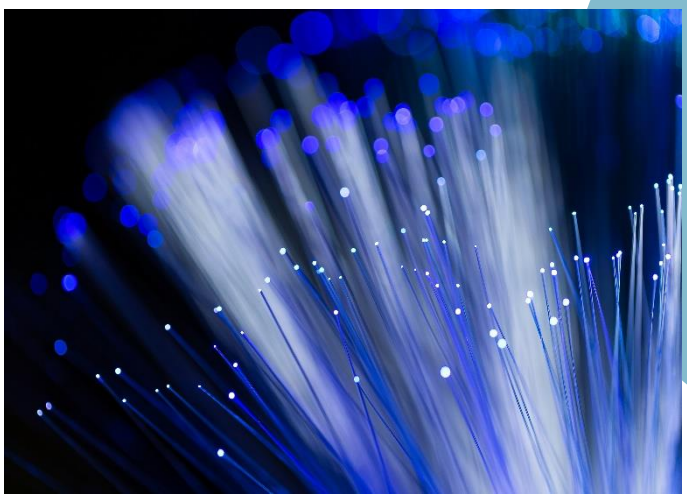


IT-Sicherheit

Durch das TOR-Netzwerk können Sie zwar anonym surfen und sich frei bewegen - beachten Sie jedoch, dass Ihre Daten hierbei weiterhin auf Ihrem Gerät unverschlüsselt gespeichert sind und somit durch Dritte gelesen werden können.

Navigation

Eine Navigation im TOR-Netzwerk ist nicht so komfortabel wie im normalen Internet.
Sie können aber mit z.B. dem TOR-Browser auch normale Webseiten und somit auch Suchmaschinen aufrufen und dort nach bestimmten Diensten suchen.
Als Ergebnis sollten Sie dann darauf achten, dass Sie Webseiten mit der Endung **.onion** erhalten.
So wie verschieden Webseiten Endungen wie .de oder .com enthalten können, haben alle Webseiten im TOR-Netzwerk die Endung .onion.
Diese Seiten können Sie dann auch nur mit z.B. dem TOR-Browser aufrufen und dann anonym surfen.



Über die Endung .onion erkennen Sie bei einer Webadresse, dass Sie sich im TOR-Netzwerk befinden.

Einige TOR-Webseiten

Mail-Account

ProtonMail

Über den Anbieter können die Nutzer anonym Mails senden und empfangen.
Es gibt auch einen kostenfreien Zugang.

Link ins TOR-Netzwerk

Such-maschine

DuckDuckGo

Es handelt sich hierbei um eine Suchmaschine, die einen hohen Grad an Privatsphäre bietet. Beachten Sie, dass eine Suche im Darknet häufiger auch nicht funktionieren kann, da die Seiten offline sind.

Link ins TOR-Netzwerk

Social-Media

Facebook

Viele Nutzer sind in den sozialen Medien, wie z.B. Facebook, unterwegs.
Deshalb hat Facebook auch seinen Dienst in das TOR-Netzwerk gebracht. Suchen Sie ggfs. nach weiteren Diensten.

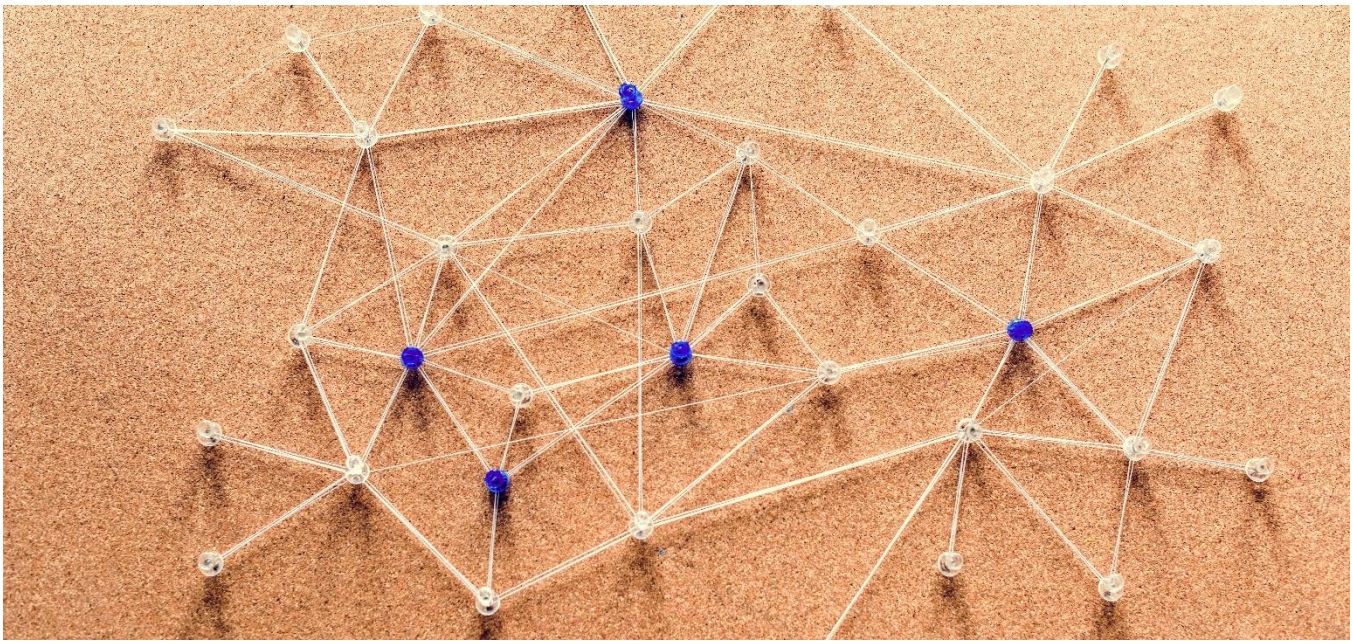
Link ins TOR-Netzwerk

News

SecureDrop

Über SecureDrop können Dokumente und Dateien mit Medienorganisationen weltweit geteilt werden.

Link ins TOR-Netzwerk



Welche „sicheren“ Messenger-Dienste gibt es?

Grundsätzlich sollte man unabhängig der Nachrichten immer auf einen sicheren Messenger setzen. Aber gerade in einer Krisen- oder Kriegsregion sollte man verstärkt auf die Daten achten, die man versendet und welche Software man nutzt. Hier sind einige Messenger als Beispiel:

Signal

Edward Snowden selbst hat die Nutzung von Signal empfohlen, da dieser Messenger-Dienst als einer der sichersten in der Welt gilt.
Die Verschlüsselung wurde mehrfach getestet und hat gut abgeschnitten.

Threema

Threema stammt aus der Schweiz und dort stehen auch die Server. Unter anderem durch die Standorte der Server verspricht der Anbieter einen hohen Sicherheitsstandard und Datenschutz.

Telegram

Auch dieser Messenger setzt auf eine Ende-zu-Ende-Verschlüsselung (aktivieren Sie diese), damit Dritte nicht mitlesen können. Das Projekt ist jedoch nicht komplett open source (nicht zu 100 % von Dritten überprüfbar).

Sie haben Rückfragen?

Gerne stehen wir Ihnen unter info@cyber-fuchs.de für Rückfragen zur Verfügung.

Dieser Leitfaden soll Ihnen eine erste Orientierung geben und Ihnen helfen, sicher zu kommunizieren.

Es wurde bewusst nicht in die technische Tiefe gegangen; soll Ihnen aber einen ersten Überblick verschaffen.