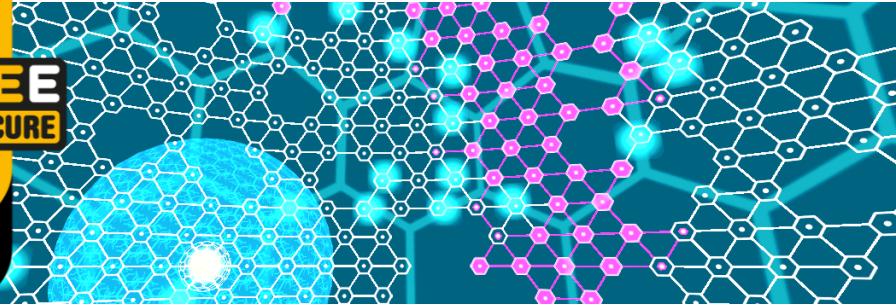
# Darknet

## Die dunkle Seite des Netzes



Das Darknet wird regelmäßig in den News erwähnt, im Allgemeinen in Verbindung mit kriminellen Machenschaften. Auf den ersten Blick handelt es sich um ein „Underground"-Netz, das von Schwarzhändlern, von Hackern und von Pädophilen heimgesucht wird. Aber diese Betrachtungsweise ist recht vereinfachend. Das Darknet empfängt ebenfalls Verfechter der Meinungsfreiheit, Blogger oder Whistleblower, die vor Zensur und strafrechtlicher Verfolgung fliehen.

### Was ist das Darknet?

Das Darknet ist vor allem eine große Menge nicht indexierter Seiten, die weder mit den traditionellen Suchmaschinen noch mit einem normalen Webbrowser zu finden sind. Für den Zugriff hierauf muss man die Software Tor herunterladen, die einen spezifischen Browser enthält, um auf die im Darknet versteckten Seiten zu gelangen. Das System Tor befördert den Datenverkehr über mehrere Stufen so, dass die Navigation unmöglich (oder nur sehr schwierig) zu verfolgen ist. Mit anderen Worten, bei Verwendung von TOR kann Ihre IP-Adresse nicht mehr identifiziert werden und niemand kann die von Ihnen besuchten Seiten erkennen. Die Größe des Darknets genau zu einzuschätzen ist schwierig. Bestimmte Quellen nennen 600 Terabytes…

Das Darknet enthält eine große Menge illegaler Inhalte: Drogen, Waffen, Kinderpornographie, Leugnung von Holocaust oder Völkermord… Man kann dort ebenfalls „Anbieter" illegaler oder verbrecherischer Handlungen finden: Hacker, Profikiller… Kurz gesagt hat das Darknet eine wirklich dunkle („dark") Seite.

### Mit allen Vor- und Nachteilen.

Es wäre falsch, das Darknet als ein Schlupfwinkel von Verbrechern zusammenzufassen. Das Darknet beherbergt ebenfalls viele Aktivisten, Journalisten oder einfache Bürger, die die Meinungsfreiheit verteidigen wollen und die das Bedürfnis haben, sich der Massenüberwachung oder der Zensur ihrer Regierung zu entziehen.

So findet man eine große Anzahl von chinesischen Bloggern, von Reportagen und von Fotos über die Lage in Syrien oder in der Ukraine, oder einfach nur Seiten zur Förderung der Verschlüsselungstechnik.

### Ist es legal?

Die Benutzung von TOR und der Zugang zum Darknet sind in Luxemburg vollkommen legal, was in anderen Ländern nicht der Fall ist. Dagegen sind einige der in diesem unsichtbaren Netz praktizierten Aktivitäten illegal. Beim Zugriff darauf muss man sich einfach vor Augen halten, dass der Kauf oder Verkauf bestimmter Produkte oder Dienstleistungen (Drogen, Waffen, Auftragsmord…) strafbar ist.

### Ist es sicher?

Alles hängt davon ab, was man unter „sicher" versteht. Das Hauptinteresse des Darknets ist die Vertraulichkeit, die es seinen Benutzern anbietet. Durch seine Zwiebelstruktur werden mehrere Verschlüsselungsschichten zwischen dem Benutzer und den von ihm besuchten Seiten verwandt.

Dies hindert normalerweise Spione und Nachrichtendienste daran, Personen zu identifizieren, die die Dienste des Darknets benutzen.

Jedoch sind die Cyberpolizei und die Nachrichtendienste ebenfalls im Darknet unterwegs, um die Spur von Verbrechern zurückzuverfolgen. Auf den ersten Blick interessieren sie sich nicht für die „normalen“ Benutzer.

Konkret ermöglicht der Tor-Browser, in aller Vertraulichkeit zu surfen. Dieser Browser enthält mehrere Verschlüsselungsschichten zwischen dem Benutzer und den von ihm besuchten Seiten. Es gibt auch andere Mittel, sich im Internet zu schützen, wie VPN (Virtual Private Network), das einen verschlüsselten Kommunikationskanal bildet.

Dann sollte man darauf achten, seinen Computer und seinen Browser zu sichern, insbesondere, indem man die Skripts sperrt. In der Tat benutzen zahlreiche Seiten des Darknets JavaScript aus den falschen Gründen.

## In der Praxis

Nach Downloaden des Tor-Browsers können Sie beginnen, nützliche Adressen mit der Erweiterung „.onion" zu suchen. Ab hier erschwert sich die Sache, denn es ist nicht selbstverständlich, ein gültiges und zuverlässiges Adressbuch zu finden. Um Ihnen die Aufgabe zu vereinfachen, finden Sie hier eine Auswahl getesteter Verbindungen, die Sie im Tor-Browser benutzen können.

- Suchmaschinen: http://hss3uro2hsxfogfq.onion
- Hidden Wiki: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- Verzeichnis der Links: http://torlinkbgs6aabns.onion
- Facebook für Tor:  https://Facebook.onion
- Suchmaschine Darknet: http://grams7enufi7jmdl.onion
- Verkauf von entsperrten Mobiltelefonen: http://mobil7rab6nuf7vx.onion
- Suchmaschinen DuckDuckGo: http://3g2upl4pq6kufc4m.onion

Neben dem Darknet gibt es ebenfalls verschiedene Typen „geheimer Bibliotheken“, oft um literarische oder wissenschaftliche Inhalte zu veröffentlichen, die urheberrechtlich geschützt oder einfach nicht auf herkömmlich Weise veröffentlicht sind. Diese Bibliotheken sind im allgemeinen das Werk von Personen oder militanten Gruppen, die das Recht auf Information im Gegensatz zum Urheberrecht verteidigen.

## Einige Warnhinweise:

Mit Tor auf Diensten zu surfen, bei denen man sich authentifizieren muss (soziale Netzwerke, E-Mail) ist kontraindiziert. Zunächst, weil dies die angestrebte Anonymität aufhebt. Aber auch weil Sie leicht einen Sicherheitsalarm in diesen Netzwerken auslösen können. In der Tat könnten sie den Eindruck haben, Ihr Konto sei beschädigt, weil man versucht, sich dort von sehr weit voneinander entfernten Punkten zu verbinden…

Tor verursacht eine Verlangsamung der Navigation, gerade wegen der Komplexität des Datenweges.

Tor stellt auf keinen Fall einen Schutz vor auf manchen Webseiten vorhandenen bösartigen Codes dar, noch gegen das Phishing.

Bei Fragen bezüglich des Internetbetrugs
oder der Nutzung des Internet im Allgemeinen,
wenden Sie sich bitte an die BEE SECURE Helpline:

BEE SECURE HELPLINE
CONSEIL & AIDE
8002-1234





Herausgeber:  BEE SECURE · B.P. 707 · L-2017 Luxemburg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.luwww.bee-secure.lu



THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union
Connecting Europe Facility