7

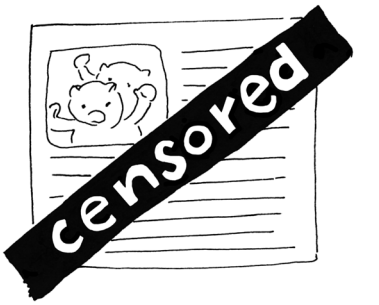
WIE KÖNNEN INFORMATIONEN ANONYM ÜBER DAS INTERNET ÜBERTRAGEN WERDEN?

Nachdem wir nun die verschiedenen Möglichkeiten besprochen haben, wie Regierungen, Unternehmen und Organisationen Inhalte im Internet zensieren, wollen wir nun erörtern, wie wir die Zensur überwinden können. In diesem Kapitel werden wir uns darauf konzentrieren, wie wir herausfinden, was zensiert wird, bekannt als Zensurüberwachung, und wie wir die Zensur umgehen können.

Zensurüberwachung

Um die Zensur zu überwinden, müssen wir zunächst wissen, dass sie stattfindet.
Wir können Zensur von temporären Ausfällen unterscheiden, indem wir die Internet-Konnektivität global überwachen. Wir können die Überwachung der Zensur auf verschiedene Weise durchführen. Benutzerberichte können aufzeigen, ob Inhalte unzugänglich gemacht wurden. Einige Regierungen und Unternehmen sind transparent, was die von ihnen verhängte Zensur angeht. Oft können wir jedoch nur dann definitiv wissen, ob Internetzensur auf technischer Ebene stattfindet, wenn wir verschiedene Arten von Anfragen an Server und Dienste von bestimmten Standorten aus testen. Wir analysieren die Antworten oder Ergebnisse dieser Anfragen im Vergleich zu den Antworten von Anfragen, die über nachweislich intakte, unzensierte Verbindungen eingehen, um zu sehen, ob es Unterschiede zwischen den Antworten gibt. Diese Tests zielen darauf ab, die Möglichkeit auszuschließen, dass ein Antwortfehler (wie z. B. ein 404, erklärt in Kapitel 4) auf eine Blockade oder einen Filter im Netzwerk zurückzuführen ist und nicht auf einen anderen Grund, der vom angefragten Dienst stammt.

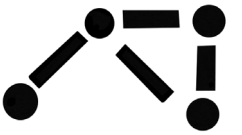
Es gibt mehrere Organisationen und Forschungsprojekte, die versuchen, die Internetzensur zu überwachen.



Netblocks

→ *https://netblocks.org*

NetBlocks ist eine Gruppe, die Messungen und Tools zur Datenvisualisierung erstellt, um Internetabschaltungen, Telekommunikationsausfälle und politisch oder wirtschaftlich motivierte Onlinezensur zu erkennen.



Ihre Tools machen nicht nur Zensur sichtbar, sondern sind auch effektiv bei der Darstellung von Ausfällen aufgrund von Naturkatastrophen wie Erdbeben oder Wirbelstürmen sowie von Cyberangriffen auf die Netzwerkinfrastruktur. NetBlocks veröffentlicht Berichte über Internetabschaltungen weltweit, zusammen mit Erklärungen und Echtzeit-Updates.

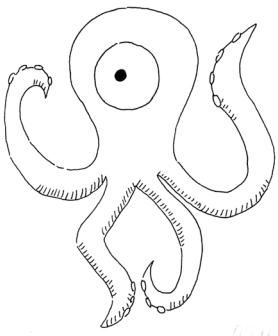
Open Observatory of Network Interference (OONI)

→ *https://explorer.ooni.org*

Open Observatory of Network Interference (OONI) ist ein globales und dezentrales Beobachtungsnetzwerk zum Aufspüren von Zensur, Überwachung und Manipulationen des Datenverkehrs im Internet. OONI ist freie Software, sodass jeder mit OONI Verbindungen zu Websites testen kann, die möglicherweise verboten sind. Die Messwerte werden im OONI Explorer veröffentlicht.

Mit OONI kann man testen,

- ob Websites gesperrt sind,
- ob Instant-Messaging-Apps (wie WhatsApp und Facebook Messenger) blockiert sind,
- ob Tools zur Umgehung der Zensur (wie Tor) blockiert werden,
- ob Systeme (»Middleboxen«) in Ihrem Netzwerk vorhanden sind, die für Zensur und/oder Überwachung verantwortlich sein könnten und
- wie Geschwindigkeit und Leistung Ihres Netzwerks sind.



OONI schützt allerdings nicht die Privatsphäre derjenigen, die Tests durchführen, weil dabei Information hinterlassen werden, die unter Umständen eine Identifikation möglich machen.

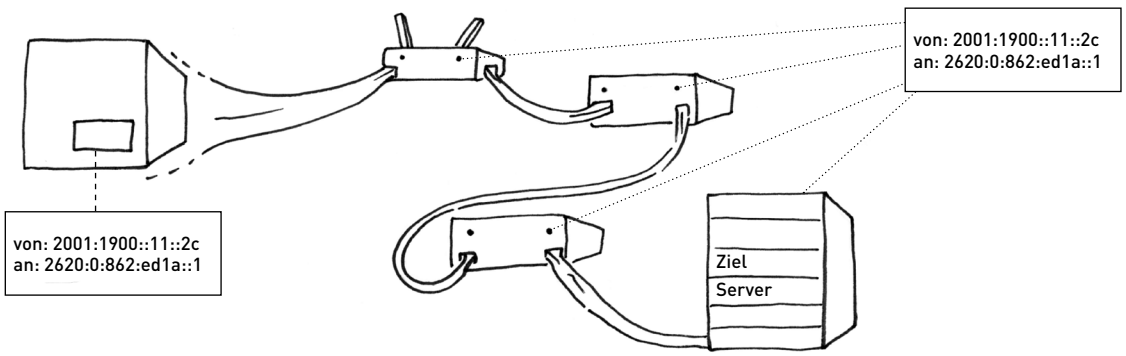
Transparenzberichte

Unternehmen veröffentlichen **Transparenzberichte**, in denen die Art der Zensuranfragen von Regierungen, Urheberrechtsinhaberinnen oder anderen und die Einhaltung durch das Unternehmen detailliert beschrieben werden. Transparenzberichte können auch Statistiken über Anfragen nach Benutzerdaten enthalten.
Google zum Beispiel stellt anonymisierte Informationen über Anfragen zur Aufhebung von Suchergebnissen und Inhalten auf anderen Google-Produkten wie YouTube oder Blogger zur Verfügung. Viele dieser Anfragen sind auf rechtmäßige Copyright-Ansprüche zurückzuführen sowie auf behördliche und individuelle Löschungsanfragen im Zusammenhang mit Bedenken hinsichtlich der nationalen Sicherheit, Verleumdung, Privatsphäre und Sicherheit, Drogenmissbrauch oder Pornografie.

Google klassifiziert die Zensuranfragen, die sie erhalten, im Allgemeinen in vier verschiedene Kategorien:

Geschützt – Google filtert und blockiert automatisch Zehntausende von URLs pro Woche aus den Suchergebnissen, um zu versuchen, User vor Websites mit Malware und Phishing zu schützen.[16]
Entfernt – Aufforderungen zur Entfernung von Inhalten aufgrund von Urheberrechtsverletzungen. Mehr als 20.000 private Unternehmen und Urheberrechtsinhaber haben Google aufgefordert, insgesamt 4.683.688.889 URLs zu entfernen.[17]
Versteckt – Suchergebnisse, die aufgrund von Datenschutzgesetzen entfernt wurden. Google erhält wöchentlich Tausende von Anfragen zum Entfernen von URLs; von den angeforderten URLs entfernt Google 46 Prozent.[18]
Zensiert – Aufforderungen der Regierung, Inhalte zu entfernen. Google hat im Jahr 2019 etwa 30.000 erhalten.[19]

Wie Daten wandern



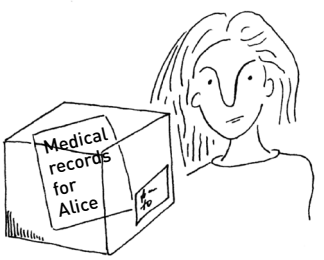
Bevor wir über die Umgehung der Zensur sprechen, lassen Sie uns kurz die Art und Weise besprechen, wie unsere Daten übertragen werden.
Daten werden in Stücken übertragen, die man **Pakete** nennt.
Jedes Paket hat ein **Adress-Tag** oder einen **Paket-Header**, der seine Quell- und Zieladresse angibt.

Im Internet gibt es keine direkten Verbindungen. Pakete reisen durch zwischengeschaltete Netzwerke und Router, die den Paket-Header lesen, um die Pakete an ihr Ziel zu leiten.

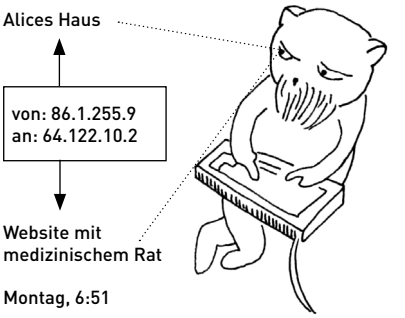
Durch das Lesen des Paket-Tags wissen diese zwischengeschalteten Netzwerke, woher sie das Paket erhalten haben und wohin sie es senden.
Alle diese Zwischenstationen können Pakete kopieren, speichern oder sogar verändern.

Anonymität und Pseudo-Anonymität

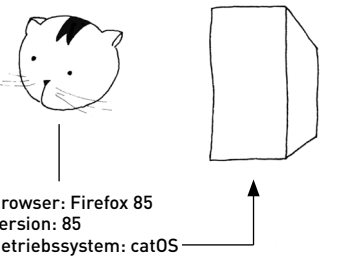
Wenn wir Pakete ohne Ende-zu-Ende-Verschlüsselung senden, können unsere Pakete unverschlüsselte Inhalte enthalten, die Informationen über unsere wirkliche Identität preisgeben.



Außerdem enthalten die Metadaten der Pakete Informationen über unseren Standort und unsere Interessen in der realen Welt, wie z. B. Quell- und Ziel-IP-Adresse, die von Websites und ISP leicht erfasst werden können.

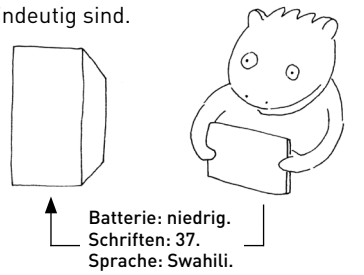


Wenn wir Websites besuchen, senden und empfangen wir Pakete, die weitere Informationen über uns enthalten, die gelesen, extrahiert und weiter analysiert werden können, einschließlich des Betriebssystems und der verwendeten Browserversionen.

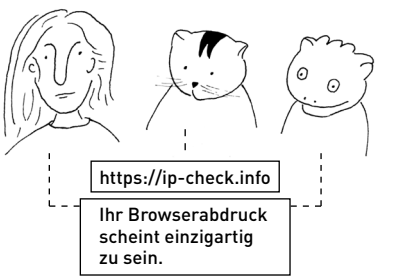


Websitebetreiber können sogar noch mehr identifizierende Details aus unseren Datenpaketen extrahieren, wenn wir Websites besuchen, die mit aktuellen Webtechnologien wie JavaScript und HTML5 programmiert sind. Die Betreiber können wissen, welche eingestellte Sprache der Browser verwendet, welche Schriftarten auf unserem Computer installiert sind, welche Bildschirmauflösung wir verwenden und sogar den Batteriestatus unseres Geräts.

Wir nennen das Verfolgen und Extrahieren dieser Art von Informationen **Fingerprinting**, weil diese Informationen in der Regel für einzelne Nutzer eindeutig sind.



Unternehmen und Institutionen können mittels Fingerprinting unsere IP-Adresse und andere Metadaten herausfinden, um genau zu bestimmen, wer wir sind.



Wenn wir über **Anonymität** im Internet sprechen, meinen wir die Verschleierung oder die Verknüpfbarkeit von Informationen zur Identifizierung. Selbst wenn wir Anwendungen und Dienste nutzen, die unsere persönlichen Daten schützen, wie z. B. Transport- oder Inhaltsverschlüsselung, können andere die Metadaten unserer Pakete, wie z. B. unsere IP-Adresse, erfassen. Wir können also online nur **pseudoanonym** sein, nicht anonym.

Um anonym zu werden, benötigen wir Techniken, die unsere IP-Informationen und damit auch unseren Standort verbergen.

Umgehung der Zensur

Zwischengeschaltete Router können Pakete leicht verändern, was zu einem Problem wird, wenn Staaten, Unternehmen, Arbeitgeber, Eltern oder Netzwerkbetreiber versuchen, Sie am Zugriff auf bestimmte Inhalte im Internet zu hindern.

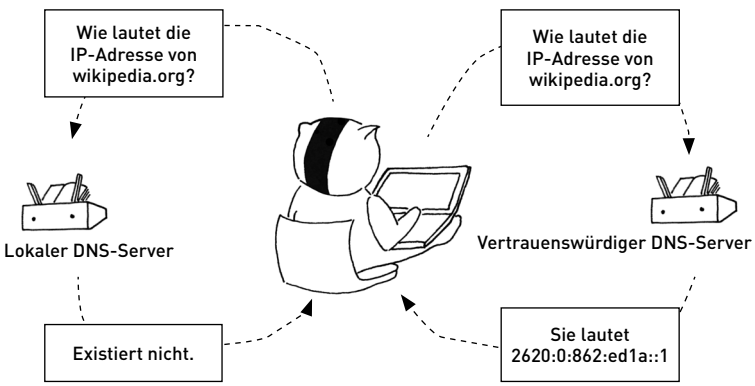
Versuche, Inhalte zu zensieren, können jedoch an jeder Stelle stattfinden: an der Quelle, an Zwischenroutern oder am Ziel. Verschiedene Parteien, die das Netzwerk betreiben, führen diese Eingriffe durch, in Form von Blockierung, Filterung und Throttling, wie in Kapitel 6 beschrieben.

Es gibt viele gute Gründe, warum Internetnutzer die Zensur umgehen oder ihre persönlichen Daten, ihre Privatsphäre, ihre Anonymität oder ihre Pseudonymität im Internet schützen wollen.

Wir werden uns jedoch mehr auf die technische Umsetzung der Zensur konzentrieren und auf die Möglichkeiten, die Zensur in Form von Filtern und Sperren zu umgehen bzw. zu verhindern.

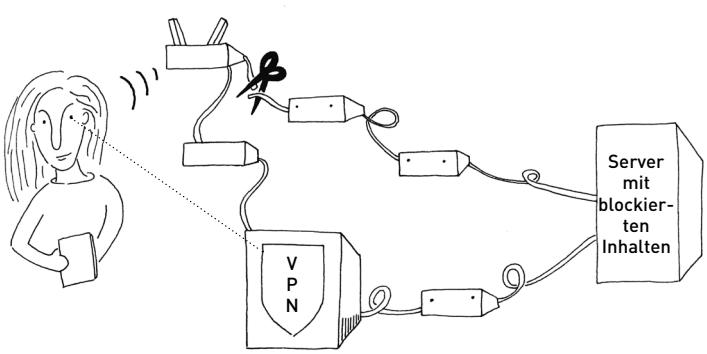
DNS-Proxy

Um einer DNS-Blockierung entgegenzuwirken, können Sie einen DNS-Server verwenden, dem Sie vertrauen, anstatt desjenigen, der automatisch von ISP bereitgestellt wird. Mit einem **DNS-Proxy** können Sie DNS-Filter oder -Sperren umgehen, die möglicherweise auf der Ebene eines lokalen oder nationalen ISP eingerichtet sind.



Virtuelles privates Netzwerk (VPN)

Um der Überwachung oder Zensur an Ihrem Arbeitsplatz oder Ihrer Universität entgegenzuwirken, können Sie sich mit einem **virtuellen privaten Netzwerk (VPN)** oder einem **Proxy** verbinden, das Ihren Netzwerkverkehr verbirgt und DNS-Anfragen in Ihrem Namen stellt und empfängt. Der VPN-Anbieter weiß, wer Sie sind, daher bietet ein VPN keine vollständige Anonymität.



Der VPN-Anbieter selbst oder ein starker externer Gegner kann immer noch Ihren ein- und ausgehenden Datenverkehr zurückverfolgen, um Sie zu identifizieren, also stellen Sie sicher, dass Sie Ihrem VPN vertrauen. Ein VPN verlagert lediglich die Last des Schutzes Ihrer identifizierenden Informationen von Ihnen auf den VPN-Anbieter. In den Vereinigten Staaten ist die Umgehung einer IP-Sperre, um auf eine Website zuzugreifen (z. B. durch anonyme Proxys), ein Verstoß gegen den Computer Fraud and Abuse Act (CFAA), der mit zivilrechtlichen Schadensersatzforderungen oder sogar Gefängnisstrafen für »unautorisierten Zugriff« geahndet wird.[20]