FERDINAND PORSCHE
FERNFH

Netzsperren in Österreich: Evaluierung technischer Umgehungsmöglichkeiten

Masterarbeit

Eingereicht von: **Christian Hahn, BA**
Matrikelnummer: 51906731

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Christoph Jungbauer, BA MA MA

Zweitgutachten: Ing. Peter Völkl, BA MA MSc

Wiener Neustadt, Mai 2024

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.
3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Gföhl, 20.05.2024 Unterschrift

Kurzzusammenfassung: Netzsperren in Österreich: Evaluierung technischer Umgehungsmöglichkeiten

Die Masterarbeit untersucht die Wirksamkeit technischer Umgehungsmethoden von Netzsperren in Österreich. Netzsperren werden eingesetzt, um den Zugang zu bestimmten Internetinhalten zu blockieren. Die zentrale Forschungsfrage lautet: Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen? Zur Beantwortung der Fragestellung wird der aktuelle Forschungsstand erhoben und eine experimentelle Analyse durchgeführt. Es zeigt sich, dass in Österreich DNS-Sperren zur Blockierung von Inhalten eingesetzt werden. Vier Methoden zur Umgehung von DNS-Sperren in Österreich werden identifiziert und evaluiert: Verwendung von IP-Adressen, Änderung des DNS-Resolvers, Nutzung von VPN und das Tor-Netzwerk. Die Untersuchung der Umgehungsmethoden werden mithilfe eigens entwickelter Python-Skripte durchgeführt, um die Erfolgsrate und Antwortzeiten der Methoden zu ermitteln. Die experimentelle Analyse ergibt, dass DNS-Resolver-Änderungen, VPN und das Tor-Netzwerk effektive Mittel zur Umgehung von Netzsperren darstellen. Aufgrund technischer und sicherheitsrelevanter Barrieren ist die Verwendung von IP-Adressen nicht geeignet. Die entwickelten Python-Skripte und methodischen Ansätze können als Grundlage für zukünftige Studien in verschiedenen Netzumgebungen dienen und die Forschung im Bereich der Netzsperren vorantreiben.

Schlagwörter:

Netzsperren, DNS-Sperren, Internetzensur, VPN, Tor-Netzwerk, DNS-Resolver

Abstract: Internet Censorship in Austria: Evaluation of Technical Circumvention Methods

This thesis investigates the effectiveness of technical methods to circumvent Internet censorship in Austria. The central research question is: Which of the identified technical methods can effectively circumvent Internet censorship in Austria? Both theoretical and practical research show that DNS blocking is used to restrict content in Austria. Four circumvention methods are identified and evaluated: Accessing content by IP address, changing the DNS resolver, using VPN, and the Tor network. Tests evaluate the effectiveness of these methods, using specially developed Python scripts to record success rates and response times. The empirical analysis shows that DNS resolver changes, VPN, and the Tor network are effective means of circumventing Internet censorship in Austria. Accessing content by IP address proves unreliable due to technical and security barriers. These findings provide valuable practical guidelines for circumventing Internet censorship, and the developed Python scripts and methodological approaches serve as a basis for future studies.

Keywords:

Internet censorship, DNS blocking, circumvention methods, VPN, Tor network, DNS resolver

Inhaltsverzeichnis

1. Einleitung

Netzsperren sind ein zunehmend kontroverses Thema in Österreich [Pr22]. Ein Beispiel dafür ist eine Netzsperre im Jahr 2022, die IP-Adressen des Internetdienstleisters Cloudflare blockierte. Diese Sperre führte nicht nur zum Ausfall eines Musikportals, sondern beeinträchtigte auch viele unbeteiligte Dienste [on22]. Netzsperren sind eine Form der Internetzensur, die den Zugang zu bestimmten Inhalten oder Dienste im Netz verhindern oder erschweren soll. Netzsperren sind in bestimmten Fällen rechtlich zulässig, insbesondere wenn sie auf Gesetzen basieren oder gerichtlich angeordnet werden. Dies umfasst Maßnahmen gegen illegales Glücksspiel, Urheberrechtsverletzungen oder zum Schutz von Jugendlichen [RT24b]. Diese Sperren sind jedoch nicht nur ein Werkzeug der Kontrolle, sondern werfen auch schwerwiegende Fragen bezüglich der Meinungsfreiheit, der Privatsphäre und der technischen Sicherheit des Internets auf [to17]. Netzsperren können zu unbeabsichtigten Kollateralschäden führen, indem sie den Zugang zu legitimen oder relevanten Webseiten beeinträchtigen [Re22b], wie auch das angesprochene Beispiel in Österreich zeigt. Netzsperren können auch die Anonymität und Privatsphäre der Internetnutzer*innen gefährden, indem sie deren Online-Aktivitäten überwachen oder manipulieren [Ve23]. Gleichzeitig gibt es eine Vielzahl von Technologien und Methoden, die entwickelt wurden, um diese Sperren zu umgehen und die zensierte Information trotzdem zu erreichen [Th20]. Die Masterarbeit konzentriert sich auf die technischen Aspekte von Netzsperren in Österreich. Dabei werden Blockierungs- und Umgehungstechniken untersucht. Die Wirksamkeit dieser Techniken wird durch empirische Tests verschiedener Methoden evaluiert. Diese technische Fokussierung ermöglicht eine tiefergehende Analyse der Mechanismen hinter den Netzsperren und deren Umgehung. Dieser Ansatz zielt darauf ab, präzise technische Lösungen und Erkenntnisse zu erarbeiten, die die Effektivität verschiedener Umgehungsmethoden in der Praxis aufzeigen. Durch die Untersuchung der Effizienz technischer Umgehungsmethoden wird das Verständnis dafür erweitert, wie technologische Lösungen in den breiteren Kontext gesellschaftlicher und wirtschaftlicher Anforderungen eingebettet werden können. Sie deckt nicht nur die im Curriculum verankerten Kernbereiche der Informationstechnologie und -sicherheit ab, sondern fördert auch mein Verständnis für die Schnittstellen zwischen Technologie, Wirtschaft und gesellschaftlichen Belangen. Meine Arbeit leistet somit einen wertvollen Beitrag zur Entwicklung von Richtlinien und Technologien, die einen ausgewogenen Ansatz zwischen Sicherheitsanforderungen und dem Recht auf freien Informationszugang verfolgen.

1.1. Forschungsfrage

Die zentrale Forschungsfrage dieser Masterarbeit lautet:

Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen?

Diese Frage zielt darauf ab, die Effektivität verschiedener technischer Strategien zur Umgehung von Netzsperren im spezifischen rechtlichen und technischen Kontext von Österreich zu bewerten. Die Bedeutung dieser Forschungsfrage ergibt sich aus dem zunehmenden Einsatz von Netzsperren durch Internet Service Provider und Regierungen weltweit, einschließlich Österreich, um den Zugang zu bestimmten Internetinhalten zu blockieren. Netzsperren stellen eine Herausforderung für die Meinungsfreiheit, die Privatsphäre der Nutzer*innen und die technische Integrität des Internets dar.

Bisherige Studien haben sich hauptsächlich auf Länder mit strenger Internetzensur konzentriert, wie China und Iran, und dort die unterschiedlichen Techniken zur Durchsetzung von Netzsperren und deren Umgehung analysiert. In Österreich hingegen lag der Fokus bisher vor allem auf den rechtlichen Aspekten von Netzsperren und theoretischen Erörterungen zu Umgehungsmethoden, jedoch fehlten umfassende empirische Analysen der praktischen Anwendung dieser Methoden.

1.2. Arbeitsziel

Das primäre Ziel dieser Masterarbeit ist die Identifikation und Evaluierung verschiedener Umgehungsmethoden von Netzsperren und deren technischer Implementierung im Kontext Österreich. Die Arbeit soll die Wirksamkeit technischer Umgehungsmöglichkeiten untersuchen. Durch die Kombination von theoretischer Forschung und praktischen Tests verschiedener Umgehungstechniken wird angestrebt, ein tiefgreifendes Verständnis für Netzsperren und deren Umgehung zu entwickeln.

Die Untersuchung umfasst mehrere zentrale Aspekte:

- **Identifikation von Netzsperren:** Es soll untersucht werden, welche Arten von Netzsperren in Österreich eingesetzt werden und wie diese technisch umgesetzt werden.
- **Evaluierung technischer Umgehungsmethoden:** Die Arbeit untersucht die Wirksamkeit verschiedener technischer Strategien zur Umgehung identifizierter Netzsperren. Dabei werden geeignete Methoden zur Umgehung gewählt und auf ihre Erfolgsrate und Antwortzeit hin getestet und bewertet.
- **Beitrag zur wissenschaftlichen Gemeinschaft:** Die Ergebnisse dieser Arbeit sollen zur wissenschaftlichen Diskussion über Netzsperren und deren Umgehung beitragen.

1.3. Nicht-Ziele

Während es das Ziel dieser Masterarbeit ist, die Wirksamkeit von technischen Umgehungsmethoden für Netzsperren in Österreich zu evaluieren, gibt es bestimmte Bereiche, die nicht im Fokus dieser Untersuchung stehen. Diese Nicht-Ziele werden im Folgenden definiert:

- **Rechtliche und politische Analyse:** Diese Arbeit konzentriert sich auf die technischen Aspekte von Netzsperren und deren Umgehung. Eine Analyse der rechtlichen Rahmenbedingungen und politischen Implikationen, wie etwa die Gesetzgebung zur Netzneutralität oder spezifische Urteile und Gesetze in Österreich, wird nicht vorgenommen. Rechtliche Aspekte werden zwar im Kapitel 2 angesprochen, sind aber nicht Hauptgegenstand der empirischen Untersuchung.
- **Soziale und wirtschaftliche Auswirkungen:** Die Untersuchung der sozialen und ökonomischen Folgen von Netzsperren und ihrer Umgehung, wie etwa die Auswirkungen auf das Nutzerverhalten, die Meinungsfreiheit, die Geschäftstätigkeit von Online-Dienstleistern oder die digitale Ökonomie im Allgemeinen, ist nicht Gegenstand dieser Arbeit.
- **Technische Implementierung und Entwicklung neuer Umgehungstechnologien:** Obwohl die Arbeit bestehende Umgehungsmethoden evaluiert und empirisch testet, liegt der Fokus nicht auf der Entwicklung neuer Technologien oder der technischen Implementierung von Umgehungsstrategien. Ziel ist es, die Effektivität bereits etablierter Methoden zu bewerten, nicht jedoch, neue Ansätze oder Technologien zu entwickeln.
- **Globale Analysen:** Diese Arbeit beschränkt sich auf den spezifischen Kontext Österreichs und erhebt keinen Anspruch darauf, eine umfassende globale Analyse der Wirksamkeit von Umgehungsmethoden durchzuführen. Die Ergebnisse und Schlussfolgerungen sind daher primär auf Österreich anwendbar und können nicht ohne Weiteres auf andere Länder mit unterschiedlichen rechtlichen und technischen Rahmenbedingungen übertragen werden.

Durch die klare Abgrenzung dieser Nichtziele wird der Fokus der Arbeit geschärft, um die technische Evaluierung der Umgehungsmethoden unter den spezifischen Bedingungen in Österreich präzise und fundiert durchführen zu können.

1.4. Aufbau der Arbeit

Der Aufbau der Arbeit beginnt mit einer Einleitung, gefolgt von Theorie und Forschungsstand, methodischer Vorgehensweise, empirischer Untersuchung, Ergebnissen, Schlussfolgerungen, und endet mit einer Zusammenfassung und einem Ausblick.

Kapitel 2 legt die theoretische Basis, indem es die Mechanismen und Methoden von Netzsperren sowie deren Umgehung im spezifischen Kontext Österreichs darstellt. Es wird beschrieben, dass DNS-Sperren von ISPs eingesetzt werden, um den Zugang zu bestimmten Internetinhalten zu blockieren, und dass diese Sperren durch DNS-Manipulationen technisch umgesetzt werden. Vier Umgehungsmethoden wurden theoretisch analysiert: Die Verwendung von IP-Adressen, die Änderung des DNS-Resolvers, die Nutzung von VPNs und des Tor-Netzwerks. Die theoretische Untersuchung ergab, dass jede Methode spezifische Vor- und Nachteile hat, die je nach Anwendungsszenario variieren können.

Kapitel 3 und 4 beschreiben den methodischen Ansatz und die empirische Analyse. Die Untersuchung wurde mit den zum Zeitpunkt der Durchführung drei größten ISPs in Österreich (A1, Drei und Magenta) durchgeführt, welche über 80 % der Internetnutzer*innen in Österreich bedienen, um ein repräsentatives Bild der durchschnittlichen Internetnutzung zu erhalten. Zielseiten wurden auf Basis ihrer Präsenz auf der DNS-Sperrliste der RTR ausgewählt. Vier Umgehungsmethoden wurden getestet: IP-Adresse verwenden, DNS-Resolver ändern, VPN und Tor.

Für die empirischen Tests wurden Python-Skripte entwickelt, um die Erfolgsraten und Antwortzeiten der Umgehungsmethoden zu messen. Zur Analyse der Antwortzeiten wurden Mittelwert, Median, Standardabweichung und Variationskoeffizient berechnet.

In Kapitel 5 werden die empirischen Ergebnisse präsentiert, die weitgehend die theoretischen Annahmen bestätigen. Es zeigt sich, dass DNS-Resolver-Änderungsmethoden wie Google DNS und Cloudflare DNS Erfolgsraten von über 90 % erreichen und gegenüber VPN und Tor kürzere Antwortzeiten aufweisen. VPNs und das Tor-Netzwerk erweisen sich ebenfalls als effektive Umgehungsmethoden, obwohl sie aufgrund der zusätzlichen Sicherheitsschichten längere Antwortzeiten haben. Die direkte Verwendung von IP-Adressen stellt sich aufgrund von Zertifikatsfehlern und technischen Barrieren als nicht effektiv heraus.

Kapitel 6 fasst die Ergebnisse der Untersuchung zusammen und analysiert die untersuchten Umgehungsmethoden von DNS-Sperren in Österreich im Bezug zur Forschungsfrage und Forschungsstand. Darüber hinaus werden die Methodik und Ergebnisse kritisch reflektiert und deren Bedeutung für praktische Anwendungen diskutiert.

Kapitel 7 fasst die wesentlichen Ergebnisse der Arbeit zusammen und gibt einen Ausblick auf zukünftige Forschungsrichtungen. Eine potenzielle Forschungsrichtung, die sich in Zukunft eröffnen könnte, ist die Anwendung der entwickelten Python-Skripte in weiteren regionalen Kontexten.

2. Theoretische Grundlagen und derzeitiger Stand von Wissenschaft und Technik

In diesem Kapitel werden zunächst die notwendigen theoretischen Grundlagen dargelegt, um die Mechanismen und Methoden von Netzsperren sowie deren Umgehung zu verstehen. Es wird analysiert, wie Netzsperren implementiert werden und welche Techniken zu ihrer Umgehung existieren. Weiterhin beleuchtet das Kapitel vorhandene Untersuchungen und Studien, die sich mit der Bewertung der Effektivität und den Auswirkungen von Netzsperren beschäftigen.

2.1. Grundlagen von Netzsperren

Netzsperren beschränken oder verhindern den Zugang zu bestimmten Inhalten im Internet bzw. im World Wide Web[1] und werden eingerichtet, um gesetzliche Anforderungen zu erfüllen, Urheberrechte zu schützen oder politische und ethische Normen durchzusetzen. Technisch gesehen können Netzsperren auf verschiedenen Ebenen des Netzzugangs erfolgen, zum Beispiel durch DNS-Sperre, IP-Sperre oder Unterbrechung des Datenverkehrs zu bestimmten Servern. Derartige Eingriffe in die Netzinfrastruktur werfen jedoch Fragen der Meinungsfreiheit und der Selbstbestimmung auf und motivieren die Entwicklung und den Einsatz von Umgehungstechnologien. Diese Technologien, zu denen VPNs, Proxy-Server, das Tor-Netzwerk und verschlüsselte DNS-Abfragen zählen, bieten den Nutzer*innen Möglichkeiten, Zensurmaßnahmen zu umgehen und den freien Zugang zu Informationen wiederherzustellen.

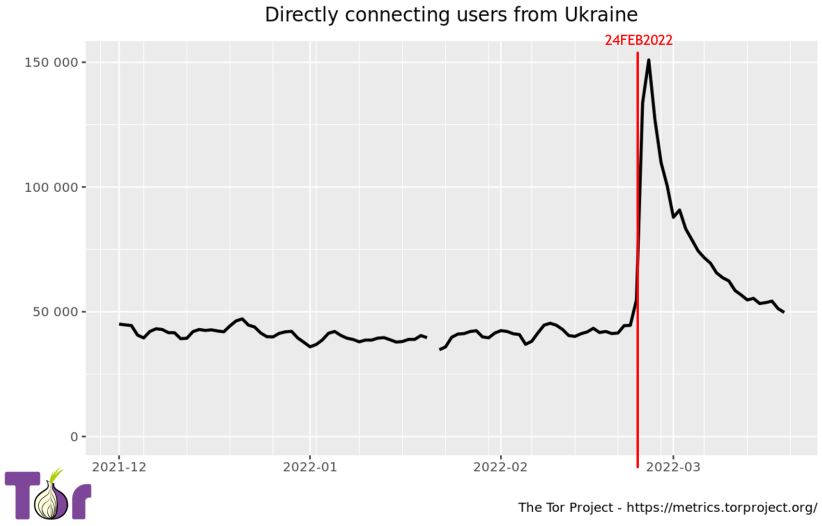
Die Verbreitung des Internetzugangs hat den schnellen und weit verbreiteten Austausch von Informationen auf der ganzen Welt ermöglicht. Das Internet hat Fernsehen, Printmedien und Radio in Bezug auf den Medieneinfluss überholt und ist seit den 2000er Jahren zu einem unersetzlichen Bestandteil unseres Lebens geworden [DKK17]. Mit der zunehmenden Bedeutung des World Wide Web haben die Regierungen der einzelnen Länder weltweit

[1]. Das Internet ist ein globales Netzwerk von Computern und Netzwerken, das verschiedene Dienste wie E-Mail, das World Wide Web und Internet-Telefonie ermöglicht. Das World Wide Web hingegen ist lediglich einer dieser Dienste und bietet ein System, durch das Informationen über Webseiten weltweit zugänglich gemacht werden. Umgangssprachlich werden Internet und World Wide Web regelmäßig als Synonyme verwendet.

begonnen, den Einfluss zu erkennen und zensieren Inhalte. Auch private Organisationen können Zensurmaßnahmen für ihre Internetnutzer*innen einführen [Mc11] oder von ihren Regierungen dazu gezwungen werden [Go17]. Internetzensur ist ein relativ neues Phänomen in der Geschichte der Menschheit. Mit dem Übergang vom Industrie- zum Informationszeitalter wurden Informationstechnologien und Computersysteme für das Funktionieren und den Fortschritt der Gesellschaft von zentraler Bedeutung. Die ersten Internet-ähnlichen Möglichkeiten, wie das Advanced Research Projects Agency Network (ARPANET), standen nur staatlichen Stellen und Forscher*innen ausgewählter Institutionen zur Verfügung. Mit dem Aufkommen des World Wide Web in den frühen 1990er Jahren und sinkenden Kosten für Computerhardware und -software wurden Internettechnologien weltweit für Durchschnittsbürger*innen verfügbar. Die Verbreitung von Geräten, die mit dem Internet verbunden sind, nimmt weiter zu und ermöglicht es immer mehr Menschen, über verschiedene Medien und Protokolle weltweit und nahezu in Echtzeit zu kommunizieren [Ma23, S. 16].

Aceto und Pescapé definierten Internetzensur als die absichtliche Beeinträchtigung oder Sperrung des Zugangs zu Online-Ressourcen und -Diensten, unabhängig von der Absicht, dem Umfang oder der Legitimität der Maßnahmen [AP15]. Die technischen Mittel, mit denen Netzsperren umgesetzt werden, sind sehr unterschiedlich, aber im Allgemeinen durch standardisierte Internet-Protokolle begrenzt. Einige Internetzensoren blockieren Webseiten mit anstößigem Inhalt und informieren die Nutzer*innen, dass ihre Anfrage abgelehnt wurde. Andere unterbrechen einfach die Verbindung oder manipulieren den Datenverkehr, sodass die Verbindung scheinbar nicht zustande kommt. Andere drosseln die Konnektivität von Nutzer*innen, wenn unerwünschte Aktivitäten erkannt werden, und machen die Kommunikation unbrauchbar. Neben der Blockierung von Kommunikation ist die Internetüberwachung eng mit Zensurmaßnahmen verbunden. Das Aufspüren unerwünschter Inhalte ist in der Regel der erste und wichtigste Schritt vor einer Sperrung. Aggressivere staatliche Zensoren unterbrechen die Internetverbindung bei kritischen Ereignissen wie Wahlen oder zivilen Unruhen auch komplett [Ma23, S. 16].

In den letzten drei Jahrzehnten gab es unzählige Beispiele für Internet-Zensur. Soziale Bewegungen wie der Arabische Frühling in den frühen 2010er Jahren wurden durch den Einsatz von Technologie zur Organisation von Protesten und zum Sammeln von Unterstützung beschleunigt und wurden zur Zielscheibe der Zensur. Autoritäre Führer*innen haben ihre Bereitschaft gezeigt, selektiv Informationen zu zensieren, die sie als gefährlich für den Machterhalt erachten, und in turbulenten Zeiten manchmal die Internetverbindung komplett zu unterbrechen [DS20]. Viele Studien haben sich mit der Great Firewall of China (GFW) beschäftigt, welcher zur Zensur und Überwachung in der Volksrepublik China eingesetzt wird. Die GFW wird als die aggressivste staatliche Zensurmaßnahme angesehen [Bo21; Ho21; KR21; Or23; WBC21]. Von März 2018 bis Juli 2019 blockierte die Republik Tschad in Afrika den Zugang zu allen wichtigen Social-Media-Plattformen, einschließlich WhatsApp, Twitter, Instagram, YouTube und Facebook, aus "Sicherheitsgründen im Zusammenhang mit terroristischen Anschlägen" [Da19]. Im Juli 2021 gingen Kubaner*innen auf die Straße, um gegen den Umgang der Regierung mit der COVID-19 Pandemie zu protestieren. Während der



Abbildungsverzeichnis 2.1.: Ukrainische Tor-Verbindungen nach der russischen Invasion 2022. Quelle: [To22]

Demonstrationen schränkten Regierungsbeamte den Zugang zu Facebook und WhatsApp ein. Viele kubanische Nutzer*innen wandten sich an das in den USA beheimatete Anti-Zensur-Tool Psiphon [Ps24], um einen offenen Kommunikationszugang zu erhalten [Sh21]. In Österreich führten breit angelegte Netzsperren im Jahr 2022, initiiert durch Urheberrechtsforderungen, zur unbeabsichtigten Blockierung zahlreicher legaler Webseiten. Kritiker*innen vergleichen das Vorgehen mit dem Schließen eines gesamten Einkaufszentrums wegen eines einzelnen Vergehens in einem Geschäft und betonen die Unverhältnismäßigkeit sowie die Notwendigkeit einer zielgerichteteren Herangehensweise, um sogenanntes Overblocking zu vermeiden und die Meinungsfreiheit nicht unnötig einzuschränken [Re22a].

Im Februar 2022 zeigten Messungen der Gesamtnutzung des Tor-Netzwerks einen Anstieg der Verbindungen aus der Ukraine um mehr als 300 Prozent unmittelbar nach dem Einmarsch Russlands in das Land [To22]. Nach dem 24. Februar ging die Nutzung rapide zurück, möglicherweise aufgrund der Zerstörung der Infrastruktur von Mobilfunkmasten durch russische Streitkräfte oder der allgemeinen Vertreibung von Zivilisten (siehe Abbildung 2.1). Während des gesamten Konflikts sind die Ukrainer*innen weiterhin auf virtuelle private Netzwerke (VPN) und Anti-Zensur-Technologien angewiesen, da Russland den Internetverkehr aus Teilen der Ukraine über russische Provider umleitet [Sa22].

2.1.1. Das Internet in Österreich

Auf Initiative von IBM erfolgte 1985 die erstmalige Anbindung der Universität Linz an das European Academic and Research Network (EARN). Dieses Netzwerk galt zu dieser Zeit als das größte wissenschaftliche Datennetzwerk, welches bereits hunderte von Forschungseinrichtungen mittels IBM-Technologie miteinander verband. Die Kooperation mit dem amerikanischen Netzwerk BITNET verstärkte seine Bedeutung zusätzlich. Die

erfolgreiche Integration der Universität Wien in das Netzwerk folgte 1986, nachdem dort ebenfalls auf IBM-Hardware umgestellt wurde [RO19].

Mit dem schnellen Wachstum des Netzwerks und der zunehmenden Anzahl angebundener Universitäten entstand der Bedarf nach einer effektiven Verwaltungsstruktur. Dies führte zur Gründung des Vereins ACOnet, der mittlerweile über 200 Mitglieder zählt und eine wichtige Rolle in der Anbindung österreichischer Bildungseinrichtungen, Ministerien sowie Landesregierungen an das Internet spielt [RO19]. Auf der Grundlage der 1987 von IBM initiierten Gründung der European Super Computer Initiative (EASI) und der Etablierung des EASInet-Netzwerks, entschied man sich 1990 für einen signifikanten Wechsel in der Netzwerktechnologie. Anstelle der bis dahin verwendeten proprietären IBM-Netzwerkarchitektur SNA (Systems Network Architecture) setzte man fortan auf das herstellerneutrale Transmission Control Protocol/Internet Protocol (TCP/IP). Diese Umstellung markierte einen entscheidenden Schritt in der Vernetzung der akademischen Welt. Speziell für die Universität Wien hatte dieser Wechsel am 10. August 1990 weitreichende Bedeutung: Sie wurde als erster Netzwerkknoten in Österreich an das globale Internet angeschlossen, was einen Meilenstein in der digitalen Vernetzung des Landes darstellte [RO19].

In der Zeit des politischen Wandels in Osteuropa im Jahr 1989 veränderte sich auch die geografische und strategische Bedeutung Wiens dramatisch. Von einer Randlage im Osten der westlichen Welt wurde Wien zum Zentrum eines sich neu formierenden Europas. Diese veränderte Position verstärkte auch die Relevanz des Wiener Internetknotenpunkts. In dieser Zeit der Umbrüche begann zudem das Aufkommen der ersten kommerziellen Internetanbieter. 1991 wurde das Konsortium Ebone ins Leben gerufen, eine Initiative, die gemeinsam von neu etablierten kommerziellen Internetanbietern in Europa getragen wurde, um den Betrieb von Internetverbindungen auf europäischer Ebene zu koordinieren. Als Pionier unter den österreichischen kommerziellen Internetanbietern trat die Firma EUnet in Erscheinung, gefolgt von weiteren Unternehmen wie Planet oder Ping. EUnet, das einerseits Kunde des ACOnet war, unterhielt andererseits auch eine eigene Verbindung nach Amsterdam. Die ineffiziente Praxis, Daten unnötig lange Wege zurücklegen zu lassen, führte schließlich zur Einigung auf ein Peering-Abkommen zwischen den beteiligten Parteien, um Datenverkehr effizienter zu gestalten [RO19]. Das neue Institutsgebäude der Universität Wien beherbergt das EDV-Zentrum, in dem der Vienna Internet Exchange (VIX) errichtet wurde. Dieser ermöglicht einen kostenfreien Datenaustausch zwischen verschiedenen Netzwerken. Der VIX, der nach wie vor unter der Verwaltung des Zentralen Informatikdienstes (ZID) der Universität Wien steht, verfügt heute über drei Standorte und zieht rund 150 nationale sowie internationale Akteure an [AC24b]. Im Januar 1988 setzte Peter Rastl, der damalige Leiter des Zentralen Informatikdienstes (ZID) an der Universität Wien, einen wichtigen Schritt in der Netzwerkverwaltung, indem er die Country-Code-Top-Level-Domain .at zur Betreuung durch den Verein ACOnet anmeldete. Dieser Prozess war nach Rastls Aussage in einem Interview unkompliziert: Eine einfache E-Mail an Jon Postel, der für solche Aufgaben zuständig war, genügte. Postel bestätigte das Anliegen mit einem knappen "done", womit der Vorgang abgeschlossen war [IS17, S. 22]. Diese Initiative führte dazu, dass das ZID der Universität Wien über mehrere Jahre hinweg die Rolle des Domain-

Registrars für Österreich übernahm. Die Verantwortung für die Vergabe von Domains wurde an die Interessensvertretung der Internet Service Provider Austria (ISPA) übergeben, welche dafür die NIC.at Internet Verwaltungs- und Betriebs GmbH ins Leben rief. Seit dem 1. Juli 1988 obliegt dieser Gesellschaft die Zuständigkeit für die Domainvergabe in Österreich. [IS17, S. 22]. Seither sind etwa 1,5 Millionen Domains unter der Endung .at registriert worden [st24].

2.1.2. Entwicklung der Internet-Regulierung in Österreich: Der Providerstreik von 1997

Im März 1997 ereignete sich in Österreich ein bemerkenswertes Ereignis, das die Internet-Regulierung und die Rechte der Internet Service Provider maßgeblich beeinflusste. Am 20. März 1997 wurden sämtliche Computer des Internet Service Providers ViP (Verbindungen in Perfektion, der in seiner ursprünglichen Form nicht mehr existiert) von der Wirtschaftspolizei beschlagnahmt. Dies geschah im Rahmen einer Hausdurchsuchung wegen des Verdachts, dass ein Kunde von ViP gegen das Gesetz zum Schutz vor Kinderpornographie (§ 207a StGB) verstoßen habe. Die Beschlagnahmung erfolgte, obwohl der verdächtige Kunde der Staatsanwaltschaft bereits bekannt war und nicht der Internet Service Provider, sondern ein einzelner Kunde den Verdacht ausgelöst hatte.

Die Konsequenz dieser Maßnahme war weitreichend: Nicht nur der betroffene Kunde, sondern auch alle anderen Kund*innen des Providers wurden abrupt vom Internetzugang abgeschnitten. Dies führte bei vielen Unternehmen, die auf den Internetzugang angewiesen waren, zu erheblichen wirtschaftlichen Einbußen. Die Vorgehensweise der Behörden war aus Sicht vieler Beobachter*innen nicht nachvollziehbar und schien willkürlich, was erhebliche Diskussionen über die Verantwortlichkeiten und Rechte von Internet Service Providern auslöste.

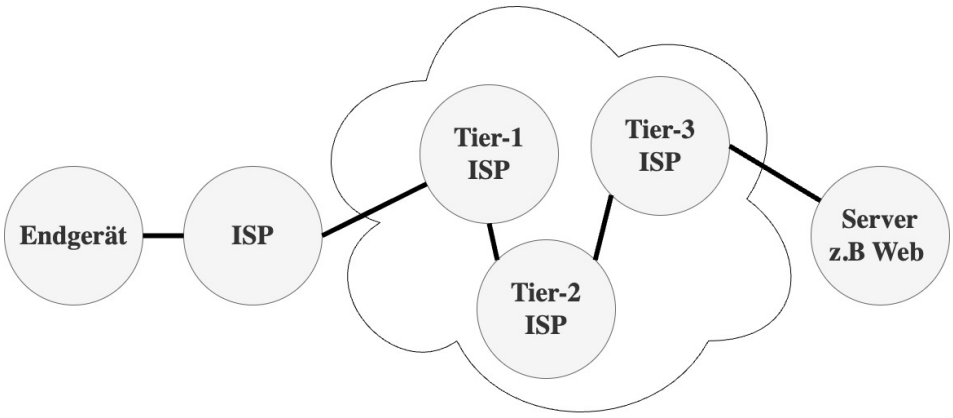
Als Reaktion auf diese als ungerechtfertigt empfundene Aktion organisierten die österreichischen Internet Service Provider am 25. März 1997 einen zweistündigen Internetstreik. Diese symbolische Aktion unterstrich die Bedeutung und Abhängigkeit der modernen Gesellschaft vom Internet. Die Tatsache, dass fast ganz Österreich vom Internet abgeschnitten war, verdeutlichte die Tragweite und die Notwendigkeit einer klaren und fairen Regulierung im digitalen Raum.

Die Ereignisse des Jahres 1997 führten schließlich zur Gründung der ISPA (Internet Service Providers Austria), einer Vereinigung, die sich für die Rechte und Interessen der Internet Service Provider einsetzt. Die damaligen Ereignisse zeigten nicht nur die Notwendigkeit einer Differenzierung zwischen Internet Service Providern und Hosting-Dienstleistern und einer klaren Regelung der Verantwortlichkeiten, sondern auch die Wichtigkeit einer Selbstorganisation der Branche. Bis heute setzt sich die ISPA für Rechte im digitalen Raum ein und kämpft für Themen wie die Nicht-Überwachung und Nicht-Zensur von Kommunikation durch Internet Service Provider. Die Diskussionen um die Rolle und Verantwortung von Internet Service Providern sind bis heute aktuell und zeigen, wie

prägend die Ereignisse des Jahres 1997 für die Internet-Regulierung in Österreich waren [IS17, S. 29], [Il24].

2.1.3. Internet Service Provider

Endgeräte (auch Hosts genannt) sind über Internet Service Providers (ISP) mit dem Internet verbunden. Beispiele für einen ISP in Österreich sind A1, Magenta, spusu, Kabelplus und Drei. Bei der Rundfunk und Telekom Regulierungs-GmbH (RTR) kann man eine Liste aller ISPs in Österreich abrufen (`https://www.rtr.at/TKP/service/agg-verzeichnis/Uebersichtseite.de.html`, abgerufen am 25. März 2024). Es gibt ISPs auf verschiedenen Ebenen. ISPs, die das Backbone-Netz betreiben, in Unternehmen, in Universitäten, in Privathaushalten und die WiFi-Hotspots in Flughäfen, Cafés, Hotels oder auf öffentlichen Plätzen anbieten. Kurz: ISPs ermöglichen Kund*innen den Zugang zum Internet über eine Zugangstechnologie (z.B. FTTH (Fibre-To-The-Home), DSL (Digital Subscriber Line) oder 5G (Mobilfunk)) [Ka24a]. Diese Internet Service Provider sind wiederum mit Internet Service Providern einer oberen Ebene verbunden, die in der Regel für den Betrieb des Internet-Kernnetzes verantwortlich sind, in dem Hochgeschwindigkeits-Glasfaserverbindungen (1-100 Gbit/s) über Router auf nationaler und internationaler Ebene verbunden sind (Backbones). Wie angesprochen, sind die Internet Service Provider hierarchisch organisiert. Ein Tier-1-ISP betreibt Internet-Backbones, ein Tier-2-ISP ist für die regionale oder nationale Abdeckung zuständig und benötigt einen Dienst von einem Tier-1-ISP, ein Tier-3-ISP deckt ein kleineres Gebiet ab und ist ein Kunde eines Tier-2-ISP. Ein solches lokales Netz kann ein Glasfasernetz oder ein lokales drahtgebundenes Telefonnetz sein, um den Zugang zum Internet zu ermöglichen. Zu den drahtgebunden Zugangstechnologien gehört DSL (Digital Subscriber Line). DSL nutzt Telefonleitungen für den Zugang zu den Netzen der ISPs. Wenn ein Haushalt einen DSL-Anschluss hat, nutzt er das Telefonnetz sowohl für Daten als auch für Sprachsignale. Ein ISP ist mit anderen ISPs über einen Point of Presence (POP) verbunden. In einem POP können netzübergreifend Verbindungen hergestellt werden, da dort zum Beispiel Router von ISP-A mit Routern von ISP-B eine Verbindung herstellen. Diese POPs befinden sich in der Regel in Rechenzentren. Wenn ein ISP ein größeres Gebiet erschließen will, schließt er im Allgemeinen einen Vertrag mit einem höherrangigen ISP ab, mietet Kommunikationsverbindungen und verbindet seine Router über POPs mit den Routern des höherrangigen ISP. In diesem Vertrag wird der höherrangige ISP zum Anbieter und der unterrangige ISP zum Kunden. Falls zwei ISPs auf dem gleichen Hierarchie-Level miteinander verbunden sind, agieren sie als gleichgestellte Partner (Peers) [Kw15, S. 6]. Die österreichischen Provider sind im Verband Internet Service Providers Austria (ISPA) organisiert [IS24c]. In Abbildung 2.2 wird vereinfacht der Aufbau des Internets dargestellt. Von links beginnend ist ein Endgerät abgebildet, welches den Ausgangspunkt der Verbindung darstellt. Von dort geht die Verbindung zu einem ISP, der als Eintrittspunkt zu weiteren ISPs im Netzwerk fungiert und damit das Bindeglied zu weiteren Netzwerkebenen ist. In der Wolke sind drei Ebenen von ISPs dargestellt: Tier-1, Tier-2 und Tier-3. Diese Ebenen bilden eine hierarchische Netzwerkstruktur, wobei Tier-1 ISPs das höchste Level repräsentieren, oft als Backbone-Provider, die große, internationale Netzwerke unterhalten. Tier-2 ISPs verbinden sich normalerweise mit mindestens einem



Abbildungsverzeichnis 2.2.: Vereinfachter Aufbau des Internets.

Tier-1 ISP und möglicherweise mit anderen Tier-2 ISPs, um Netzwerkzugriff zu ermöglichen. Tier-3 ISPs verbinden sich mit Tier-2 ISPs (und möglicherweise Tier-1 ISPs) und sind oft die ISPs, die Dienste direkt an Endkunden liefern. Auf der rechten Seite der Abbildung, ist ein Server abgebildet, der eine spezifische Dienstleistung wie beispielsweise eine Website zur Verfügung stellt. Dieser Server stellt Ressourcen zur Verfügung, auf die das Endgerät zugreift. Er ist in diesem Beispiel mit einem Tier-3 ISP verbunden und vervollständigt somit den Weg der Daten vom Endgerät der Nutzer*innen durch das Internet.

2.1.4. Internet Standards

Die Verbreitung des Internets ist mit der Entwicklung von Standards für verschiedene Anwendungsbereiche verbunden. Diese Standards sind nicht nur für die technische Umsetzung und Interoperabilität wesentlich, sondern auch für das Verständnis und die Beurteilung von Netzsperren und deren technischen Umgehungsmöglichkeiten. Sie definieren die Rahmenbedingungen, innerhalb derer Netzsperren implementiert und umgangen werden können. Sie haben damit direkten Einfluss auf die Wirksamkeit und Durchführbarkeit von Zensurmaßnahmen sowie auf die Entwicklung von Umgehungsmethoden.

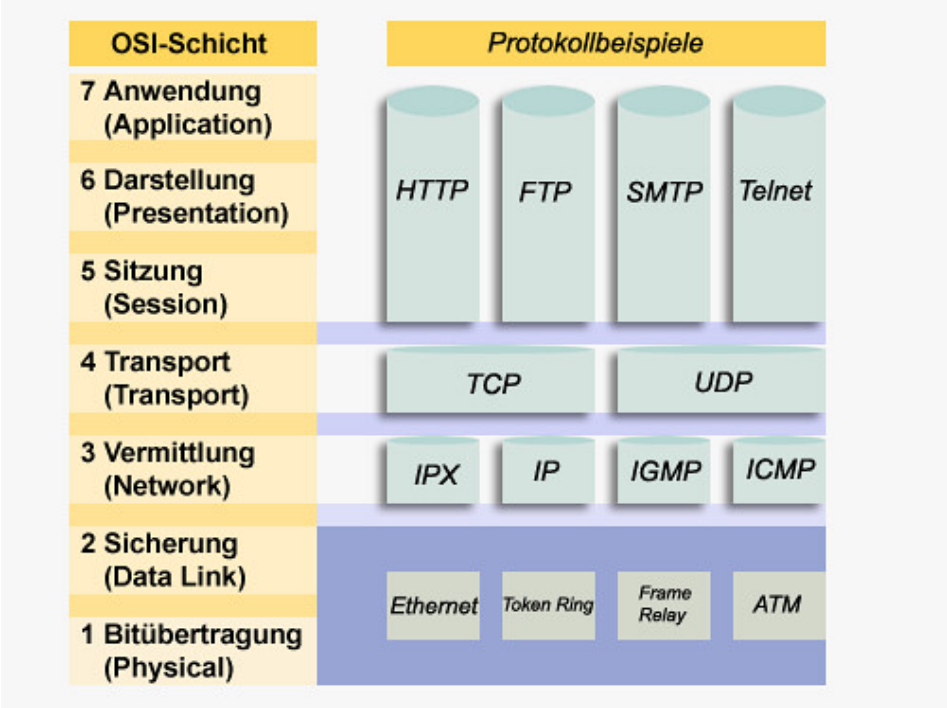
TCP/IP

Das wichtigste Protokoll ist TCP/IP (Transmission Control Protocol/Internet Protocol). TCP ist dabei für den Datentransport unter Beibehaltung der Integrität der Daten zuständig. Das Internet Protocol hingegen steuert die Kommunikation zwischen einzelnen Computern. Diese beiden Protokolle bilden fundamentale Bausteine des OSI-Schichtenmodells, welches insgesamt sieben Schichten umfasst, wie in der dargestellten Abbildung 2.3 zu sehen ist [Jo22, S. 23]. Die ursprüngliche Entwicklung von TCP/IP wurde von der DARPA (Defense Advanced Research Projects Agency), einer Behörde des US-Verteidigungsministeriums,

in den Jahren 1960-70 finanziert (z. B. wurde das ARPANET 1966 gestartet). Heute ist die IETF (Internet Engineering Task Force) zuständig für TCP/IP und verwandte Protokolle, deren Einzelheiten in RFCs (Request for Comments) niedergeschrieben sind [Kw15, S. 4]. Die Zuweisung eindeutiger Identifikatoren für Hosts im Internet erfolgt durch das Internetprotokoll (IP). Jeder Host erhält eine einzigartige, weltweit gültige IP-Adresse. Die ursprünglich eingeführte Protokollversion, IPv4 [Po81], verwendet eine Adressierung, die aus vier Byte besteht, wobei jedes Byte durch einen Wert zwischen 0 und 255 repräsentiert wird. Diese Struktur resultierte in einer begrenzten Anzahl von Adressen, die durch die Vergabepolitik und das Wachstum des Internets rasch knapp wurden. Als Reaktion darauf wurde IPv6 [DH17] entwickelt, eine erweiterte Spezifikation, die Adressen aus acht Gruppen von je vier hexadezimalen Ziffern zusammensetzt und somit einen deutlich vergrößerten Adressraum bietet, um den zukünftigen Anforderungen des Internets gerecht zu werden [Es21, S. 6]. Jedes Gerät, das sich mit dem Internet verbindet, sei es ein Computer, ein Smartphone, ein Tablet-PC, eine Spielkonsole, ein Fernseher oder ein netzwerkfähiger Drucker, ist im weltweiten Netz durch eine eindeutige IP-Adresse identifizierbar. Aufgrund der Komplexität und Benutzerunfreundlichkeit dieser numerischen Adressen wurden Domainnamen eingeführt. Diese wandeln IP-Adressen in leichter zu merkende Buchstabenkombinationen wie `www.fernfh.ac.at` um. Menschen neigen dazu, in Namen zu denken und zu arbeiten, während das technische Netz die diesen Namen entsprechenden IP-Adressen findet und verwendet. Die Vergabe dieser Internet-Namen, auch Domains genannt, erfolgt durch spezialisierte Organisationen, sogenannte Registrierungsstellen. In Österreich wird beispielsweise die Domain `.at` von der nic.at GmbH mit Sitz in Salzburg vergeben. Technisch gesehen sind Domain-Namen nicht zwingend notwendig, da der Zugriff auf Webseiten auch direkt über die Eingabe der IP-Adresse möglich ist. Tatsächlich führt die Verwendung von Domain-Namen zu einer geringfügigen Verzögerung beim Aufruf von Webseiten, da der Webserver zunächst den entsprechenden Nameserver kontaktieren muss, um die zugehörige IP-Adresse zu erfragen [Ka24b].

WEB-Technologie

Darunter wird im Wesentlichen beim Anbieter die Server-Technologie und beim Benutzer*in die WEB-Browser-Technologie verstanden. Die ursprüngliche Idee des WEB bestand aus zwei Elementen: Uniform Resource Locator (URL) und Hypertext Markup Language (HTML). URLs ermöglichen es bequem von einer Website zur anderen zu gelangen. Dieser Vorgang wird auch als Surfen bezeichnet [Jo22, S. 23]. Ein Uniform Resource Locator definiert die Adresse einer spezifischen Website im World Wide Web [BFM05]. Sie hat immer folgenden Aufbau: `https://www.domainname.toplevel/file.html`
Beispiel: `https://www.fernfh.ac.at/weiterbildung`
Die Domain `.ac.at` ist eine Top-Level-Domain (TLD), die für akademische Institutionen, Universitäten und Forschungseinrichtungen in Österreich verwendet wird. Somit zeigt `.ac.at` an, dass es sich um eine akademische oder bildungsbezogene Website in Österreich handelt [AC24a][Kl05]. Unter `/weiterbildung` wird die spezifische Seite

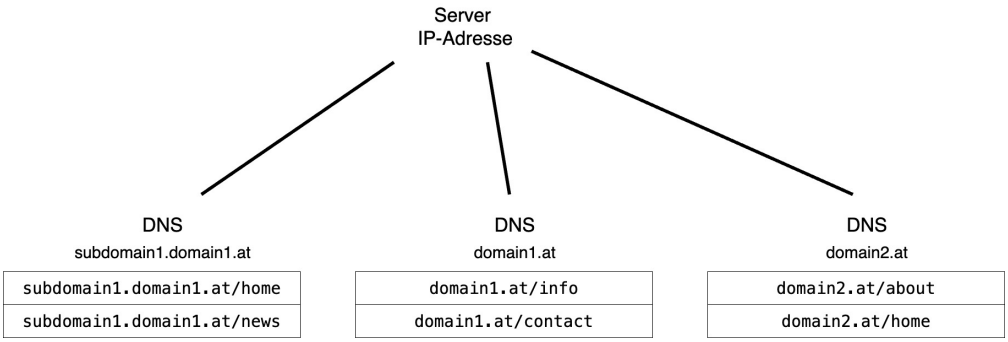


Abbildungsverzeichnis 2.3.: OSI Modell, Quelle: [ne09]

über die Weiterbildungsmöglichkeiten an der FernFH aufgerufen. HTML (Hypertext Markup Language) ist ein Standard, der es ermöglicht, Dokumente auf verschiedenen Geräten anzuzeigen. Inzwischen hat sich das Web stark weiterentwickelt und es ist heute selbstverständlich, dass nicht nur Texte und einfache Bilder, sondern auch Audio- und Videoinhalte von allen Geräten interpretiert werden können. Zur Steigerung des Komforts und der Geschwindigkeit werden personalisierte Informationen auf dem Endgerät gespeichert, um den Kund*innen unnötige, sich wiederholende Arbeitsschritte zu ersparen (Cookies) [Jo22, S. 23]. Weitere WEB Präsentations- und Datenaustauschstandards sind XML (Extensible Markup Language) sowie eine Unzahl von grafischen Formaten wie z. B. GIF, TIF, JPEG, PNG. [Jo22, S. 24].

HTTP und HTTPS

Das Hypertext Transfer Protocol (HTTP) und das Hypertext Transfer Protocol Secure (HTTPS) sind zentrale Kommunikationsprotokolle im World Wide Web, die den Datenaustausch zwischen Webservern und Browsern regeln. Während HTTP die Grundlage für die Übertragung von Informationen zwischen Server und Browser darstellt, erweitert HTTPS diese Funktion um eine entscheidende Sicherheitskomponente. HTTPS ermöglicht die verschlüsselte Übertragung von Daten, um die Sicherheit und den Datenschutz der übermittelten Informationen zu gewährleisten. Durch die Implementierung von Transportverschlüsselung schützt HTTPS die Daten vor dem Abhören durch Dritte, wodurch eine sichere Kommunikation im Internet ermöglicht wird [FNR22].



Abbildungsverzeichnis 2.4.: Darstellung einer IP-Adresse im Internet und der mit dieser über DNS verknüpften Domainnamen. Quelle: Basierend auf [Th20, S. 7]

Aufruf einer WWW-Seite

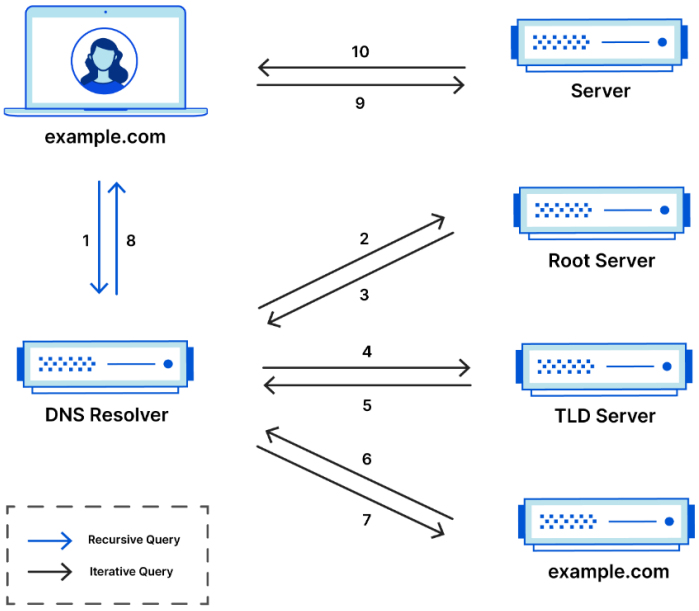
Beim Aufruf einer Webadresse wie zum Beispiel `www.fernfh.ac.at` ist es oft nicht notwendig, das Protokoll (z.B. http://) explizit einzugeben, da moderne Browser dies automatisch erledigen. Der Prozess beginnt damit, dass Nutzer*innen eine Anfrage an einen Domain Name Server des Internet Service Provider sendet. Dieser DNS sucht in seiner umfangreichen und ständig aktualisierten Datenbank nach der IP-Adresse, die der eingegebenen Domain zugeordnet ist. Findet der DNS die gesuchte IP-Adresse nicht, wird die Anfrage an weitere DNS-Server im Internet weitergeleitet, bis die entsprechende Adresse gefunden ist. Diese wird dann an den Webserver zurückgegeben. Der Webserver wandelt die ursprünglich textbasierte Adresse in eine maschinenlesbare numerische IP-Adresse um und leitet die Anfrage an den Server weiter, der die Zielwebseite hostet, wie in Abschnitt 2.1.4 detailliert erläutert wird. Die angeforderten Daten werden über zahlreiche Zwischenstationen im Internet zurück an den Internet Service Provider gesendet, von wo sie schließlich auf dem Computer der Nutzer*innen gelangen. Die Website wird dann im Browser der Nutzer*innen geladen und angezeigt. Die Daten im Internet werden in einzelne Pakete aufgeteilt. Diese Datenpakete können über verschiedene Routen durch das weltweite Netz geschickt werden, manchmal auch über Umwege, die geografisch weit vom direkten Weg entfernt sind, wie zum Beispiel von Salzburg über Paris oder New York nach Wien. Durch den Einsatz neuer Satellitentechnologien ist sogar eine Datenübertragung über den Weltraum möglich. Für Nutzer*innen sind diese Umwege und der genaue Weg der Datenpakete jedoch nicht bekannt. Wichtig ist, dass die Daten ihr Ziel erreichen. Obwohl die Übertragungszeit in der Regel unter 100 Millisekunden beträgt, kann es zu Verzögerungen kommen, wenn die Netze durch eine hohe Auslastung überlastet sind und dadurch die Datenübertragung verlangsamt wird oder die Daten nicht rechtzeitig ankommen [Sc13].

Die Abbildung 2.4 skizziert vereinfacht einen Server mit einer IP-Adresse im Internet, die von den physischen Maschinen (z. B. Webserver) verwendet wird. Der Server ist über die Domainnamen `subdomain1.domain1.at`, `domain1.at` sowie `domain2.at` erreichbar. In den Rechtecken sind konkrete Ressourcen durch ihre jeweiligen Domainnamen dargestellt, wie zum Beispiel `subdomain1.domain1.at/home`.

Domain Name System

Das Domain Name System (DNS) ist ein dezentrales und hierarchisches System zur Namensauflösung. Es wird verwendet, um Domainnamen in die zugehörigen IP-Adressen umzuwandeln. DNS ermöglicht es Benutzer*innen, Webseiten über benutzerfreundliche Namen wie `fernfh.ac.at` zu erreichen, anstatt IP-Adressen (in diesem Beispiel `5.132.190.70`) verwenden zu müssen. Die Entwicklung des DNS wurde erstmals in den RFCs 882 und 883 vorgeschlagen. Diese wurden mittlerweile durch RFC 1034 und RFC 1035 ersetzt [RF83a; RF83b; RF87a; RF87b]. DNS ist vergleichbar mit einem Telefonbuch oder einer Telefonauskunft im Telefonnetz. Ein Domainname entspricht dabei dem eingetragenen Teilnehmernamen im Telefonbuch und die IP-Adresse entspricht der zugehörigen Telefonnummer. DNS unterstützt auch die Ermittlung von Domainnamen zu gegebenen IP-Adressen, das sogenannte `Reverse Lookup`. Wenn ein Eintrag für einen Domainnamen im DNS fehlt, kann die Auflösung nicht vorgenommen werden. Die Anwendung (z. B. Webbrowser) gibt eine Fehlermeldung aus, wenn keine Verbindung hergestellt werden kann. Eine Verbindung zur IP-Adresse ist jedoch möglich, solange eine Route dorthin existiert. Dies ist vergleichbar mit dem Wählen einer Telefonnummer, unabhängig davon, ob sie im Telefonbuch eingetragen ist. Das Domain Name System ist einer der wichtigsten Basisdienste des Internets, da es die Benutzung des Internets für Menschen komfortabel ermöglicht. Das System ist ausfallsicher, mehrfach redundant und weltweit verteilt realisiert worden. Es handelt sich um ein hierarchisches System mit Root-Servern, das aus einer Vielzahl dezentral betriebener Nameserver (DNS-Server) besteht. Die Hierarchieebenen spiegeln sich in den symbolischen Namen wider, die durch einen Punkt . angegeben sind. Die oberste Ebene entspricht genau diesem Punkt. Er bildet den Abschluss jedes Domainnamens und kann daher weggelassen werden (statt `www.fernfh.ac.at` müsste es also korrekt `www.fernfh.ac.at.` heißen). Für jeden DNS-Namen gibt es einen autoritativen DNS-Server, der für bestimmte DNS-Namen verantwortlich ist und seine Informationen direkt von den Besitzer*innen des DNS-Namens oder dem ISP, bei dem der DNS-Name registriert wurde, erhält. Im Gegensatz dazu senden nicht-autoritative DNS-Server Informationen weiter, die sie von anderen DNS-Servern erhalten haben. Der Einsatz nicht-autoritativer DNS-Server ist sinnvoll, da sie DNS-Einträge lokal zwischenspeichern (cachen) können, um sie bei erneuter Anfrage schneller auszuliefern. Jedes Endgerät kann durch manuelle statische Konfiguration der Nutzer*innen oder durch den ISP einen DNS-Server konfiguriert bekommen [An08, S. 16-17].

Auf Abbildung 2.5 ist der Prozess eines vollständigen DNS-Lookups und einer Webseitenanfrage dargestellt. Dabei wird die Domain `example.com` angefragt. Es werden die verschiedenen Arten von Servern gezeigt, die in den Prozess involviert sind: DNS Resolver, Root-Server, TLD-Server und den Server, der die Domain `example.com` hostet. Die blauen Linien stellen die rekursive Abfrage dar, die sich durch die Abhängigkeit des Anfragenden von einer vollständigen Antwort des Resolvers auszeichnet. Die schwarzen Linien zeigen die iterativen Anfragen, die den Resolver zu verschiedenen Servern im DNS führen, bis die endgültige IP-Adresse gefunden ist [cl24b]. Dieser Anfrageprozess umfasst mehrere



Abbildungsverzeichnis 2.5.: DNS-Lookup und Websiteabfrage, Quelle: [cl24b]

Schritte, die in einer nummerierten Sequenz von 1 bis 10 aufgezeigt sind, wobei die Pfeile die Richtung der Anfrage oder Antwort angeben:

1. Rekursive Abfrage: Anfrage nach der Domain `example.com` an den DNS-Resolver. Rekursiv bedeutet hier, dass der Resolver alle notwendigen Anfragen stellt, bis er die endgültige Antwort erhält, die er zurückgibt.
2. Iterative Abfrage an den Root-Server: Der DNS-Resolver leitet die Anfrage iterativ weiter an den Root-Server. Im Gegensatz zur rekursiven Abfrage, bei der die Antwort vollständig zurückgeliefert wird, liefert eine iterative Abfrage Informationen, die den Resolver zum nächsten Schritt führen, ohne direkt die finale Antwort zu liefern.
3. Der Root-Server antwortet mit der Adresse des TLD-Servers (Top-Level-Domain Server).
4. Der DNS-Resolver leitet die Anfrage an den TLD-Server weiter.
5. Der TLD-Server antwortet mit der Adresse des Nameservers für `example.com`.
6. Der DNS-Resolver sendet eine Anfrage an den Nameserver der spezifischen Domain.
7. Der Nameserver für `example.com` antwortet mit der IP-Adresse der Domain.
8. Der DNS-Resolver gibt diese IP-Adresse an den Laptop zurück.
9. Der Laptop sendet eine direkte Anfrage an den Server, der `example.com` hostet.
10. Der Server liefert die angeforderten Daten, die zur Anzeige der Website `example.com` auf dem Laptop notwendig sind.

2.1.5. Internet Governance

Der Begriff Governance bezeichnet die Strukturen und Prozesse, die für die Führung und Regulierung innerhalb verschiedener Organisationen eingesetzt werden. Diese Strukturen basieren typischerweise auf einer Reihe von Richtlinien, die zwar selbstauferlegt sind, jedoch im Rahmen gesetzlicher und gesellschaftlicher Normen agieren. Da das Internet keine zentrale Unternehmensstruktur aufweist und es aufgrund seiner globalen Reichweite keiner einzelnen Rechtsprechung unterliegt, war die Schaffung eines angepassten Governance-Modells unerlässlich. Spezielle Organisationen wurden etabliert, deren Aufgabe die Entwicklung und Überwachung relevanter Internetregeln ist. Im Kontext von Netzsperren in Österreich ist insbesondere von Bedeutung, dass diese Organisationen ein ausgewogenes Verhältnis zwischen Regulierungsbedarf und den technischen Möglichkeiten der Umgehung solcher Sperren sicherstellen. Die Governance im Internet spielt daher eine entscheidende Rolle bei der Evaluierung der Effektivität von Netzsperren sowie der Entwicklung von technischen Umgehungsmethoden, da sie die rechtlichen und technischen Rahmenbedingungen definiert, innerhalb derer sich derartige Aktivitäten abspielen. Voraussetzung dafür ist, dass die Stakeholdergruppe groß genug ist [Jo22, S. 25].

Beim Weltgipfel zur Informationsgesellschaft (WSIS) im Jahr 2005, wurde folgendes gemeinsames Verständnis über Internet Governance verabschiedet [WS24]:

> Internet Governance sind Prinzipien, Regeln und Beschlussverfahren für die Entwicklung und Nutzung des Internets, die von Regierung, Privatwirtschaft und Zivilgesellschaft gemeinsam entwickelt und angewendet werden.

Das deutsche Bundesministerium für Digitales und Verkehr definiert Internet Governance folgendermaßen [BM24]:

> Unter dem Begriff Internet Governance werden Maßnahmen zusammengefasst, die den Zugang, die Stabilität und die Offenheit des Internets sicherstellen sollen. Denn trotz der grundsätzlich dezentralen Struktur des Internets müssen wesentliche Internetfunktionen verwaltet und begrenzte Internetressourcen effizient verteilt werden. Dies umfasst technische Aspekte wie die weltweite Vergabe von IP-Adressen und die Registrierung von Domainnamen, ebenso wie Themen von grundsätzlicher Bedeutung, darunter Datensicherheit, Künstliche Intelligenz und Netzneutralität.

Beispiele für wichtige Organisationen für Internet Governance werden folgend beschrieben.

Internet Governance Forum

Im Jahr 2006 initiierten die Vereinten Nationen das Internet Governance Forum (IGF), das seitdem alljährlich abgehalten wird. Die Einzigartigkeit dieses Forums liegt in seinem Multi-Stakeholder-Ansatz begründet, welcher Staaten, internationale Organisationen, die

Privatwirtschaft und zivilgesellschaftliche Akteure als gleichwertige Teilnehmer*innen einbezieht. Ein ähnliches Modell findet sich auf der europäischen Bühne als European Dialogue on Internet Governance (EuroDIG). In Anlehnung an diese Strukturen haben viele Länder eigene nationale Internet Governance Foren ins Leben gerufen. Diese Foren entwickeln auf nationaler Ebene Positionspapiere, die sowohl zur Unterstützung der nationalen Politikgestaltung dienen als auch in den globalen Diskurs eingebracht werden. Ihr Funktionieren basiert ebenfalls auf dem Prinzip des Multi-Stakeholder-Ansatzes, welcher es erlaubt, dass sämtliche betroffenen Parteien teilnehmen und ihre Standpunkte einfließen lassen. Im September 2014 führte Österreich sein erstes Internet Governance Forum Austria (IGF) durch, initiiert vom Bundeskanzleramt. Bei der Organisation halfen auch nic.at und die ISPA (Internet Service Providers Austria) als Co-Organisatoren mit [Gm24].

Global Digital Compact

Der Global Digital Compact (GDC) hat das Ziel, Grundsätze für ein offenes, freies und sicheres Internet sowie den Umgang mit neuen Technologien zu entwickeln. Er ist Teil des Reformprojekts "Our Common Agenda", das von UN-Generalsekretär António Guterres vorgestellt wurde. Die GDC soll beim UN-Zukunftsgipfel 2024 offiziell verabschiedet werden [GD24].

Internet Society (ISOC)

Die Internet Society (ISOC) wurde 1992 gegründet und ist eine globale gemeinnützige Organisation, die sich dafür einsetzt, das Internet zu einer Kraft für das Gute zu machen: Offen, global vernetzt, sicher und vertrauenswürdig. Sie hat ihren Hauptsitz in Reston, Virginia (USA) und Genf (Schweiz) und besteht aus mehr als 6000 Einzelpersonen sowie etwa 130 Organisationen aus über 170 Staaten. Die ISOC beherbergt die für die Internetstandards und Ressourcenverwaltung zuständigen Gremien wie zum Beispiel die Internet Engineering Task Force (IETF), Internet Engineering Steering Group (IESG) und Internet Research Task Force (IRTF). Seit ihrer Gründung hat es sich die ISOC zur Aufgabe gemacht, das Internet zu stärken und seine Reichweite zu erweitern [IS24a].

Internet Engineering Task Force (IETF)

Die Internet Engineering Task Force (IETF) ist eine Organisation, die seit 1986 Standards für das Internet entwickelt. Ihre Mission besteht darin, technische Dokumente zu erstellen, die die Gestaltung, Nutzung und Verwaltung des Internets beeinflussen. Diese Dokumente umfassen Protokollstandards, Best Practices und Informationsdokumente. Die IETF ist offen für alle, und es gibt keine formale Mitgliedschaft. Jeder kann teilnehmen, indem er sich für Mailinglisten anmeldet oder sich für IETF-Treffen registriert. Die IETF verfolgt Prinzipien wie offenen Prozess, dezentrale Kontrolle und Würde und Respekt für alle

Teilnehmer*innen. Sie veröffentlicht auch RFCs (Request for Comments), die wichtige Informationen über das Internet enthalten [IE24].

Internet Corporation of Assigned Names and Numbers (ICANN)

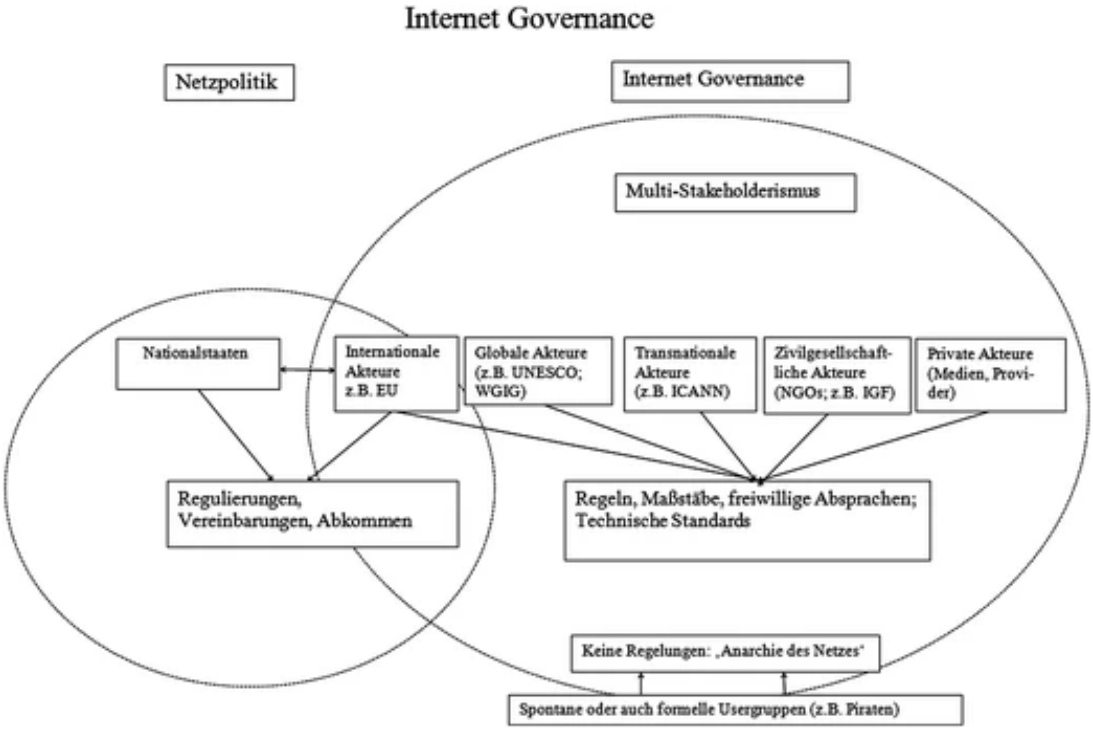
Die Internet Corporation for Assigned Names and Numbers, kurz ICANN, ist eine gemeinnützige Organisation, die eine zentrale Rolle in der Verwaltung und Koordination von Internet-Ressourcen spielt. Zu ihren Hauptaufgaben gehören die Verwaltung des zentralen Verzeichnisses der IP-Adressen, die Verantwortung für das Domain Name System (DNS) einschließlich der Root-Server und die Verwaltung sowohl der generischen Top-Level-Domains (gTLDs) als auch der länderspezifischen TLDs (ccTLDs). Gegründet wurde ICANN im Jahr 1998 als Nachfolgeorganisation von InterNIC, wobei sie anfangs unter der Aufsicht der US-Regierung stand, heute jedoch als unabhängige Entität agiert. ICANN legt großen Wert auf die Beteiligung der Gemeinschaft. Sie fordert Mitglieder und Interessenten auf, sich aktiv einzubringen, beispielsweise durch die Überprüfung von Empfehlungen oder die Mitgestaltung des nächsten gTLD-Programms [IC24].

World Wide Web Consortium (www.w3.org)

Das World Wide Web Consortium (W3C) ist eine internationale Organisation, die Standards für das Web entwickelt. Das Ziel ist, das Web barrierefrei, international, privat und sicher zu gestalten. Diese Standards finden in Browsern, Blogs und Suchmaschinen Anwendung und beeinflussen somit unsere Online-Erfahrungen. Mitglieder aus verschiedenen Bereichen, wie E-Commerce und Medien, arbeiten gemeinsam im W3C, um die Entwicklung des Internets voranzutreiben. Das Konsortium steht jedem offen, der an der Webstandardisierung mitwirken möchte. Dadurch wird das W3C zu einem wichtigen Akteur bei der Gestaltung der Zukunft des Internets [W324].

Internet Telecommuncations Union (ITU)

Die International Telecommunication Union (ITU) ist eine Sonderorganisation der Vereinten Nationen, die für viele Fragen der Informations- und Kommunikationstechnologien (IKT) zuständig ist. Sie wurde am 17. Mai 1865 als internationale Telegrafen-Union 80 Jahre vor der Gründung der Vereinten Nationen gegründet worden und ist damit die älteste UN-Agentur. Die ITU koordiniert weltweit Telekommunikationsnetze und -dienste in Zusammenarbeit mit Regierungen und der Privatwirtschaft. Ein wichtiger Bereich ihrer statistischen Arbeit ist die Erhebung von Daten über die Verbreitung von IKT, die Nutzung von Breitband- und Mobilfunkdiensten sowie die Entwicklung von IKT-Indikatoren. Diese Informationen sind für die Entwicklung politischer Maßnahmen und die Planung von Infrastrukturinvestitionen unerlässlich. Die ITU spielt auch eine wichtige Rolle bei der Festlegung technischer Normen für Telekommunikationsgeräte und -dienste. Sie fördert die Interoperabilität und die reibungslose Kommunikation zwischen verschiedenen Netzen



Abbildungsverzeichnis 2.6.: Überblick Stakeholder Internet Governance, Quelle: [BK13, S. 42]

und Technologien. Darüber hinaus setzt sich die ITU für den Zugang zu IKT in ländlichen und abgelegenen Gebieten ein, um die digitale Kluft zu verringern und sicherzustellen, dass alle Menschen von den Vorteilen der modernen Kommunikation profitieren können. Die ITU spielt eine zentrale Rolle bei der Förderung des globalen digitalen Wandels und der Schaffung einer vernetzten Welt für alle [IT24].

Zusammenhang Internet Governance und Netzsperren

Abbildung 2.6 zeigt, dass im Kontext der Verwaltung des Internets neben den genannten Organisationen wie ICANN, ITU oder ISOC, die sich den Hauptaufgaben der Internet-Regulierung widmen, unter anderem internationale Organisationen wie die Vereinten Nationen (UN), die UNESCO, die OECD, regionale Einheiten wie die Europäische Union (EU) und der Europarat sowie Vertreter aus der Zivilgesellschaft und der Privatwirtschaft. Diese Vielfalt an Beteiligten ist maßgeblich für den Prozess der Internet Governance, indem sie jeweils einzigartige Perspektiven, Expertisen und Interessen einbringen, die für die Formulierung und Umsetzung von Richtlinien und Standards von entscheidender Bedeutung sind.

Netzsperren sind eine Form der Regulierung, bei der bestimmte Inhalte oder Webseiten blockiert werden, um beispielsweise illegale Aktivitäten zu verhindern oder den Zugang zu sensiblen Informationen zu beschränken. Die Internet Governance beschäftigt sich

mit der Steuerung, Regelung, Nutzung und Bewertung des Internets. Sie umfasst verschiedene Aspekte wie technische Standards, politische Entscheidungsprozesse und die Zusammenarbeit zwischen verschiedenen Akteuren auf internationaler Ebene. Die Frage, wie das Internet reguliert werden sollte, ist ein zentrales Thema in der Internet Governance. Einige Länder, wie China, der Iran oder Russland, neigen dazu, das Internet nach dem Souveränitätsprinzip zu regulieren. Das bedeutet, dass sie die Kontrolle über den Zugang zu bestimmten Inhalten oder Webseiten ausüben. Netzsperren sind ein Instrument, das in solchen Ländern häufig eingesetzt wird, um den Informationsfluss zu steuern und unerwünschte Inhalte zu blockieren. Die Internet Governance muss einen Balanceakt zwischen der Sicherstellung der Meinungsfreiheit und dem Schutz vor schädlichen oder illegalen Inhalten finden. Die Diskussion über Netzsperren ist daher ein wichtiger Teil dieser Debatte und hat Auswirkungen auf die Gestaltung der digitalen Welt [Es18; Ho14].

2.1.6. Netzneutralität

Einer der Grundsätze des Internets ist das Neutralitätsprinzip. Es bedeutet, dass Internet Service Provider allen Teilnehmer*innen einen gleichwertigen Zugriff zu verschiedenen Internetservices gewähren. Das bedeutet es werden keine Prioritäten abhängig von Dateninhalten oder Protokollen gesetzt. Zum Unterschied davon, ist es im LAN (Local Area Network) und WAN (Wide Area Network) eines Unternehmens durchaus üblich, für bestimmte Dienste (z. B. Sprache) unterschiedliche Bandbreiten zu garantieren [Jo22, S. 25]. Die Telekom-Control-Kommission (TKK) und die RTR sind für die Durchsetzung der Netzneutralitätsregelungen in Österreich verantwortlich. Ihr Ziel ist es, den freien Zugang zum offenen Internet unter Berücksichtigung der Grundrechte aller Internetnutzer*innen und unter Wahrung der Interessen der Allgemeinheit zu gewährleisten. Zudem ist es Aufgabe der Regulierungsbehörden, dass das Internet als Umgebung für Innovationen weiterhin seine Rolle effektiv erfüllen kann [RT24c]. Einen jährlichen Überblick zu Aktivitäten bezüglich Netzneutralität in Österreich gibt der RTR Netzneutralitätsbericht. Eine Übersicht zu den Netzneutralitätsberichten findet man unter: `https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_reports.de.html` (abgerufen am 30.03.2024). Der Netzneutralitätsbericht von 2023 gibt auch einen Überblick über die Aktiväten zu Netzsperren [RT23b, S. 23-25].

Rahmenbedingungen Netzneutralität

Die gesetzliche Grundlage für Netzneutralitätsrichtlinien wird durch die Verordnung über die Netzneutralität (EU-Verordnung 2015/2120, bekannt als "TSM-VO") [EU15] und die damit verbundenen ergänzenden Bestimmungen im Telekommunikationsgesetz von 2021 geschaffen. Zudem spielen die Richtlinien des europäischen Gremiums der Regulierungsbehörden für elektronische Kommunikation (BEREC) [Eu22] eine wichtige ergänzende Rolle und müssen weitgehend berücksichtigt werden.

Die TKK und die RTR sind auf nationaler Ebene für die Durchsetzung der Vorschriften der Netzneutralitäts-Verordnung verantwortlich. Insbesondere ist die TKK für die

Durchführung von Aufsichtsverfahren gegen Internet Service Provider zuständig, wenn der Verdacht auf Verstöße gegen die Netzneutralitätsanforderungen gemäß Artikel 3 der TSM-VO besteht, wie in Artikel 5 Absatz 1 festgelegt. Die RTR bearbeitet als Geschäftsstelle der TKK vorbereitende Anfragen gemäß Artikel 5 Absatz 2 der TSM-VO und sammelt Informationen über technische sowie kommerzielle Praktiken der Internet Service Provider. Diese Informationen dienen als Grundlage für die Einleitung von Aufsichtsverfahren durch die TKK. Artikel 3 der TSM-VO enthält die Hauptvorschriften zur Netzneutralität, die durch detaillierte Transparenzanforderungen nach Artikel 4 der TSM-VO unterstützt werden. Diese Anforderungen zielen darauf ab, Regelungen für Internetzugangsdienste zu treffen und Endnutzer*innen fundierte Entscheidungen zu ermöglichen. Die TKK überwacht die Einhaltung dieser Transparenzvorschriften im Rahmen der Überprüfung der Allgemeinen Geschäftsbedingungen [RT24c].

Zusammenhang Netzneutralität und Netzsperren

Die Netzneutralitäts-Verordnung schützt das Prinzip, dass Internet Service Provider den Zugang zu Online-Inhalten nicht blockieren dürfen. Es gibt jedoch gewisse Ausnahmen, die unter spezifischen Bedingungen erlaubt sind, beispielsweise wenn gesetzliche Vorgaben eine Sperre erforderlich machen. Dies trifft etwa auf das Urheberrecht zu, das Internet Service Provider unter Umständen verpflichten kann, Zugänge zu Webseiten, die wiederholt gegen Urheberrechte verstoßen, zu sperren. Die Regulierungsbehörden befassen sich intensiv mit dem Thema der Netzsperren, da solche Maßnahmen die grundlegende Idee der Netzneutralität berühren, die Freiheit der Meinungsäußerung im Internet einschränken und die Internet Service Provider in eine problematische Position bringen können. Das Ziel besteht darin, Ansätze und Lösungen zu finden, die allen beteiligten Parteien maximalen rechtlichen Schutz und Sicherheit gewährleisten. Zu diesem Zweck werden gesetzgeberische Entwicklungen auf nationaler und europäischer Ebene sorgfältig beobachtet und aktiv zur Entwicklung und Umsetzung europäischer Richtlinien in nationales Recht beigetragen [RT24c].

Die RTR gibt an, dass die Gewährleistung an Transparenz im Bereich der Netzsperren sehr bedeutsam für die RTR ist. Deshalb gibt es eine öffentlich zugängliche Liste aller gesperrten Webseiten in Österreich, die von der RTR auch als Open Data zur Verfügung gestellt werden. Die Liste aller aktiven Netzsperren kann abgerufen werden unter: `https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_blockings.de.html` (abgerufen am 30.03.2024). Open Data zu Netzsperren sind zu finden unter `https://www.data.gv.at/katalog/de/dataset/netzsperren` (abgerufen am 30.03.2024).

Basierend auf unterschiedlichen rechtlichen Grundlagen werden RTR und TKK bei Netzsperren tätig. Unter dem Link `https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_procedures.de.html`, abgerufen am 30.03.2024, findet man einen Überblick über aktuell aufrechte Netzsperren, sowie die Verfahren, Entscheidungen und Rechtsmaterien, die diesen Sperren zugrunde liegen,

2.1.7. Internetfreiheit

Die Freiheit des Internets schließt die Beachtung der grundlegenden Menschenrechte ein, wobei vor allem die Freiheit der Meinungsäußerung, der Presse und der Information im Vordergrund steht. Artikel 19 der Allgemeinen Erklärung der Menschenrechte, der seit seinem Erlass im Jahr 1948 unverändert geblieben ist, erscheint heute relevanter denn je, als hätten die Verfasser*innen die Existenz des Internets vorausgeahnt [Me48]:

> Jeder hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung, dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten.

Der "Freedom On The Net 2023" Bericht von Freedom House dokumentiert den Zustand der Internetfreiheit weltweit und analysiert die Menschenrechte in der digitalen Welt in 70 Ländern. Der Bericht, der Ergebnisse von Juni 2022 bis Mai 2023 umfasst, hebt die zunehmende digitale Repression, Angriffe auf die freie Meinungsäußerung und Bedrohungen hervor. Die Entwicklung von generativer künstlicher Intelligenz (KI) verstärkt die Gefahr der Verbreitung von Desinformationskampagnen im Internet. KI-Tools sind in der Lage, Texte, Audio und Bilder zu generieren und machen solche Kampagnen ausgefeilter, zugänglicher und leichter durchführbar. Bereits mehr als 47 Regierungen weltweit nutzen Online-Kommentatoren, um Diskussionen zu ihren Gunsten zu manipulieren. Die Technologie eröffnet neue Wege, um diese Bemühungen zu intensivieren. Regierungen setzen KI ein, um ihre Fähigkeiten zur Online-Zensur zu verbessern. Die technologisch fortgeschrittensten autoritären Staaten passen sich schnell an KI-Chatbot-Technologien an, um ihre Zensursysteme zu stärken. In mindestens 21 Ländern existieren gesetzliche Vorgaben, die digitale Plattformen dazu anhalten oder verpflichten, maschinelles Lernen zu nutzen, um unerwünschte Inhalte zu filtern. Dies verdeutlicht, wie fortschrittliche Technologie eine Herausforderung für die Freiheit im Internet darstellt und die Notwendigkeit aufzeigt, sich mit den Auswirkungen dieser Entwicklungen auseinanderzusetzen [Ho23].

In Österreich gibt es Fälle, in denen sich bestimmte Rechte, wie das Recht auf geistiges Eigentum, gegenüber dem Recht auf freie Meinungsäußerung durchsetzen. Demnach sind in Österreich Netzsperren zulässig, um das Recht auf Eigentum zu wahren. Die rechtlichen Grundlagen werden im folgenden Abschnitt 2.2 behandelt.

2.2. Rechtlicher Rahmen für Netzsperren in Österreich

Der Fokus der Arbeit konzentriert sich auf technischen Aspekt, in diesem Abschnitt wird jedoch auch auf die rechtlichen Rahmenbedingungen von Netzsperren in Österreich eingegangen. Internet Service Provider dürfen im Allgemeinen keine spezifischen Inhalte, Applikationen, Dienstleistungen oder Kategorien blockieren, drosseln, modifizieren, einschränken, unterbrechen, herabsetzen oder diskriminieren. Es gibt jedoch Ausnahmen

von dieser Regel gemäß der Netzneutralitäts-Verordnung [EU15]. Diese Eingriffe dürfen vorgenommen werden, wenn sie notwendig sind, um den Anforderungen von EU-Gesetzen oder nationalen Rechtsnormen und den damit verbundenen Durchführungsbestimmungen zu entsprechen [RT24b].

2.2.1. Rechtsgrundlage Urheberrechtsgesetz

Gemäß § 81 Abs. 1a des Urheberrechtsgesetzes (UrhG) können Internetzugangsanbieter unter bestimmten Bedingungen dazu verpflichtet werden, den Zugang zu Webseiten zu unterbinden, die systematisch Urheberrechtsverletzungen begehen. Eine solche Verpflichtung tritt in Kraft, wenn der Anbieter formell von einem Rechteinhaber darauf hingewiesen wurde. Von systematischen Rechtsverletzungen spricht man, wenn eine Website wiederholt und gezielt gegen das Urheberrecht verstößt, zum Beispiel durch das Bereitstellen von Links zu illegal kopierten Inhalten über BitTorrent. Obwohl üblicherweise gerichtliche Instanzen über urheberrechtliche Ansprüche entscheiden, liegt es in der Zuständigkeit der Regulierungsbehörden zu prüfen, ob die von den Internetzugangsanbietern eingeführten Zugangssperren als Reaktion auf eine Abmahnung mit den Bestimmungen der Verordnung über Maßnahmen zur Zugangserschwerung (TSM-VO) vereinbar sind. Wenn solche Maßnahmen ohne gerichtliches Urteil ergriffen werden, muss geprüft werden, ob sie unter die Ausnahmen gemäß Artikel 3 Absatz 3 Unterabsatz 3 Buchstabe a) der TSM-VO fallen [EU15; Ös24a; RT24b].

2.2.2. Rechtsgrundlage Verbraucherbehördenkooperationsgesetz

Das Verbraucherbehördenkooperationsgesetz (VBKG), welches die Verordnung (EU) 2017/2394, auch bekannt als Verbraucherbehörden-Kooperationsverordnung (CBC-VO [EU19]), in nationales Recht umsetzt, legt fest, dass zur Unterstützung der grenzüberschreitenden Durchsetzung von Verbraucherrechten verschiedene Maßnahmen ergriffen werden können. Diese Maßnahmen, einschließlich Sperren, Entfernen oder Einschränken bestimmter Inhalte, kommen zum Einsatz, wenn keine anderen effektiven Mittel verfügbar sind, um das Risiko ernsthafter Beeinträchtigungen der kollektiven Interessen der Verbraucher*innen abzuwenden [Ös24b; RT24b].

2.2.3. Rechtsgrundlage EU-Marktüberwachungsverordnung

Die Marktüberwachungsverordnung [EU19] der Europäischen Union dient als rechtlicher Rahmen, um auf sich wandelnde wirtschaftliche Gegebenheiten und Herausforderungen zu reagieren. Insbesondere im Bereich des internationalen Onlinehandels und der Logistikdienstleistungen soll sie effektiv sein. Ein zentraler Aspekt dieser Verordnung ist die Schließung von Lücken, die es bisher ermöglichten, Waren aus Drittländern, die nicht den EU-Normen entsprechen, über Online-Plattformen in den EU-Binnenmarkt einzuführen, ohne dass ein in der EU ansässiger wirtschaftlich Verantwortlicher greifbar ist. Ähnlich wie in der Verordnung über die Zusammenarbeit der Verbraucherschutzbehörden werden auch

Online-Intermediäre, zu denen Anbieter von Internetzugangsdiensten, Hosting-, Caching-Anbieter und Suchmaschinenbetreiber zählen, in die Pflicht genommen, um rechtswidrige Aktivitäten im Internet zu unterbinden. In Österreich liegt die Zuständigkeit für die Durchsetzung der von Online-Intermediären zu treffenden Maßnahmen bei der Telekom-Control-Kommission (TKK) [RT23b, S. 25].

2.2.4. Rechtsgrundlage EU-Sanktionsverordnung

Im März 2022 führte die EU durch die Sanktionsverordnung [EU22] neue Verpflichtungen zur Sperrung von Inhalten für Internet Service Providern ein, um die Verbreitung von Materialien ausgewählter staatsnaher russischer Medien innerhalb der EU zu verhindern. Diese Verpflichtungen wurden seitdem mehrfach erweitert. Die österreichischen Regulierungsbehörden für Netzneutralität vertreten die Auffassung, dass für die Umsetzung der EU-Sanktionsverordnung kein nationaler Verwaltungsakt erforderlich ist, da sie als EU-Verordnung direkt in Österreich gilt und sich unmittelbar an die Anbieter von Internetzugangsdiensten richtet. Diese Interpretation wird auch von BEREC, dem Gremium europäischer Regulierungsstellen, geteilt [BE22]. Darüber hinaus wurde am 13. April 2022 durch eine Änderung des AMD-G (Audiovisuelles Mediendienste-Gesetz [Ös22]) die Kommunikationsbehörde Austria (KommAustria) als zuständige Behörde für die Überwachung und Bestrafung von Verstößen durch ISPs im Kontext der EU-Sanktionsverordnung benannt. KommAustria bietet auf ihrer Website eine detaillierte Liste der aktuell zu sperrenden Inhalte [RT23a]. Maßnahmen von Internet Service Providern, die in Übereinstimmung mit dieser Anleitung ergriffen werden, stehen in der Regel nicht im Widerspruch zu den gesetzlichen Anforderungen zur Wahrung der Netzneutralität [RT23b].

2.3. Technische Implementierung von Netzsperren in Österreich

Internet-Zensoren verwenden eine Vielzahl technischer Mittel, um den Zugang zu Internet-Ressourcen zu verhindern. Eine grobe und einfache Methode ist die Abschaltung des Internets. Feldstein definiert die Abschaltung des Internets als *activities undertaken by states to intentionally restrict, constrain, or disrupt Internet or electronic communications within a given geographic area or affecting a specific population in order to exert control over the spread of information, within a timebound period* [Fe21]. Abschaltungen können durch physische Trennung von Kabelverbindungen, logische Segmentierung des Netzwerkverkehrs oder Manipulation von Routing-Tabellen erreicht werden, um sicherzustellen, dass der Verkehr sein Ziel nicht erreicht. Zensoren setzen auch Bandbreitendrosselung ein, um den Zugang zu bestimmten Plattformen oder Medienquellen [An13; Xu21] für einen bestimmten Zeitraum einzuschränken, manchmal während Wahlen oder bei zivilen Unruhen. Die

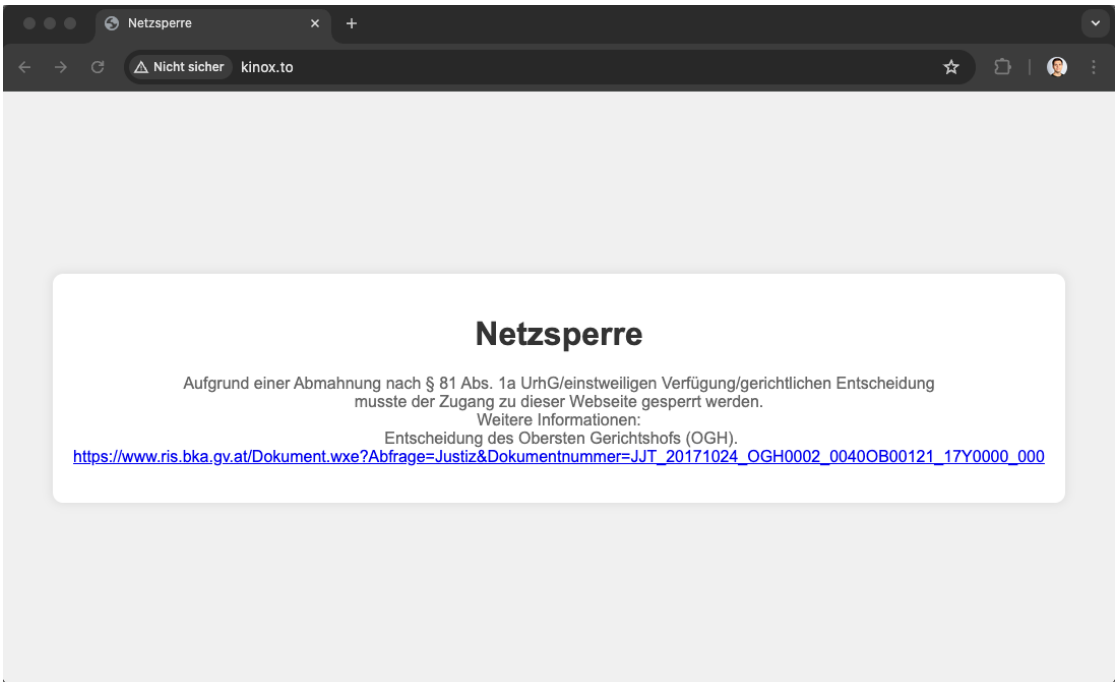
Drosselung kann durch die Einführung künstlicher Latenzzeiten, die Änderung von Routing-Pfaden, Traffic Shaping, Traffic Policing oder die Anwendung von Quality of Service (QoS)-Algorithmen auf unerwünschten Traffic erfolgen [Mü20].

Zensoren erstellen Verzeichnisse von IP-Adressen, die Server identifizieren, deren Datenaustausch sie unterbinden möchten. Sie verwenden auch das Blockieren von Ports, oft gegen Transmission Control Protocol (TCP), User Datagram Protocol (UDP) oder QUIC Transport Layer Protocols, um Netzwerkpakete zu blockieren. Da ein Großteil des heutigen Internetverkehrs webbasiert ist, konzentrieren sich viele Zensurmethoden auf webbasierte Protokolle: Hypertext Transfer Protocol (HTTP), Domain Name System (DNS) und Transport Layer Security (TLS). Wenn Nutzer*innen eine Website anfordern, kann ein Zensor die DNS-Anforderung manipulieren, um eine Website zu blockieren. Mit Web-Proxies und URL-Filtersoftware können Zensoren auch Listen von Webseiten von der Verbindung ausschließen, indem sie einen HTTP-Fehlercode an den Webbrowser senden oder die Verbindung mit einem TCP-Reset beenden [MG21, S. 2].

Wenn ein Zensor über Deep Packet Inspection (DPI)-Fähigkeiten verfügt, kann er die Payload von IP-Paketen überwachen. DPI ermöglicht das Filtern von HTTP, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) und anderem Verkehr auf der Grundlage von Keywords im Inhalt der Kommunikation [BM11]. Wenn Benutzer*innen Webseiten anfordern, die durch TLS geschützt sind, wird der Verkehr verschlüsselt, sodass ein Sniffer den Inhalt nicht lesen kann. Zensoren können jedoch die Plaintext Server Name Indication (SNI)-Erweiterung eines TLS-Headers lesen und auf dieser Grundlage eine Zielwebsite blockieren. Fortgeschrittene Zensoren schließlich verwenden Protokoll-Fingerprinting-Techniken, um bestimmte Protokolle, Anwendungen oder andere verschlüsselte Pakete anhand von Verkehrsmustern zu identifizieren und dann den entsprechenden Verkehr zu blockieren [SNB16].

In Österreich setzen Internet Service Provider DNS-Sperren und IP-Sperren ein, um Netzsperren umzusetzen. Dies ist in den Open Data zu Netzsperren ersichtlich, welche unter `https://www.data.gv.at/katalog/de/dataset/netzsperren` verfügbar sind (abgerufen am 13.04.2024). Weiters werden auf der Website der RTR [RT24a] werden alle aktiven Netzsperren angeführt. Folglich fokussiert sich dieser Abschnitt auf DNS-Sperre und IP-Sperre.

Wie eine Netzsperre in der Praxis für Nutzer*innen aussehen kann, ist auf Abbildung 2.7 zu sehen. In der Adresszeile ist die Domain `kinox.to` zu sehen, anstelle der Website jedoch eine Mitteilung zur Netzsperre. Diese informiert Nutzer*innen darüber, dass der Zugang zu dieser Website aufgrund einer Abmahnung nach § 81 Abs. 1a UrhG und einer einstweiligen Verfügung oder einer gerichtlichen Entscheidung gesperrt wurde. Es wird auf eine Entscheidung des Obersten Gerichtshofes (OGH) verwiesen und ein Link zum Rechtsinformationssystem der Republik Österreich (RIS) angegeben, wo weitere Informationen zu finden sind. Der gesamte Bildschirm wirkt nüchtern und offiziell, um die Ernsthaftigkeit der rechtlichen Maßnahmen zu unterstreichen.



Abbildungsverzeichnis 2.7.: Beispiel einer Netzsperre aus Sicht der Nutzer*innen.

2.3.1. DNS-Sperre

Domainnamen dienen dazu, Internetressourcen wie Webseiten oder Dienste zu identifizieren. Wenn Nutzer*innen eine spezifische Website aufrufen möchte und deren Adresse in die Browserzeile eingeben, wird diese Adresse durch das Domain Name System (DNS) in die zugehörige numerische IP-Adresse umgewandelt. Um den Zugriff auf eine bestimmte Website zu sperren, kann ein Internet Service Provider Änderungen in den von ihm verwalteten DNS-Verzeichnissen vornehmen, indem er die DNS-Anfragen bearbeitet. Dadurch wird verhindert, dass Nutzer*innen auf die angeforderte Website zugreifen können. Eine solche Blockierung hat zur Folge, dass sämtliche Webseiten einer Domain, unabhängig von ihrer Legitimität, über deren Domainnamen nicht mehr erreichbar sind. Auch der E-Mail-Verkehr kann beeinträchtigt werden und alle Subdomains betroffen sein [IS24b]. Es gibt mehrere Möglichkeiten, die DNS-Funktionalität zu verändern. Eine Möglichkeit besteht darin, die Existenz der unerwünschten Domain mit dem Eintrag `NXDOMAIN` zu verneinen. In diesem Fall erhalten die Nutzerinnen die Fehlermeldung `Host not found`. Eine andere Methode ist das sogenannte `DNS-Spoofing`. Hierbei werden verfälschte Informationen zurückgesendet, die die Nutzerinnen zu einer völlig anderen Website als der gewünschten führen können. Ansonsten kann der DNS-Server des Internet Service Providers die Antwort auch einfach verweigern. Dies kann wiederum zum Fehler `Host not found` führen [Do04b, S. 8-9].

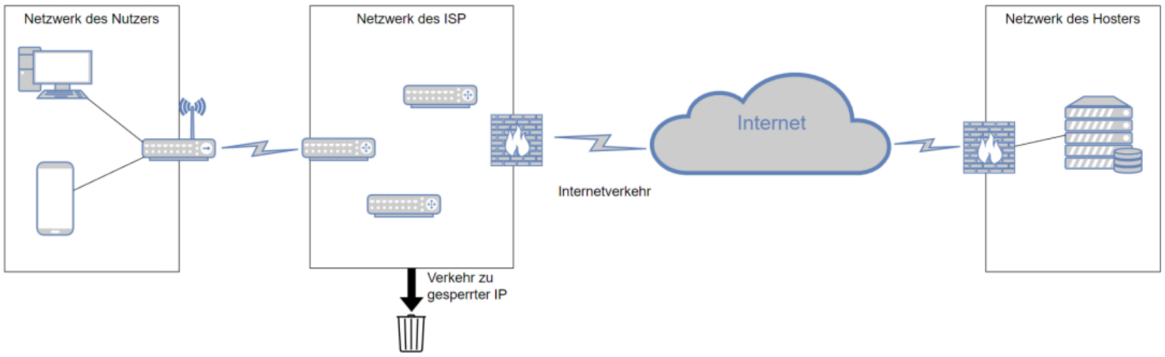
2.3.2. IP-Sperre

Technisch werden IP-Sperren realisiert, indem IP-Pakete, die an die zu sperrende Ziel-IP-Adresse adressiert sind, von Internet Service Providern (ISP) nicht weitergeleitet, sondern verworfen werden. Grafisch ist die Position einer Sperre in Abbildung 2.8 dargestellt. Folglich ist keine Kommunikation mit der gesperrten Ziel-IP-Adresse möglich. Für Endnutzer*innen des sperrenden Anbieters resultiert dies in der Nichterreichbarkeit der betreffenden IP-Adresse. Diese Sperre beeinflusst ausschließlich Nutzer*innen des sperrenden Anbieters und bleibt für Nutzer*innen anderer Anbieter sowie für den Inhaber der gesperrten IP-Adresse in der Regel unbemerkt. Letzterer kann die Sperre nur indirekt identifizieren, nämlich durch das Ausbleiben von Verbindungen mit Quell-IP-Adressen, die dem sperrenden ISP zugehörig sind. Eine IP-Sperre bezieht sich ausschließlich auf eine spezifische IP-Adresse und ist nicht auf eine bestimmte Domain oder einen spezifischen Dienst beschränkt. Dies bedeutet, dass alle Dienste, die unter dieser IP-Adresse erreichbar sind, blockiert werden. Dies umfasst neben Webseiten auch andere Services wie VoIP-Server oder E-Mail-Dienste. Die Umsetzung einer IP-Sperre erfordert, dass der ISP jede zu blockierende Adresse in die Filter seiner Border-Router einträgt. Die Router unterbinden dann die Weiterleitung der entsprechenden IP-Pakete. Die Anwendung von IP-Sperren kann jedoch erhebliche Nebenwirkungen haben. Aufgrund der Tatsache, dass viele Webhosting-Anbieter mehrere Webseiten auf einer einzigen IP-Adresse hosten, kann das Blockieren einer solchen Adresse dazu führen, dass zahlreiche legitime Webseiten nicht mehr zugänglich sind. Eine solche Maßnahme kann vorübergehend oder dauerhaft sein und erhebliche finanzielle Einbußen für die Betreiber dieser Webseiten nach sich ziehen. Die Sperre verhindert den Zugang zu potenziell legitimen Inhalten und beeinträchtigt somit die Rechte der Betreiber. IP-Sperren sind eine kostengünstige und technisch einfach umzusetzende Methode zur Beschränkung des Netzwerkzugangs darstellen. Allerdings ist die Anzahl der Regeln, die ein Router verarbeiten kann, begrenzt, was die Skalierbarkeit von IP-Sperren einschränkt. Angesichts dieser Einschränkungen müssen ISPs die Anwendung von IP-Sperren sorgfältig abwägen, um unbeabsichtigte Auswirkungen zu minimieren und die Zugänglichkeit des Internets nicht übermäßig zu beschränken ([Ts17, S. 34], [Sc23, S. 7], [Do04b, S. 3])

2.3.3. Überschüssige Netzsperren - Overblocking

Sowohl das Blockieren von Domain-Namen (DNS-Sperre) als auch das Blockieren von IP-Adressen (IP-Sperre) kann zu Overblocking führen. Overblocking ist ein Zustand, bei dem auch legale Webseiten fälschlicherweise gesperrt werden. Dies verhindert, dass Nutzer*innen auf diese Seiten zugreifen können und verursacht zusätzliche Kosten für die Internet Service Provider durch Beschwerden. Außerdem kann es den Ruf der Internet Service Provider schädigen. Bei einer IP-Sperre kann es laut einem technischen Gutachten [Sc23, S. 9] für die Telekom-Control-Kommision immer zu einem Overblocking kommen:

> Bei der Umsetzung einer IP-Sperre durch einen Internet Service Provider kann es aus technischer Sicht immer zu einem Overblocking kommen, da eine vollständige Ermittlung aller von einer Sperre umfassten Inhalte für einen Internet Service Provider technisch nicht möglich ist.



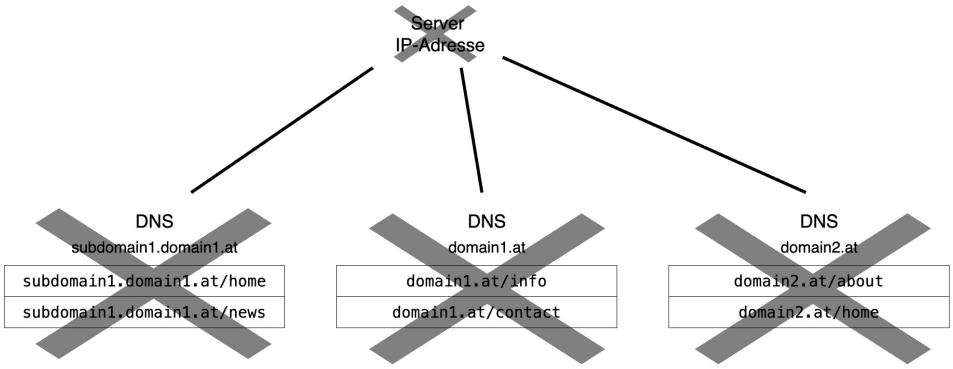
Abbildungsverzeichnis 2.8.: Grafische Darstellung IP-Sperre. Eine IP-Sperre wird innerhalb des Netzwerksegments des ISP implementiert, also bevor der Datenverkehr an das öffentliche Internet weitergeleitet wird. Quelle: [Sc23, S. 6]

Dabei gilt es zu beachten [Sc23, S. 8]:

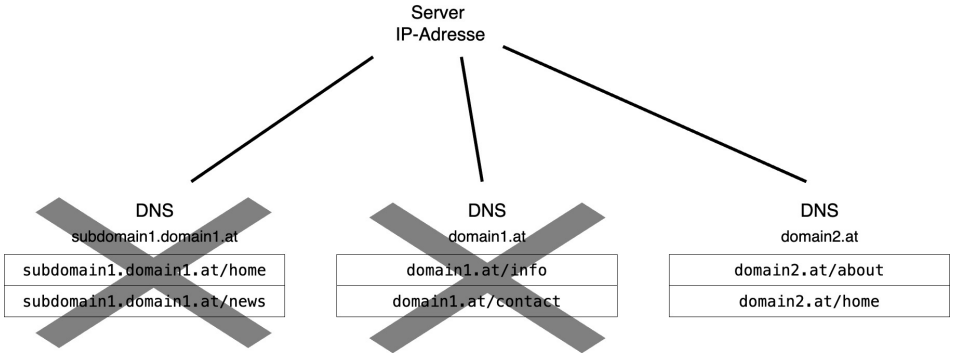
> Es ist für einen Internet Service Provider technisch nicht möglich, proaktiv abschließend und umfassend zu erkennen, ob im Fall einer konkreten IP-Sperre auch andere Dienste mit umfasst sind.

Begründet wird dies dadurch, dass es aufgrund der Ausgestaltung von HTTP und DNS nicht möglich ist, alle Inhalte, die unter einer IP-Adresse abrufbar sind, aufzulisten. Es ist weder möglich, alle Inhalte abzurufen, die hinter einer Domain hinterlegt sind, noch ist es möglich, alle Domains abzufragen, die einer IP-Adresse zugeordnet sind. Diese Möglichkeit besteht weder für Endnutzer*innen noch für Internet Service Provider oder andere Dritte. Ausschließlich der Serveradministrator hat die Kontrolle und Übersicht über alle angebotenen Inhalte und Dienste [Sc23, S. 8]. Bekräftigt wird dies dadurch, dass seit 1999 das Hypertext Transfer Protocol (HTTP) es Servern ermöglicht, angeforderte Domains zu unterscheiden. Diese Funktionalität ist in der IETF RFC 2616 unter Abschnitt 14.23 definiert *The Host field value MUST represent the naming authority of the origin server or gateway given by the original URL. This allows the origin server or gateway to differentiate between internally-ambiguous URLs, such as the root "/" URL of a server for multiple host names on a single IP address.* Die gängigen Webserver wie Apache und nginx nutzen die Möglichkeit, unterschiedliche Domains über ein einzelnes Server-System zu verwalten, indem sie sogenannte `Virtual Hosts` [Fo24] bzw. `Server Blocks` [ng24] einsetzen. Dies ermöglicht es einem Server, unter einer einzigen IP-Adresse eine praktisch unbegrenzte Anzahl von verschiedenen Domains zu bedienen. Diese Domains müssen nicht zwangsläufig miteinander in Verbindung stehen. Es gibt keine technischen Einschränkungen bezüglich der Art der Domains, die durch denselben Server oder dieselbe IP-Adresse bedient werden können [Sc23, S. 7].

Eine DNS-Sperre hingegen führt zur Sperrung einer gesamten Domain auf DNS-Ebene. Wenn illegale Inhalte innerhalb einer Subdomain gehostet werden, können auch alle anderen Subdomains derselben Hauptdomain blockiert werden. Dies kann insbesondere



Abbildungsverzeichnis 2.9.: Darstellung der nicht mehr erreichbaren Server und Inhalte bei einer IP-Sperre. Die Kreuze zeigen, dass im Falle der IP-Sperre alle Server und Inhalte nicht mehr erreichbar sind. Quelle: Basierend auf [Th20, S. 9],



Abbildungsverzeichnis 2.10.: Darstellung der nicht mehr erreichbaren Server und Inhalte bei einer DNS-Sperre. Die Kreuze zeigen, dass in diesem Falle der DNS-Sperre nur bestimmte Server und Inhalte nicht mehr erreichbar sind. Quelle: Basierend auf [Th20, S. 10]

dann problematisch sein, wenn dadurch benutzergenerierte Inhalte auf großen sozialen Netzwerken oder Mediendiensten betroffen sind. Ein Beispiel hierfür ist, wenn die Blockade eines spezifischen illegalen Inhalts auf einer Social-Media-Plattform zur Sperrung der gesamten Plattform für die Kund*innen eines Internet Service Providers führt. Diese Praktiken werfen Fragen nach der Verhältnismäßigkeit der Eingriffe im Vergleich zu weniger einschneidenden Alternativen auf. Außerdem besteht das Risiko des geografischen Overblocking für Anbieter mit europaweit operierenden Netzwerken. Je nach Standort des Servers kann ein Provider unbeabsichtigt Inhalte in anderen Ländern blockieren, was die Komplexität dieser Thematik noch erhöht [IS24b]. Abbildung 2.9 stellt das Verhalten einer IP-Sperre vereinfacht grafisch dar und Abbildung 2.10 bildet das Verhalten der DNS-Sperre vereinfacht ab.

2.3.4. Überschüssige Netzsperren 2022 in Österreich

Im August 2022 kam es zur unerwarteten Nichtverfügbarkeit vieler Webseiten. Die Ursache hierfür war die Sperre einiger IP-Adressen aufgrund einer Unterlassungsaufforderung seitens Vertreter:innen aus der Musik- und Filmindustrie. Die Konsequenzen dieser IP-Sperre verdeutlichten die Risiken, vor denen Expert*innen aus der Internetwirtschaft gewarnt hatten [IS23a]. Die Verwertungsgesellschaft LSG hat bei einem Gericht die Sperrung von IP-Adressen der Firma Cloudflare durchgesetzt und österreichische Internet Service Provider haben diese umgesetzt. Cloudflare ist ein Unternehmen, dessen Dienste von vielen Betreibern großer Webseiten genutzt werden, um ihre Online-Präsenzen zu schützen. Die IP-Adressen von Cloudflare werden dabei nicht exklusiv einer einzelnen Website zugeordnet, sondern von einer Vielzahl von Angeboten gemeinsam genutzt. Wenn eine der von Cloudflare verwendeten IP-Adressen blockiert wird, können potenziell Dutzende von anderen, nicht zielgerichteten Webseiten beeinträchtigt werden. Betroffen von der Netzsperre waren unter anderem unbeteiligte Online-Shops, ein Sachverständiger und die Menschenrechtsorganisation SOS Mitmensch [Re22b]. Die IP-Sperren wurden nach wenigen Tagen wieder aufgehoben [TK23].

2.3.5. DNS-Sperren im Sinne der Verhältnismäßigkeit

IP-Sperren können in die Grundrechte Dritter eingreifen, da sie neben den Zielseiten auch andere, unabhängige Dienste beeinträchtigen. Website-Betreiber*innen können Eingriffe in ihre Meinungsfreiheit und wirtschaftlichen Interessen erleiden, wenn ihre Seiten unzugänglich werden. Auch Internetnutzer*innen können durch übermäßige Blockaden betroffen sein, indem auch legale Inhalte versehentlich zensiert werden. Im Gegensatz dazu ermöglichen DNS-Sperren eine gezieltere Einschränkung, da sie sich spezifisch auf einzelne Domains konzentrieren und somit das Risiko von Kollateralschäden minimieren. Obwohl es relativ einfach ist, DNS-Sperren von Diensteanbietern zu umgehen, zum Beispiel durch die Registrierung einer neuen, ähnlichen URL (zum Beispiel kino.to zu `kinox.to`), ist dieser Umstand nicht allein ausschlaggebend. Schließlich können Webseiten-Betreiber*innen eine IP-Sperre umgehen, indem man die IP-Adresse ändert. Obwohl solche Änderungen durch eine kombinierte DNS- und IP-Sperre erschwert werden könnten, ist es dennoch möglich, eine neue URL zu erstellen und die Sperre erneut zu umgehen. Nutzer*innen haben außerdem die Möglichkeit, IP-Sperren durch den Einsatz von Proxys oder VPNs zu umgehen (näheres zur Umgehung von Netzsperren in Abschnitt 2.4). Folglich bieten beide Sperrmethoden keinen absoluten Schutz gegen Umgehungen. DNS-Sperren erscheinen jedoch als das mildere und verhältnismäßigere Mittel im Vergleich zu IP-Sperren, da letztere das zusätzliche Risiko erheblicher Kollateralschäden bergen [Ts17, S. 52-54].

In einer Pressemitteilung [RT23c] vom 10.08.2023 gibt die Regulierungsbehörde Telekom-Control-Kommission (TKK) eine wegweisende Grundsatzentscheidung bekannt. Die TKK gibt bekannt, dass um die Rechte Dritter effektiv zu schützen, sich DNS-basierte Netzsperren als angemessen erweisen und generell ausreichend sind. Eingriffe, die über diese DNS-Sperren hinausgehen und auf der Blockierung spezifischer IP-Adressen basieren, sind nicht notwendig und folglich als rechtlich unzulässig zu bewerten. Diese Praxis soll entscheidend

zur Aufrechterhaltung der Netzneutralität beitragen und deren Bestand für die Zukunft gewährleisten. Dr. Klaus M. Steinmaurer, Geschäftsführer der RTR für den Fachbereich Telekommunikation und Post, in seiner Funktion als Sprecher der TKK erklärt [RT23c]:

> Da unter einer einzigen IP-Adresse unzählige Webseiten abrufbar sein können, ist im Falle einer Sperre das Risiko, auch Webseiten oder Internetdienste unbeteiligter Dritter mit zusperren, ganz besonders hoch. In Österreich wurden Netzsperren bisher überwiegend mit sogenannten ‚DNS-Sperren' umgesetzt. Bei dieser Art der Sperre werden lediglich einzelne Domains blockiert und stattdessen Sperrhinweise angezeigt. Es ist wichtig, dass diese Praxis beibehalten wird, um auch zukünftig die rechtlich gebotene Verhältnismäßigkeit zu wahren.

Der ISPA-Generalsekretär Stefan Ebenberger hat hierzu ebenfalls eine Stellungnahme abgegeben [IS23b]:

> Die Sperre von IP-Adressen ist völlig unverhältnismäßig, denn dabei besteht immer die Gefahr, auch legale Webseiten zu blockieren. Die Rechteinhaber:innen betonen immer den Schutz von geistigem Eigentum. Das ist grundsätzlich richtig und wichtig. Aber was ist mit dem Eigentum an den zu Unrecht gesperrten Webseiten? Es müssen die Rechte aller geschützt werden, nicht nur die einer einzelnen Gruppe.

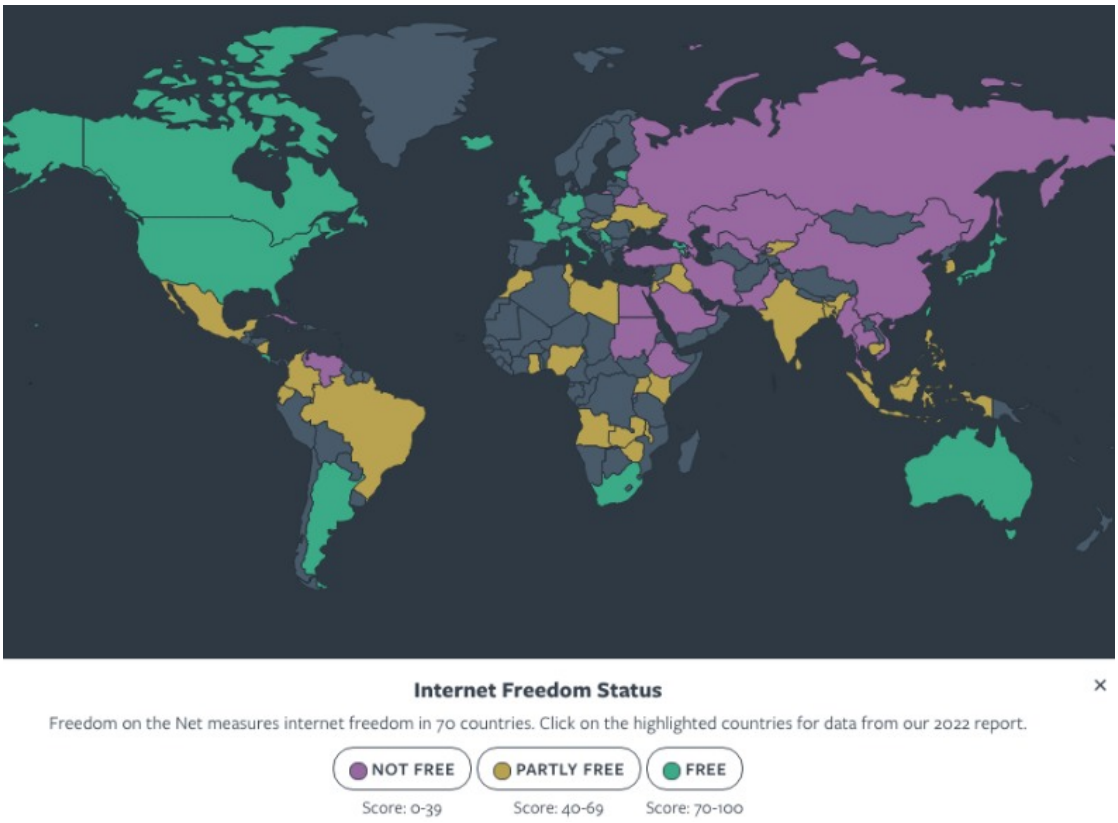
ISPA-Präsident Harald Kapper sagt dazu [IS23b]:

> Endlich wurde berücksichtigt, was der Gesetzgeber ignorierte, nämlich die technischen Realitäten. Das ist wichtig, weil genau hier eine weitere Gefahr schlummert: IP-Sperren bergen immer das Risiko auch legale Inhalte oder Dienste zu sperren und bedrohen damit die Meinungs- und Informationsfreiheit aller Bürger*innen. Hier reden wir über zentrale Grundrechte einer demokratischen Gesellschaft, die im Einzelfall abgewogen werden müssen. Diese Verantwortung darf der Staat nicht länger auf die Internetanbieter, also private Unternehmen, abwälzen.

Die TKK stützt sich bei der Entscheidung auf ein technisches Amtsgutachten [Sc23]. Darin wird bestätigt, dass es technisch nicht möglich ist, bei einer IP-Adresse im Vorhinein zu erkennen, welche anderen Webseiten diese ebenfalls nutzen. Mit dieser Entscheidung möchte die TKK einen fundamentalen Beitrag zum Schutz digitaler Rechte von Internetbenutzer*innen in Österreich leisten. Diese Maßnahme soll laut TKK garantieren, dass das Internet seine Funktion als Treiber für Meinungsfreiheit, ökonomisches Wachstum und Innovation fortsetzen kann [RT23c].

2.3.6. Netzsperren weltweit

Der jährlich von Freedom House in den USA herausgegebene Freedom on the Net Report bewertet die Internetfreiheit auf einer 100-Punkte-Skala als "free", "partly free" oder "not



Abbildungsverzeichnis 2.11.: Karte Internet Freedom Status. Quelle: [MG21, S. 6]

free". Die Methodik umfasst 21 Fragen und rund 100 Unterfragen aus den drei Kategorien "Zugangshindernisse", "Inhaltsbeschränkungen" und "Verletzungen von Nutzerrechten". Die Kategorie "Inhaltsbeschränkungen" bezieht sich speziell auf die technische Filterung von Webseiten. Der Bericht gibt einen Überblick darüber, wo Netzsperren stattfinden und welche Trends von Jahr zu Jahr zu beobachten sind. Abbildung 2.11 zeigt die kartografischen Ergebnisse des Berichts Freedom on the Net 2022 [Ho22]. Auf der abgebildeten Karte ist zu sehen, dass vorwiegend östliche Länder die Bewertung "not free" erhalten haben.

In der Studie "A Worldwide View of Nation-state Internet Censorship" untersuchen Alexander Master und Christina Garman von der Purdue University die staatlichen Internetzensuren weltweit. Basierend auf Daten und früheren Forschungen, analysieren sie Zensurmethoden in 70 Ländern und identifizieren Trends und Techniken, die über zwei Jahrzehnte hinweg eingesetzt wurden. Abbildung 2.12 zeigt das Ergebnis deren Studie. Insgesamt gibt es in 62 der 70 untersuchten Staaten Anzeichen für eine Zensur des Internets, entweder während des Untersuchungszeitraums oder in der historischen Dokumentation. Jeder Staat ist mit einer Bewertung versehen, die den Grad der Internetfreiheit "Not Free", "Partly Free" oder "Free" darstellt. Der Untersuchungszeitraum erstreckt sich vom 1. Juni 2020 bis zum 31. Mai 2021 und bietet einen Überblick über die verschiedenen Techniken, die Staaten weltweit zur Zensur und Kontrolle des Internets einsetzen. In der rechten oberen Ecke des Bildes erklärt eine Legende die Symbole, die in den Zellen der Tabelle verwendet

werden, um das Vorhandensein und die Art der Zensur anzuzeigen [MG21, S. 5-6].

Die Tatsache, dass Österreich in Berichten wie "Freedom on the Net" und der Studie "A Worldwide View of Nation-state Internet Censorship" nicht erwähnt wird, zeigt, dass noch viel Forschungsbedarf besteht. Diese Forschungslücke bietet die Möglichkeit, die Praxis der Netzsperren in Österreich genauer zu untersuchen. Damit trägt diese Masterarbeit dazu bei, unser Verständnis von Internetfreiheit zu erweitern, indem sie die technischen Methoden der Netzsperren in Österreich analysiert.

● = observed, persistent censorship
○ = observed, time-based censorship
▼ = historical censor observations
□ = unconfirmed

COUNTRY	ISO 3166-1 Country Code	FOTN 2021 Total Score	Obstacles to Access	Limits on Content	Violations of User Rights	FOTN 2021 Status	Internet Shutdowns	IP Address or Port Blocking	BGP Attacks and Disruption	Bandwidth Throttling	DNS Tampering	HTTP/URL/Keyword Filtering	TLS-based Filtering	Protocol Fingerprinting	Notes (Study period for ●/○: June 01, 2020 to May 31, 2021)
China	CN	10	8	2	0	Not Free	○	○●		▼	●	●	●	●	Centralized active blocking of VPNs, circumvention tools, and secure messengers
Iran	IR	16	8	5	3	Not Free	○	○●*		▼	●	●	●	●	*Particular endpoints associated with QUIC/UDP targets, and residual censorship
Myanmar (Burma)	MM	17	4	7	6	Not Free	○	●	●	○	●	▼			Military junta coup d'état after 2020 elections
Cuba	CU	21	5	9	7	Not Free	○					●	●	▼	Mass anti-government protests of COVID-19 pandemic response, censored social media
Vietnam	VN	22	12	6	4	Not Free					▼	▼			Censorship focus in print media
Saudi Arabia	SA	24	12	8	4	Not Free		▼			▼	●	●		Reduced overall Internet filtering between 2017-2020
Pakistan	PK	25	5	13	7	Not Free	○	▼	▼*		▼	●	●		*Global YouTube disruption via BGP 24FEB2008
Egypt	EG	26	12	10	4	Not Free	○	●			●	●	●	●	
Ethiopia	ET	27	4	12	11	Not Free	○	▼				●	▼	▼	Tigray civil war
United Arab Emirates	AE	27	12	9	6	Not Free					●	●	●	▼	
Uzbekistan	UZ	28	9	12	7	Not Free	○					●	●		
Venezuela	VE	28	6	12	10	Not Free					▼	●	●		
Bahrain	BH	30	16	8	6	Not Free					▼	●	●		
Russia	RU	30	12	10	8	Not Free	○	●	▼	○	●	●	○●	●	Decentralized, novel hybrid censor approaches observed
Belarus	BY	31	10	14	7	Not Free	○	▼			●	●	●		
Kazakhstan	KZ	33	11	11	11	Not Free	○	○●		▼	▼	●	●	▼	Nation-wide deployment of government-issued root certificate, MITM interception 2019
Sudan	SD	33	6	15	12	Not Free	○					▼			
Turkey	TR	34	15	10	9	Not Free	▼	▼	▼*	▼	●	●	●		*Global Internet disruption via BGP routes to Turkey 24DEC2004
Azerbaijan	AZ	35	10	14	11	Not Free	○	▼				●	●		Second Nagorno-Karabakh war, late 2020
Thailand	TH	36	16	13	7	Not Free					▼	●			High levels of inconsistency in routing, content mismatches
Rwanda	RW	38	13	11	14	Not Free						▼			
Bangladesh	BD	40	12	17	11	Partly Free	○			▼		●	●		
Iraq	IQ	41	11	16	14	Partly Free	○				▼				
Cambodia	KH	43	13	18	12	Partly Free						●	●		
Zimbabwe	ZW	46	8	22	16	Partly Free	▼					▼			
Jordan	JO	47	13	17	17	Partly Free		▼		○*	●	●	●		*Throttling of a social media service during public protests
Indonesia	ID	48	14	17	17	Partly Free					▼	●	●		
Libya	LY	48	7	25	16	Partly Free	▼		▼						
Nicaragua	NI	48	12	18	18	Partly Free						●	●		
India	IN	49	11	21	17	Partly Free	○	▼		○	●	●	●		89 Internet shutdowns during the measurement period
Uganda	UG	49	11	19	19	Partly Free	○	▼				●	□*		2021 elections - shutdowns and social media; *Potential DPI censorship from AS21491
Lebanon	LB	51	11	22	18	Partly Free						□*			*Limited data available
Sri Lanka	LK	51	11	23	17	Partly Free	○								
Kyrgyzstan	KG	53	13	23	17	Partly Free						▼			Inconclusive for evidence of URL filtering during study period
Morocco	MA	53	15	22	16	Partly Free					▼				
The Gambia	GM	53	12	22	19	Partly Free	▼					□			Internet freedom improvement since 2017
Singapore	SG	54	19	17	18	Partly Free					●	□			
Malaysia	MY	58	18	21	19	Partly Free	▼				●	▼			
Malawi	MW	59	11	25	23	Partly Free	□*					□**			*2019 elections; **2011 alleged short-term blocking of news and social media
Nigeria	NG	59	17	25	17	Partly Free	○	▼			▼	▼			
Zambia	ZM	59	15	24	20	Partly Free	▼					▼	▼		2021 elections, social media platform blocking (outside study period)
Mexico	MX	60	18	25	17	Partly Free		▼*				●	●**		*Blocking of Tor directory authorities; **state-owned AS8151 TLS-based filtering
Angola	AO	62	12	30	20	Partly Free							●*		*Blocking of anti-censorship software websites
Ecuador	EC	62	17	25	20	Partly Free						●	●		
Ukraine	UA	62	20	21	21	Partly Free					●	●	●		
Tunisia	TN	63	16	28	19	Partly Free		▼				▼			
Brazil	BR	64	20	24	20	Partly Free					▼	▼			
Ghana	GH	64	14	27	23	Partly Free						●	●		
Colombia	CO	65	19	25	21	Partly Free	□*					▼			*Potential shutdown in parallel with anti-government protests
Philippines	PH	65	17	26	22	Partly Free	▼*					●		▼	*Cellular telephony service shutdowns
Kenya	KE	66	16	27	23	Partly Free									Government orders for removal of content in leu of blocking actions
South Korea	KR	67	22	24	21	Partly Free		▼	▼		▼	●	●		Authorities have publicized their use of TLS-based filtering for illegal content
Hungary	HU	70	21	24	25	Free						□*	□*		*AS60436 potentially performing filtering actions
Argentina	AR	71	19	27	25	Free					▼				
Armenia	AM	71	19	26	26	Free	●					●	●		Second Nagorno-Karabakh war, late 2020
Serbia	RS	71	21	25	25	Free						▼*			*State blocking of gambling websites
South Africa	ZA	73	17	29	27	Free									
Australia	AT	75	23	27	25	Free			▼			□			State blocks gambling, torrent, and streaming sites
United States	US	75	21	29	25	Free									Law Enforcement compels the removal of intellectual property theft rather than blocking
Italy	IT	76	21	30	25	Free					●*				*Mostly blocking alleged criminal activity or copyright infringement
Japan	JP	76	21	29	26	Free									
Georgia	GE	77	19	31	27	Free						□*			*Temporary blocking of "pro-Islamic State" websites 2015
France	FI	78	23	30	25	Free					●	●			State blocking of websites related to "terrorism" and copyright infringement
United Kingdom	GB	78	23	30	25	Free	▼	▼				●	●		IWF maintains court-ordered blocklist ("extreme pornography" and copyright infringement)
Germany	DE	79	22	29	28	Free					▼	▼			Repeal of the Access Impediment Law (Zugangserschwerungsgesetz) 2011
Taiwan	TW	80	24	31	25	Free						□*			*City of Taipei filters select websites on its public wifi
Canada	CA	87	23	32	32	Free		▼	▼		●	●			State blocking of copyright infringement
Costa Rica	CR	87	20	33	34	Free									
Estonia	EE	94	25	32	37	Free					●*				*State blocking of gambling websites
Iceland	IS	96	25	34	37	Free					□*				*State blocking of copyright infringement

Abbildungsverzeichnis 2.12.: Weltweit eingesetzte Techniken für Internetzensur. Quelle: [MG21, S. 6]

2.4. Technologien zur Umgehung von Netzsperren

In diesem Abschnitt werden Technologien zur Umgehung von Netzsperren primär aus Sicht der Internetnutzer*innen vorgestellt. Auf die Umgehung von Netzsperren aus Sicht der Website-Betreiber*innen wird nicht näher eingegangen. Die im Kapitel 4 durchgeführte empirische Untersuchung wird ebenfalls aus Sicht der Nutzer*innen durchgeführt.

Bevor die Techniken zur Umgehung von Netzsperren behandelt werden, wird kurz der Prozess des Aufrufs einer Website am Beispiel der URL `https://www.orf.at/` wiederholt. Dieser Prozess involviert mehrere technische Komponenten und Protokolle, die zusammenwirken, um eine nahtlose Datenübertragung über das Internet zu ermöglichen. Dieses Verständnis ist essentiell, um nachvollziehen zu können, an welchen Stellen des Kommunikationsweges Netzsperren ansetzen können und wie Umgehungstechniken diese Sperren überwinden:

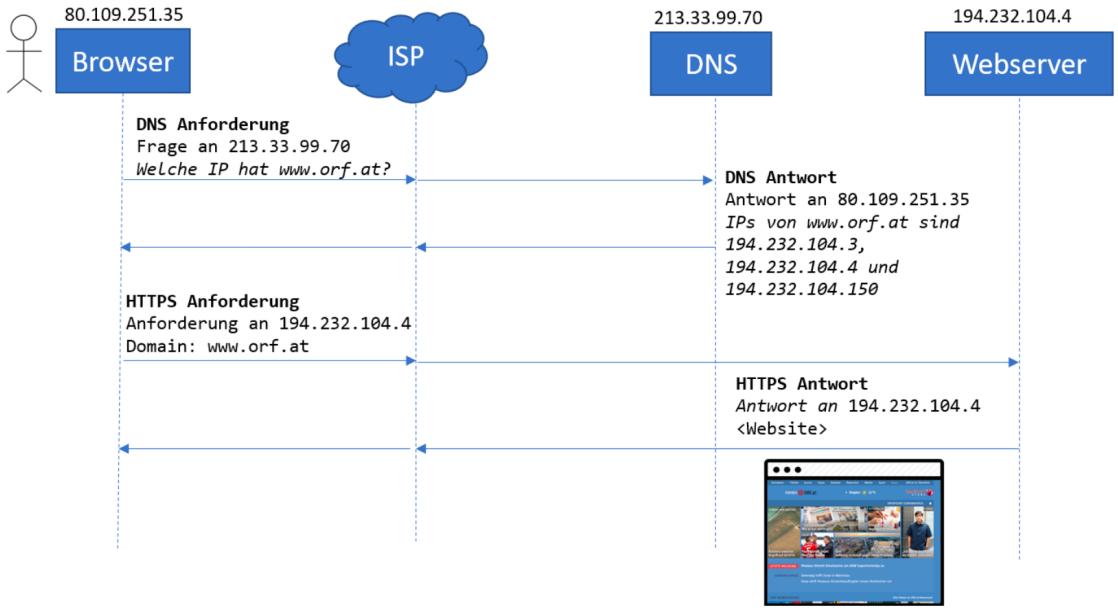
1. **IP-Ebene:** Die Datenübertragung erfolgt über das Internetprotokoll (IP), das den Transport von Datenpaketen steuert. Diese Pakete sind durch die IP-Adressen des Senders und des Empfängers definiert.

2. **Domain Name System (DNS):** Dieses System ist verantwortlich für die Umwandlung von benutzerfreundlichen Domainnamen wie `orf.at` in die technisch erforderlichen IP-Adressen wie `94.232.104.3` (IPv4) und `2a01:468:1000:9::150` (IPv6).

3. **Hypertext Transfer Protocol (HTTP):** Dieses Protokoll wird für die strukturierte Übertragung von Inhalten zwischen Webservern und Clients verwendet.

4. **Web-Technologien:** CSS und JavaScript sind Technologien, die zur Aufbereitung und Darstellung der Inhalte im Webbrowser eingesetzt werden.

Der technische Prozess beginnt üblicherweise damit, dass der Browser der Nutzer*innen eine Anfrage an den DNS-Resolver des Internet Service Providers stellt. Dies geschieht, nachdem der Browser die IP-Adresse des DNS-Resolvers über das Dynamic Host Configuration Protocol (DHCP) erhalten hat, welches je nach Netzwerkkonfiguration die IP-Adresse entweder direkt dem aufrufenden Computer oder einem verwendeten Router zuweist. Der DNS-Resolver antwortet mit einer oder mehreren IP-Adressen für die Domain `www.orf.at`. Anschließend baut der Browser, wie beispielsweise Mozilla Firefox, Google Chrome oder Microsoft Edge, mithilfe des Transmission Control Protocols (TCP) und eines vordefinierten Ports (üblicherweise 443 für verschlüsselte Verbindungen) eine Verbindung zu einer der zurückgegebenen IP-Adressen auf. Falls der DNS-Resolver mehrere IP-Adressen zurückgibt, entscheidet der Browser, welche IP-Adresse für die Verbindung genutzt wird. Mittels der etablierten Verbindung kommuniziert der Browser über das HTTP-Protokoll mit dem Server, um die Ressource `/` (die Startseite) der Domain `www.orf.at` zu erfragen. Sofern die Ressource verfügbar ist, antwortet der Server mit einem im HTTP definierten Statuscode, typischerweise `200 OK` für eine erfolgreiche Anfrage, und sendet den entsprechenden HTML-Code zurück. Dieser Code wird vom Browser verarbeitet, grafisch aufbereitet und Nutzer*innen angezeigt. Dieser gesamte Kommunikationsprozess ist in Abbildung 2.13 visualisiert. Für die initiale Auflösung einer Domain ist ein DNS-Request

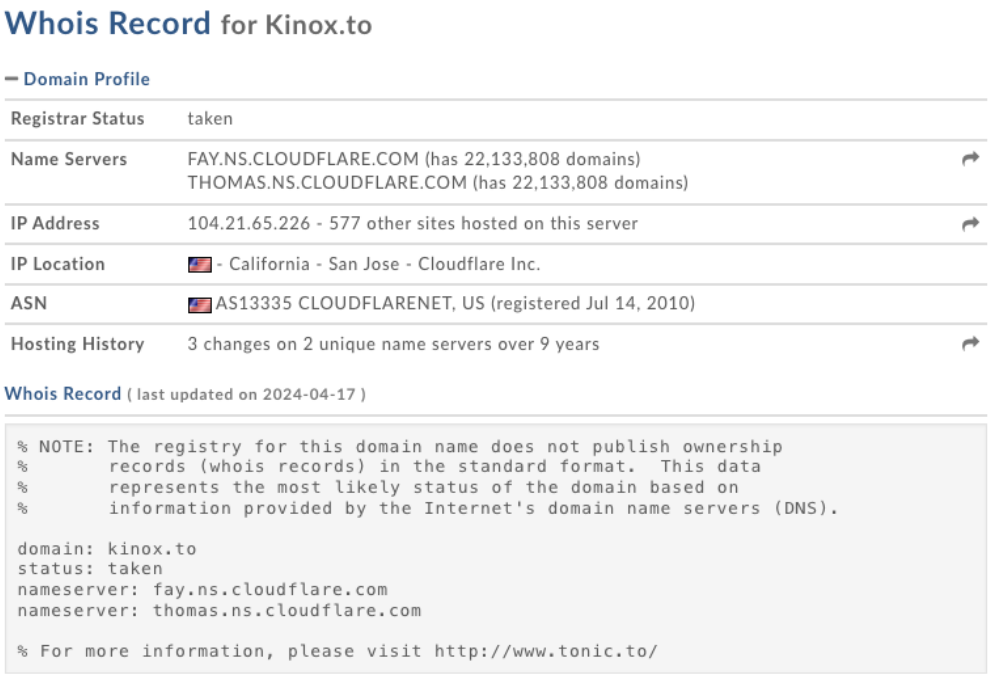


Abbildungsverzeichnis 2.13.: Ablauf beim Aufruf einer Website. Quelle: [Sc23, S. 6]

erforderlich. Bei weiteren Anfragen zu unterschiedlichen Ressourcen derselben Domain, wie beispielsweise `https://www.orf.at/news` und `https://www.orf.at/impressum`, ist in der Regel keine zusätzliche DNS-Abfrage mehr notwendig, da die IP-Adresse bereits aufgelöst und gespeichert wurde. Aus technischer Perspektive ist zu berücksichtigen, dass keine eindeutige Beziehung zwischen einer IP-Adresse, wie zum Beispiel `194.232.104.4`, und einer Domain, wie `orf.at`, bestehen muss. Diese Tatsache resultiert aus der Unabhängigkeit der IP-Adressen und Domains als unterschiedliche Bestandteile des World Wide Web. Es ist nicht zwingend erforderlich, dass einer Domain genau eine IP-Adresse zugeordnet ist. Tatsächlich kann eine Domain, abhängig von der geografischen Region, auf verschiedene Server und IP-Adressen verweisen. Ebenso ist es gängig, dass ein Hostname aus Gründen der Redundanz und Leistungssteigerung auf mehrere IP-Adressen verteilt wird. Im spezifischen Fall der Domain `orf.at` sind beispielsweise acht IPv4-Adressen und acht IPv6-Adressen hinterlegt. Technisch ist es zudem nicht erforderlich, dass ein DNS-Server eine vollständige Liste aller zugehörigen IP-Adressen liefert, noch muss eine IP-Adresse ausschließlich für das Hosting einer einzelnen Domain verwendet werden. Dies wird deutlich, wenn der DNS-Resolver von `orf.at` eine Liste von IP-Adressen zurückgibt, aus der dann der Browser eine spezifische Adresse für den Verbindungsaufbau auswählt [Sc23, S. 5-7].

2.4.1. IP-Adresse verwenden

DNS-Sperren können grundsätzlich durch die Verwendung von IP-Adressen anstelle von Domainnamen in URLs umgangen werden. Allerdings stößt dieser Ansatz an seine Grenzen, wenn es um den Zugriff auf Webseiten geht, die auf Servern mit domainbasiertem virtuellem Hosting liegen, da hierbei die IP-Adresse allein nicht ausreicht, um die spezifische Domain



Whois Record for Kinox.to

— Domain Profile

Registrar Status	taken
Name Servers	FAY.NS.CLOUDFLARE.COM (has 22,133,808 domains) THOMAS.NS.CLOUDFLARE.COM (has 22,133,808 domains)
IP Address	104.21.65.226 - 577 other sites hosted on this server
IP Location	- California - San Jose - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Hosting History	3 changes on 2 unique name servers over 9 years

Whois Record (last updated on 2024-04-17)

```
% NOTE: The registry for this domain name does not publish ownership
%       records (whois records) in the standard format.  This data
%       represents the most likely status of the domain based on
%       information provided by the Internet's domain name servers (DNS).

domain: kinox.to
status: taken
nameserver: fay.ns.cloudflare.com
nameserver: thomas.ns.cloudflare.com

% For more information, please visit http://www.tonic.to/
```

Abbildungsverzeichnis 2.14.: WHOIS-Eintrag für "kinox.to". Quelle: [Do24]

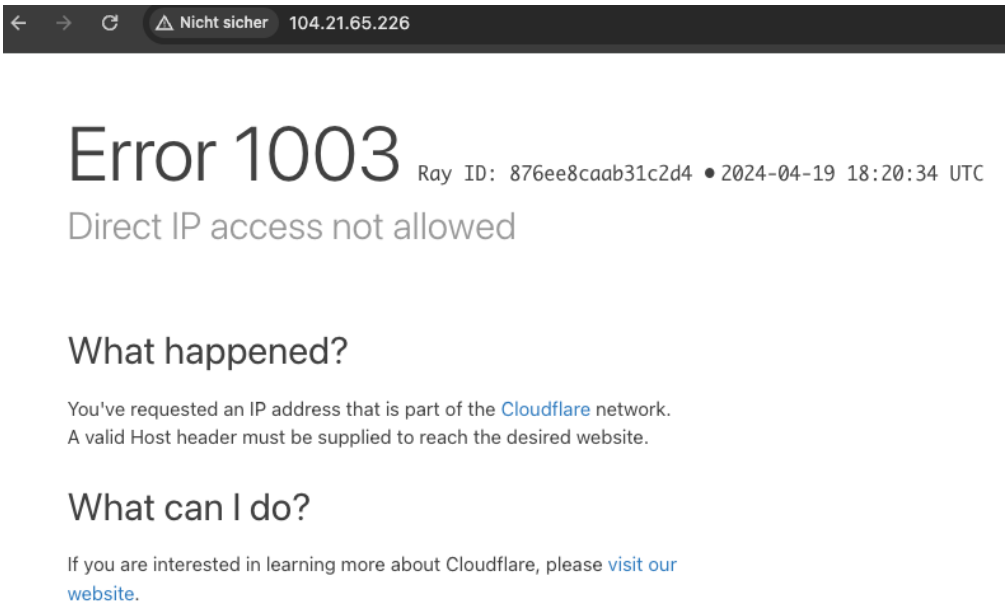
zu identifizieren [Do04a, S. 17].

Das virtuelle Hosts in der Praxis verwendet werden, wurde bereits in Abschnitt 2.3.3 erwähnt. Ein Praxisbeispiel anhand der gesperrten Domain `kinox.to` zeigt, dass diese durch Verwendung der IP-Adresse nicht aufgerufen werden kann. Abbildung 2.14 zeigt einen Ausschnitt aus einem WHOIS-Eintrag für die Domain `kinox.to`. Die IP-Adresse der Domain wird mit `104.21.65.226` angegeben, wobei vermerkt ist, dass 577 andere Webseiten auf diesem Server gehostet werden. In Bezug auf Netzsperren könnte dieser WHOIS-Eintrag dazu dienen, alternative Wege zur Umgehung der Sperre zu identifizieren. Dazu zählt beispielsweise die direkte Verwendung der IP-Adresse, sollte eine DNS-Sperre vorliegen. Allerdings kann wie erwähnt und gezeigt die Effektivität dieser Methode eingeschränkt sein, wenn die Website auf domainbasiertem virtuellem Hosting aufbaut.

Die Abbildung 2.15 präsentiert den `Error 1003` im Webbrowser, der darauf hinweist, dass ein direkter IP-Zugriff nicht gestattet ist. Diese Meldung tritt auf, wenn eine IP-Adresse aus dem Cloudflare-Netzwerk direkt angefordert wird. Damit ist in Bezug auf die Website `kinox.to` ist festzuhalten, dass die IP-Adresse möglicherweise nicht ausreicht, um die Website abzurufen. Eine umfassendere empirische Analyse dazu wurde in Abschnitt 4.4 durchgeführt.

2.4.2. Änderung des DNS-Resolvers

Bei einer DNS-Sperre wird die Auflösung einer zu sperrenden Domain durch den DNS-Resolver des Internet Service Providers auf die IP-Adresse einer Seite mit einem



Abbildungsverzeichnis 2.15.: Beispiel direkter IP-Zugriff nicht erlaubt. Quelle: [cl24a]

Sperrvermerk ausgelöst. Während bei einer DNS-Sperre mit wenig technischer Expertise eine Umgehung der Sperre durch Änderung des DNS-Resolvers auf einen alternativen Resolver möglich ist, hilft diese Maßnahme bei einer IP-Sperre nicht. Der DNS-Resolver kann entweder durch eine Änderung der Einstellungen im Betriebssystem, am CPE-Geräte (Customer Premises Equipment [2]) oder durch eine Änderung der Einstellungen in Browsern wie Mozilla Firefox oder Google Chrome [Sc23, S. 38] geändert werden.

Es können alternative DNS-Resolver wie die von Google (8.8.8.8 und 8.8.4.4) oder Cloudflare (1.1.1.1 und 1.0.0.1) verwendet werden. Da diese öffentlichen Resolver die Anfragen nicht auf gesperrte Seiten umleiten, sondern die Anfrage direkt auf die tatsächliche IP-Adresse der angefragten Domain auflösen, kann auf die Inhalte zugegriffen werden, als ob es keine Sperre gäbe. Nach dem Eintragen der neuen DNS-Adressen werden alle DNS-Anfragen über die neuen Server geleitet, was zu einer Umgehung der DNS-Sperre führen kann [Br24].

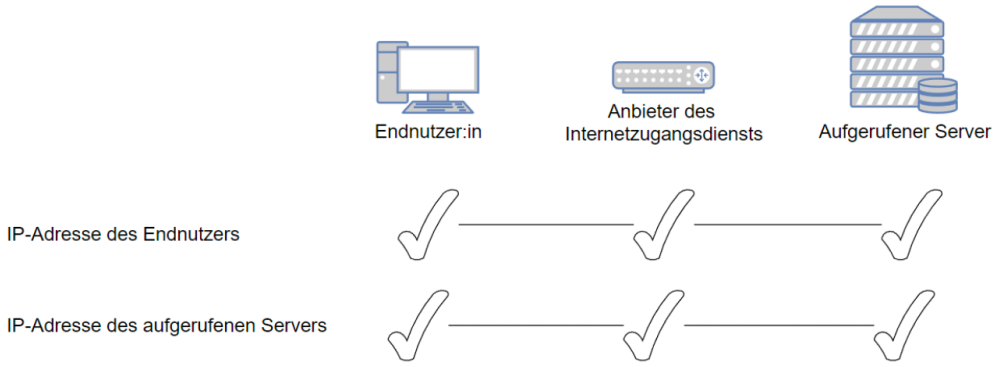
Der technische Ablauf zur Änderung des DNS-Resolvers ist je nach Betriebssystem und Gerät unterschiedlich. In Windows 11 beispielsweise kann der DNS-Resolver wie folgt geändert werden: Zunächst öffnet man die "Einstellungen" und navigiert zu "Netzwerk und Internet". Im nächsten Schritt wählt man die "Eigenschaften" des aktuell verbundenen Netzwerks aus. Unter "IP-Einstellungen" findet man die Option "Bearbeiten", wo man die Wahl hat, entweder automatisch zugewiesene DNS-Adressen zu verwenden oder "Manuell"'eigene DNS-Server-Adressen einzutragen. Nach der Auswahl von "Manuell" können die bevorzugten DNS-Adressen eingegeben werden. Siehe Abbildung 2.16 für eine visuelle Anleitung.

[2] Ein CPE dient dazu, die Endkunden*innen mit den Diensten des Providers zu verbinden und damit den Zugang zum Internet zu ermöglichen [Ko24].

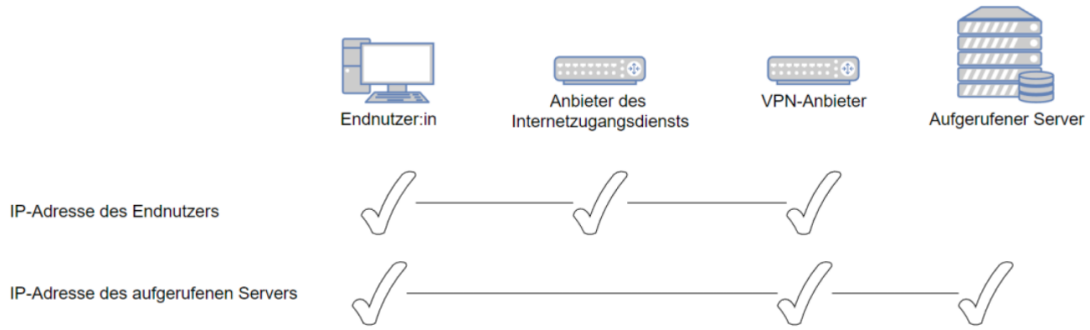
Abbildungsverzeichnis 2.16.: Windows 11 DNS-Einstellungen ändern. Quelle: Windows 11

Abbildungsverzeichnis 2.17.: DNS-Einstellungen direkt am CPE ändern. Quelle: FRITZ!Box

Um einen alternativen DNS-Server für alle Geräte im eigenen Netzwerk zu nutzen, ist es möglich, die DNS-Einstellungen direkt am CPE vorzunehmen. Der spezifische Ablauf hängt dabei vom jeweiligen Modell ab. Bei einer FRITZ!Box beispielsweise erreicht man die Benutzeroberfläche gewöhnlich über die Adresse "http://fritz.box". Nach der Anmeldung gelangt man über das linke Menü zum Bereich "Internet" und von dort weiter zu den "Zugangsdaten". Im Menüpunkt "DNS-Server" können die entsprechenden Einstellungen vorgenommen werden. Dabei ist zu unterscheiden, ob IPv4 oder IPv6 verwendet wird. Bei IPv4 ist die Option "Andere DNSv4-Server verwenden" auszuwählen, bei IPv6 hingegen "Andere DNSv6-Server verwenden". In die vorgesehenen Felder sind die primäre und sekundäre Adresse des gewünschten DNS-Dienstes einzugeben, beispielsweise die von Google oder Cloudflare. Die Eingaben sind durch Betätigen der Schaltfläche "Übernehmen" zu bestätigen. Die Benutzeroberfläche mit Eingabefeld für den DNS-Server ist in Abbildung 2.17 dargestellt.



Abbildungsverzeichnis 2.18.: Aufruf eines Services ohne VPN: Quell- und Ziel-IP-Adresse sind für alle Beteiligten sichtbar. Quelle: [Sc23, S. 39]

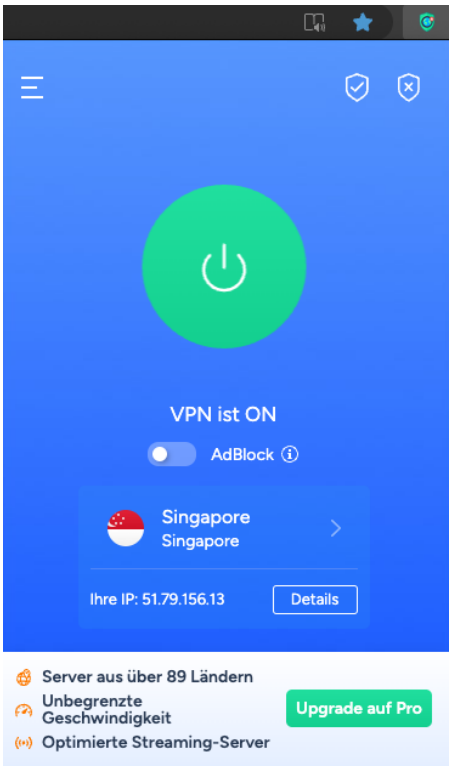


Abbildungsverzeichnis 2.19.: Aufruf eines Services mit VPN: Die Quell-IP-Adresse ist für den aufgerufenen Server nicht sichtbar, die aufgerufene IP-Adresse ist für den ISP nicht sichtbar. Quelle: [Sc23, S. 39]

2.4.3. VPN

Ein Virtual Private Network (VPN) ermöglicht den Zugang zu Netzwerken mittels einer verschlüsselten Verbindung über das Internet. Dies ist besonders nützlich für Unternehmen, die ihren Mitarbeiter*innen von externen Standorten Zugriff auf firmeninterne Ressourcen ermöglichen wollen. Neben der geschäftlichen Nutzung werden VPNs auch privaten Nutzer*innen angeboten. Es gibt viele Anbieter solcher Dienste und die Produkte sind oft zu monatlichen Preisen von unter 5 Euro erhältlich. Bei der Nutzung eines VPN wird der gesamte Internetverkehr des/der Nutzer*in über eine verschlüsselte Verbindung vom Client zum VPN-Anbieter geleitet, bevor er die eigentlichen Zielserver erreicht. Dies verhindert, dass der ISP die Daten kontrollieren oder überwachen kann. Für den ISP ist nur die Verbindung zwischen Endnutzer*in und dem VPN-Anbieter sichtbar. Der Zielserver wiederum sieht nur die IP-Adresse des VPN-Anbieters und nicht die der Nutzer*innen. Diese Vorgänge sind in Abbildung 2.18 und Abbildung 2.19 dargestellt [Sc23, S. 39-40].

Eine vom ISP implementierte IP-Sperre oder DNS-Sperre wird daher bei der Nutzung



Abbildungsverzeichnis 2.20.: Beispiel der Benutzeroberfläche eines VPN-Anbieters am Beispiel "VeePN".

eines VPN unwirksam. Im Gegensatz zu Tor (siehe 2.4.4) gibt es bei der Nutzung von VPNs normalerweise keine Einschränkungen beim Streaming von Videos, da die von VPN-Diensten angebotenen Geschwindigkeiten in der Regel hoch genug sind, um Videostreams flüssig wiederzugeben. Dies ist häufig Teil der Marktstrategie der VPN-Anbieter: Sie weisen darauf hin, dass die Nutzer*innen durch den Zugriff auf VPN-Server in verschiedenen geografischen Regionen in der Lage sind, die geografischen Beschränkungen zu umgehen, die für Video-Streaming-Dienste gelten [Sc23, S. 39-40]. VPN-Dienste sind in der Regel kostenpflichtig, die Preise für streamingfähige Angebote liegen in der Regel zwischen ca. 2,50 Euro und 5 Euro brutto pro Monat [Mi24]. Alternativ zur Nutzung eines kommerziellen VPN-Dienstes kann auch ein eigener VPN-Dienst eingerichtet werden. Dazu wird lediglich ein virtueller Server bei einem Hosting-Anbieter benötigt. Die Kosten sind mit denen eines kommerziellen VPN-Anbieters vergleichbar, allerdings sind für die Einrichtung technische Grundkenntnisse erforderlich [Sc23, S. 39-40].

Die Abbildung 2.20 zeigt die grafische Benutzeroberfläche einer VPN-Anwendung. Es wird eine aktive VPN-Verbindung mittels des Status-Symbols dargestellt. Darunter wird die aktuelle Verbindung über einen Server in Singapur angezeigt, ergänzt durch die dort zugewiesene IP-Adresse 51.79.156.13. Am unteren Bildrand sind weitere Optionen und Informationen zu sehen, wie die Auswahl aus Servern in über 89 Ländern, "unbegrenzte Geschwindigkeit" und "optimierte Streaming-Server".

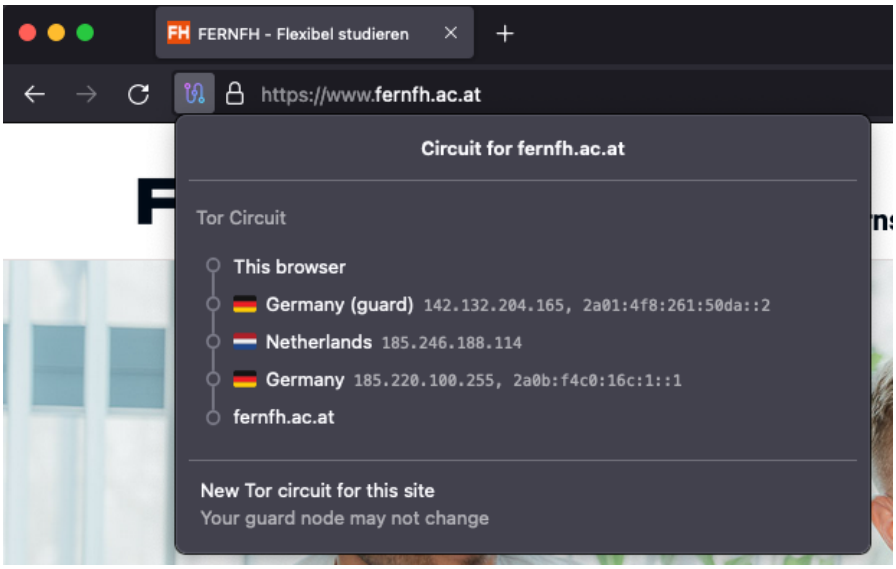
2.4.4. Anonymisierungsnetzwerk Tor

as Tor-Netzwerk ist ein dezentrales Anonymisierungsnetzwerk, das es Nutzer*innen ermöglicht, ihre Online-Aktivitäten zu verschleiern und Überwachung sowie Zensur zu umgehen. Es basiert auf einer Technik namens "Onion Routing", bei der Daten verschlüsselt durch mehrere Knotenpunkte (sogenannte Tor-Nodes) geleitet werden, wodurch die Rückverfolgung zum ursprünglichen Nutzer*innennahezu unmöglich gemacht wird. Tor wird häufig eingesetzt, um Zugang zu blockierten Webseiten zu erhalten und die Privatsphäre der Nutzer*innen zu schützen, obwohl die Datenübertragung dadurch in der Regel langsamer wird. Diese Geschwindigkeitsreduktion ist eine Folge der mehrfachen Verschlüsselung und der indirekten Routenführung durch die diversen Knoten [Sc17]. Damit bietet das Tor-Netzwerk eine kostenlose und benutzerfreundliche Alternative, die zwar langsamer ist als beispielsweise ein VPN, aber für bestimmte Anwendungen ausreichen kann. Dies wird zum Beispiel durch den kostenlosen Tor-Browser ermöglicht. In speziellen Fällen, wie bei der Nutzung des Portals `s.to`, stellt der geringe Datendurchsatz von Tor kein praktisches Hindernis dar. `s.to` hostet die Videostreams nicht direkt, sondern bietet lediglich Links zu den Streams an. Die Streams selbst können dann außerhalb des Tor-Netzwerks mit normaler Internetgeschwindigkeit abgerufen werden. Die Einrichtung ist ohne weiterer technischer Fachkenntnisse möglich. Der Tor Browser kann mittels Downloads von der offiziellen Seite `https://www.torproject.org/` heruntergeladen werden und ist sofort ausführbar [To24], [Sc23, S. 40-41].

Die Abbildung 2.21 zeigt ein Fenster des Tor-Browsers, das die verschlüsselte Verbindungskette, den sogenannten Tor Circuit, für die aufgerufene Website `fernfh.ac.at` darstellt. Der Datenverkehr dieses Browsers wird zunächst über einen sogenannten Guard-Node in Deutschland geleitet, erkennbar an der Flagge und der Angabe "(guard)", gefolgt von der IP-Adresse. Danach wird die Verbindung über einen weiteren Knoten in den Niederlanden und anschließend über einen weiteren Knoten in Deutschland fortgesetzt. Die letzte Station auf diesem spezifischen Weg ist die Ziel-Website `fernfh.ac.at`. Unterhalb der aufgelisteten Knoten befindet sich die Option "New Tor circuit for this site", die es Nutzer*innen ermöglicht, einen neuen Verbindungsweg durch das Tor-Netzwerk für diese Seite zu erstellen. Zusätzlich wird darauf hingewiesen, dass sich der Guard-Node dabei möglicherweise nicht ändert. Das Interface ist klar strukturiert und bietet dem Nutzer*innen sowohl Transparenz über die gewählten Verschleierungspunkte als auch Kontrolle über die Verbindungskette.

Weitere Umgehungsmethoden

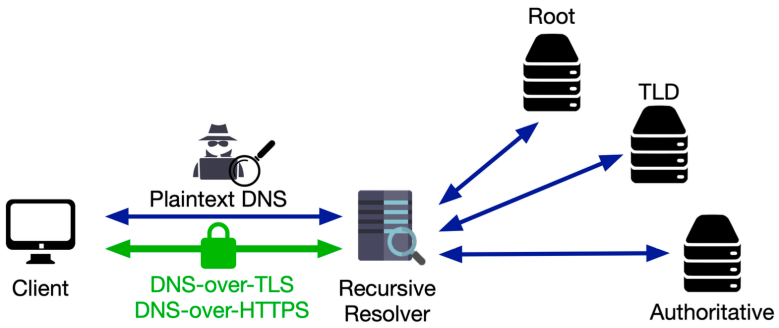
In diesem Abschnitt werden weitere Umgehungsmethoden aus Sicht der Nutzer*innen vorgestellt. Für das Experiment sind die bereits näher vorgestellten Umgehungsmethoden in den Abschnitten 2.4.1, 2.4.2, 2.4.3 und 2.4.4 ausreichend, da in Österreich ausschließlich DNS-Sperren zum Einsatz kommen. Dennoch werden in diesem Abschnitt weitere Methoden aufgeführt, die im Rahmen der Literaturrecherche identifiziert wurden.



Abbildungsverzeichnis 2.21.: Beispiel Tor Circuit. Quelle: Tor-Browser

Eine solche Methode ist die Verwendung von Proxy-Servern, die als Vermittler zwischen Endgeräten und dem Zielserver fungieren. Durch die Weiterleitung der Anfragen über einen Proxy-Server können Nutzer*innen die Sperren umgehen, da sich dieser Server an einem anderen geografischen Standort befinden kann, außerhalb der Jurisdiktion, in der die Sperren wirksam sind. Außerdem kann ein Proxy-Server so konfiguriert werden, dass er DNS-Anfragen über seinen eigenen DNS-Resolver leitet, der nicht von der Sperre betroffen ist. Somit können Nutzer*innen eine Website über den Domainnamen aufrufen, selbst wenn der lokale DNS-Resolver den Zugang zur Domain blockiert. Allerdings bieten Proxy-Server standardmäßig keine Verschlüsselung, was ein Sicherheitsrisiko darstellen kann. Ein VPN funktioniert nach dem gleichen Prinzip wie ein Proxy-Server und bietet zusätzlich eine Verschlüsselung [Sc23, S. 41], [Do04a, S. 17].

Eine weitere Umgehungstechnik stellt der Einsatz von verschlüsseltem DNS, wie DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT), dar. Diese Protokolle bieten eine verschlüsselte Übertragung von DNS-Anfragen und -Antworten zwischen den Nutzer*innen und dem DNS-Resolver. Das DNS-Protokoll sieht eine unverschlüsselte Übertragung vor, sodass DNS-Anfragen für Einsicht und Veränderung durch Dritte offenstehen. Verschlüsselte DNS-Verbindungen bieten somit einen Vorteil gegenüber unverschlüsselten DNS-Verbindungen, indem sie die Anfragen vor Sniffing und Manipulation durch Dritte schützen. Die Verschlüsselung verhindert, dass Internet Service Provider (ISPs) oder andere Akteure die besuchten Webseiten nachvollziehen können, was bei der Umgehung von DNS-Sperren von Vorteil ist. Dadurch sind ISPs nicht in der Lage, verschlüsselte Anfragen zu filtern oder zu blockieren. Abbildung 2.22 illustriert eine verschlüsselte DNS-Verbindung. Die blauen Linien zeigen den unverschlüsselten DNS-Verkehr und die grüne Linie den verschlüsselten DNS-Verkehr. Verschlüsseltes DNS trägt somit nicht nur zur Umgehung von Zensurmaßnahmen bei, sondern erhöht auch die allgemeine Sicherheit und Privatsphäre der Internetnutzung. Dies kann insbesondere in Regionen von Bedeutung sein, in denen



Abbildungsverzeichnis 2.22.: Abbildung von DNS- und verschlüsselten DNS-Verbindungen. Quelle: [Ji21, S. 485]

Internetzensur durch Filterung von Datenverkehr (z. B. Deep Packet Inspection) stattfindet [Ji21, S. 485].

2.4.5. Vergleich der Umgehungsmethoden

Der folgende Abschnitt bietet eine Übersicht der Umgehungsmethoden, die in vorangehenden Abschnitten eingehend erläutert wurden. Die nachstehende Tabelle 2.1 stellt die Charakteristiken jeder Methode gegenüber, um Nutzer*innen eine fundierte Entscheidungsgrundlage für die Wahl der geeigneten Umgehungsmethode im Kontext österreichischer Netzsperren zu bieten.

Die detaillierte Betrachtung der Tabelle 2.1 zeigt, dass jede Umgehungstechnik ihre spezifischen Vor- und Nachteile hat. Die Verwendung einer IP-Adresse zum Abruf von Inhalten stellt einen einfachen und kostenlosen Ansatz dar, ist aber aufgrund von Einschränkungen bei virtuelles Hosting-Plattformen und der Notwendigkeit, die korrekte IP-Adresse zu kennen, nur bedingt anwendbar. Außerdem bietet diese Methode keine Verschlüsselung, was ein Sicherheitsrisiko darstellen kann und ist nur bei DNS-Sperren wirksam. Die Änderung des DNS-Resolvers bietet eine einfache und ebenfalls kostenlose Alternative, die das Potenzial hat, die Privatsphäre der Nutzer*innen zu erhöhen. Allerdings ist diese Technik nur gegen DNS-Sperren wirksam und nicht gegen IP-Sperren und kann je nach gewähltem Resolver zu einer Verlangsamung der Internetverbindung führen. Ein VPN hingegen ermöglicht nicht nur die Umgehung von DNS- und auch IP-Sperren, sondern schützt die Datenübertragung zusätzlich durch Verschlüsselung. Dieser erhöhte Schutz ist jedoch oft mit Kosten verbunden und/oder erfordert ein gewisses technisches Verständnis für die Einrichtung. Außerdem kann die Verschlüsselung zu langsameren Verbindungen führen und die Notwendigkeit, einen vertrauenswürdigen Anbieter zu finden, stellt eine zusätzliche Herausforderung dar. Das Tor-Netzwerk schließlich soll ein hohes Maß an Anonymität bieten und ist in der Lage, sowohl DNS- als auch IP-Sperren ohne Kosten zu umgehen. Allerdings sind die Internetverbindungen oft langsamer, da die Bandbreite geringer ist, was insbesondere beim Abruf datenintensiver Inhalte von Nachteil sein kann. Insgesamt hängt die Wahl der geeigneten Umgehungstechnik stark von den individuellen Bedürfnissen und Umständen der Nutzer*innen ab. Es gilt, eine Balance

zwischen Anonymität, Geschwindigkeit, Kosten und technischem Aufwand zu finden. Für eine effektive Umgehung von Netzsperren ist daher oft eine Kombination verschiedener Techniken ratsam, um sowohl Zugänglichkeit als auch Sicherheit und Privatsphäre optimal zu gewährleisten.

Es kann festgehalten werden, dass Netzsperren durch Internet Service Provider zwar möglich sind, die beschriebenen Techniken der DNS- und IP-Sperre jedoch mit relativ wenig Aufwand überwunden werden können. Weiterhin ist hinsichtlich der Verhinderung des Zugriffs auf bestimmte Webseiten zu bemerken, dass eine präzise Netzsperre angesichts der aktuellen Beschaffenheit des Internets fast unmöglich ist, ohne unbeabsichtigte Auswirkungen hinzunehmen. Wie festgestellt wurde, befinden sich in Österreich aufgrund der Verhältnismäßigkeit seit 2023 nur noch DNS-Sperren im Einsatz. Deshalb werden diese vier in der Tabelle 2.1 dargestellten Methoden für die empirische Untersuchung in Betracht gezogen.

Methode	DNS-Sperre umgehen	IP-Sperre umgehen	Vorteile	Nachteile
IP-Adresse verwenden 2.4.1	Ja, aber nur ohne virtuellem Hosting	Nein	- Einfacher Ansatz - Keine Kosten	- Korrekte IP muss ermittelt werden - Einschränkungen bei Verwendung von virtuellem Hosting - Keine Verschlüsselung - Effektiv nur bei DNS-Sperren
DNS-Resolver ändern 2.4.2	Ja	Nein	- Einfach einzurichten - Keine Kosten - Erhöhte Privatsphäre	- Effektiv nur bei DNS-Sperren - Möglicherweise langsamer als ISP DNS - Kein Schutz bei IP-Blockaden
VPN 2.4.3	Ja	Ja	- Einfache Anwendung - Umgeht DNS- als auch IP-Sperren - Verschlüsselte Verbindung	- Kostenpflichtig oder technisches Know-how bei Einrichtung erforderlich - Möglicherweise langsamer durch Verschlüsselung - Vertrauenswürdiger Anbieter erforderlich
Tor 2.4.4	Ja	Ja	- Einfache Bedienung - Umgeht DNS- und IP-Sperren - Hohe Anonymität - Keine Kosten	- Verringerte Bandbreite - Aufwendiges Routing - Dadurch langsamere Verbindungen

Tabelle: 2.1.: Übersicht der Umgehungsmethoden für DNS- und IP-Sperre

2.5. Bestehende Forschung und Lücken

Die bestehende Forschung bietet wertvolle Erkenntnisse über die Methoden der Netzsperren in Europa und weltweit. Allerdings wurde der spezifische Kontext von Netzsperren in Österreich und die dortigen technischen Umgehungsmöglichkeiten noch nicht hinreichend untersucht. Diese Masterarbeit verfolgt das Ziel, diese Forschungslücke zu schließen und liefert Ergebnisse zu Methoden der technischen Umgehungsmöglichkeiten von Netzsperren in Österreich. Die vorliegende Arbeit verbindet bestehende Forschungsansätze mit der spezifischen Situation in Österreich, um ein umfassendes Bild der aktuellen Herausforderungen und Möglichkeiten zu zeichnen.

2.5.1. Bestehende Forschung zu Netzsperren in der EU

Die Forschungsarbeit von Ververis et al. (2023) [Ve23] untersucht die Methoden zur Blockierung von Webseiten in der Europäischen Union. Die Analyse zeigt, dass trotz der strengen Regulierungen und Richtlinien zur Gewährleistung eines offenen Internets die Mitgliedsstaaten weiterhin verschiedenste Webseiten und Dienste blockieren. Die Autor*innen analysierten umfangreiche Netzwerkdaten, darunter Millionen von historischen Netzwerkmessungen, öffentlich zugängliche Blockierungslisten der EU-Mitgliedstaaten und Berichte von Netzwerkregulierern. Die Ergebnisse verdeutlichen, dass die Transparenz von Blockierungsmaßnahmen in den EU-Ländern mangelhaft ist. Obwohl die Regulierungsbehörden in ihren Jahresberichten detailliert auf die Einhaltung der Netzneutralität eingehen, fehlen oft klare Informationen darüber, wie und warum spezifische Blockierungen durchgeführt werden. Die Studie legt dar, dass verschiedene Arten von Inhalten und Diensten ohne offensichtliche Gründe blockiert werden, wobei diese Blockierungen nicht immer in den öffentlich zugänglichen Listen vermerkt sind. Interessanterweise bieten die Forschungsergebnisse auch einen tiefen Einblick in die technischen und politischen Herausforderungen, die mit der Bewertung und Überwachung von Internetzensur verbunden sind. Die Studie unterstreicht die Relevanz von Transparenz und rechtlicher Klarheit, um die Rechtmäßigkeit von Blockierungen zu gewährleisten und gleichzeitig die Grundrechte der Nutzer*innen zu schützen.

2.5.2. Bestehende Forschung zu Netzsperren in Spanien

Die umfassende Untersuchung von Isaakidis et al. (2021) [Ve21] zur Internetzensur in Spanien beleuchtet insbesondere die Ereignisse rund um das katalanische Unabhängigkeitsreferendum im Jahr 2017. Die Autor*innen dieser Studie haben detailliert analysiert, wie staatliche und private Anbieter durch technische Eingriffe in Netzwerke den Zugang zu spezifischen Inhalten regulierten und kontrollierten. Die Eingriffe umfassten Techniken wie DNS-Manipulation und das Blockieren von HTTP-Anfragen, um den Zugriff auf politisch sensible Inhalte effektiv zu unterbinden. Die Forscher*innen identifizierten und dokumentierten 16 verschiedene Blockseiten, die von den Internet Service Providern eingesetzt wurden. Zudem wurde aufgedeckt, dass zwei Arten von Deep Packet Inspection (DPI)-Geräten benutzt wurden, um insgesamt 78 Webseiten zu blockieren. Die Analyse

basiert auf Daten, die vom Open Observatory of Network Interference (OONI) gesammelt wurden, und umfasst verbesserte Testmethoden zur Erkennung von TLS-Blockierungen. Ein wesentlicher Beitrag der Studie ist die Entwicklung und Validierung einer Methodologie, die zukünftige Forschungen zur Internetzensur unterstützen kann. Die entwickelte Methodik erlaubt eine detaillierte Analyse der technischen Aspekte von Netzeingriffen und stellt eine solide Grundlage für die Reproduzierbarkeit der Forschungsergebnisse in anderen geografischen oder politischen Kontexten dar. Des Weiteren diskutieren Isaakidis und sein Team die politischen und ethischen Implikationen ihrer Erkenntnisse. Die Autor*innen betonen die Notwendigkeit einer transparenten Offenlegung der Zensurmaßnahmen durch ISPs und Regierungen, um eine informierte öffentliche Debatte und die Einhaltung demokratischer und rechtlicher Normen zu gewährleisten.

2.5.3. Verschlüsseltes DNS und Internetzensur

Die Studie von Jin et al. (2021) [Ji21] untersucht die Auswirkungen von verschlüsseltem DNS auf die Internetzensur. Dabei fokussieren sich die Autor*innen auf DNS-over-TLS (DoT) und DNS-over-HTTPS (DoH), zwei Technologien, die entwickelt wurden, um die Privatsphäre und Sicherheit bei der Internetnutzung durch DNS-Verschlüsselung zu verbessern. Die Studie offenbart, dass trotz der Verschlüsselung Manipulationen an DNS-Antworten weiterhin ein ernsthaftes Problem darstellen. Die Autor*innen führten umfangreiche Messungen durch, bei denen sie 7,4 Millionen DNS-Abfragen an 3.813 DoT- und 75 DoH-Resolver sendeten. Die Studie zeigt, dass 1,66 Prozent der DoT- und 1,42 Prozent der DoH-Antworten manipuliert wurden. Diese hohen Manipulationsraten deuten darauf hin, dass Zensurbehörden möglicherweise Wege gefunden haben, auch verschlüsselte DNS-Anfragen zu beeinflussen. Darüber hinaus zeigt die Studie, dass die Wirksamkeit verschlüsselter DNS-Dienste bei der Umgehung von Zensur stark regional abhängig ist. Während in einigen Ländern, wie beispielsweise China, eine teilweise Umgehung der Zensur durch den Einsatz von verschlüsseltem DNS erlaubt ist, zeigt sich in anderen Ländern, wie etwa dem Iran, dass verschlüsseltes DNS allein nicht ausreicht, um staatliche Internetzensur vollständig zu umgehen. Diese Ergebnisse sind insbesondere im Kontext der Diskussion um digitale Rechte und Internetfreiheit von Bedeutung. Die Ergebnisse legen nahe, dass Technologien, die eigentlich der Sicherung der Privatsphäre dienen, auch für Zwecke missbraucht werden können, die dieser entgegenstehen. Zudem wird ersichtlich, dass der Kampf gegen Internetzensur ständige technologische Weiterentwicklungen erfordert.

2.5.4. Taxonomie von Netzsperren

Die Dissertation "Modeling and Characterization of Internet Censorship Technologies" von Alexander Master [Ma23] untersucht Internetzensurtechnologien und deren Anwendung durch Staaten weltweit. Es wird ein Referenzmodell für Zensurtechnologien entwickelt, das zur konzeptionellen Verständigung über Zensurmaßnahmen im Internet dient. Zudem wird eine umfassende Taxonomie der Methoden der Internetzensur bereitgestellt. Anhand einer

weltweit repräsentativen Stichprobe wird untersucht, wie Staaten das Internet zensieren. Insgesamt wird deutlich, dass viele Staaten mindestens eine Form der Internetzensur einsetzen.

Der Autor hat die Taxonomie im Rahmen des OSI-Modells organisiert, damit wird eine logische Visualisierung und das Verständnis gefördert. Die Taxonomie ist zu sehen in Abbildung 2.23. Eine Zensurmethode wird als Abstraktion ähnlicher Techniken dargestellt. Die Liste der Techniken, die eine Zensurmethode umfassen, ist umfangreich, aber nicht erschöpfend. Die Schichten 1-4 repräsentieren Methoden, die nur eine "shallow packet inspection" erfordern, das heißt sie beschränken sich auf das Lesen von Paket-Headern und sind wesentlich weniger ressourcenintensiv. "Deep packet inspection"-Methoden analysieren den Inhalt der Datenpakete, die Payload, jenseits der Paket-Header. Eine Bandbreitendrosselung kann sowohl auf Netzwerk- als auch auf Applikationsebene erfolgen. "Distributed Denial of Service"-Angriffe finden ebenfalls sowohl auf Netzwerk- als auch auf Applikationsebene statt. Unterhalb von DPI stellt der Autor die "Traffic Behavior Analysis" vor. Diese Analyse beinhaltet das Beobachten von Mustern oder ungewöhnlichen Verhaltensweisen in Datenströmen, einschließlich derjenigen, die verschlüsselt sind. "Encrypted Traffic Analysis" (ETA) verwendet häufig maschinelles Lernen oder statistische Modelle, um Verkehrsverhaltensprofile für bestimmte Anwendungen oder Protokolle zu erstellen. Im Allgemeinen nimmt die Komplexität der Implementierung zu, je höher die OSI-Schichten sind [Ma23, S. 104-105].

2.5.5. Forschungslücken und Bedeutung für diese Arbeit

Die vorhandene Forschung zur Effektivität und zum Potenzial von Technologien zur Umgehung von Internetzensur liefert grundlegende Einblicke, die für das Verständnis und die Bewertung von Zensurumgehungstechnologien von Bedeutung sind. Die Studien zeigen, wie unterschiedlich diese Technologien in verschiedenen globalen Kontexten funktionieren und welche Herausforderungen sich in der praktischen Anwendung ergeben können. Sie verdeutlichen die Bedeutung technologischer Innovationen und deren Rolle in der Auseinandersetzung mit staatlich veranlassten Netzsperren. Trotz dieser umfassenden Analysen bleibt jedoch oft unklar, wie effektiv spezifische Methoden in bestimmten regionalen oder rechtlichen Rahmenbedingungen, wie etwa in Österreich, sind. Die in der Literatur vorhandene Forschungslücke manifestiert sich insbesondere in der unzureichenden spezifischen Untersuchung der Wirksamkeit dieser Technologien unter den Bedingungen von Netzsperren in Österreich. Die vorhandenen Studien fokussieren sich häufig entweder auf theoretische Aspekte oder auf die allgemeine Anwendbarkeit in diversen geografischen oder politischen Kontexten abseits von Österreich. Die vorliegende Masterarbeit schließt diese Forschungslücke, indem sie sich explizit mit den technischen Umgehungsmethoden von Netzsperren in Österreich auseinandersetzt. Durch die empirische Bewertung verschiedener Techniken und deren Effektivität in der Praxis wird ein bedeutender Beitrag zur bestehenden Forschung geleistet. Dies erweitert nicht nur das technische Verständnis von Zensur und deren Umgehung, sondern bietet auch praktische Empfehlungen für Nutzer*innen und Entwickler*innen zur Wahrung der Internetfreiheit. Die Arbeit leistet

	OSI Model	Censorship Methods	Example Techniques
Shallow Packet Inspection	Physical Layer	Internet Shutdowns	Physical network disconnection
	Data Link Layer		Logical denial
		Local Network Attacks	ARP poisoning DoS
			MAC address filtering
	Network Layer	IP Address Blocking	IP address blocklist/allowlist
			IP subnet blocklist/allowlist
			Residual censorship
		Internet Shutdowns	Routing blackhole
			Routing manipulation
		Resource Exhaustion	Network DDoS
	Transport Layer	Port Blocking	Port blocklist/allowlist
			TCP/UDP/QUIC manipulation
			Residual censorship
		BGP Attacks and Disruption	BGP hijacking
			AS path forgery
			BGP collusion attack
		Bandwidth Throttling	Indiscriminate throttling
Deep Packet Inspection	Session, Presentation, and Application Layers		DPI latency injection
			Traffic shaping/policing
			Quality of Service (QoS)
		DNS Tampering	DNS blocklist/allowlist
			DNS cache poisoning
			DNS hijacking
			DNS transparent proxy
		Protocol/Application Content Filtering	URL blocklist/allowlist
			HTTP web content matching
			Keyword filtering (FTP, SMTP, IMAP, etc.)
		TLS-based Filtering	SNI blocklist
			MITM Attack
			Application targeting
		Resource Exhaustion	Application-layer DDoS
		Computer Network Attack	Offensive cyberspace operations
Traffic Behavior Analysis		Protocol/Application Fingerprinting	Protocol or application blocking
			Active probing
			Encrypted traffic analysis
			Pattern/heuristic matching

Abbildungsverzeichnis 2.23.: Taxonomie von Netzsperren. Quelle: [Ma23, S. 106]

einen Beitrag zur Bereicherung der Debatte über Informationsfreiheit und -sicherheit in digitalen Wirtschaftsgütern sowie zur Förderung des Diskurses über die Balance zwischen Sicherheitsanforderungen und dem Recht auf freien Informationszugang. Die Fokussierung auf Österreich ermöglicht zudem einen Beitrag zur globalen Diskussion um Internetfreiheit.

3. Konzeptioneller Vorgehens- und Lösungsansatz

Aufbauend auf der Forschungsfrage *Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen?* und den Erkenntnissen des Kapitels 2 wird im Kapitel 3 ein Lösungsansatz konzipiert und eine Vorgehensweise aufgezeigt, die für die Beantwortung der Forschungsfrage benötigt wird. Es braucht also noch eine oder mehrere Methoden, um die Forschungsfrage zu beantworten. Die Gesamtheit der Methoden, die man zur Erreichung des Forschungsziels der wissenschaftlichen Arbeit anwendet, nennt man auch das Forschungsdesign [St21, S. 44]. Das Ziel dieses Kapitels ist die Entwicklung einer fundierten und effektiven Methode zur Evaluierung der Wirksamkeit verschiedener Technologien zur Umgehung von Netzsperren in Österreich. Dabei wird insbesondere berücksichtigt, dass DNS-Sperren in Österreich vorherrschen. Das Forschungsdesign dieses Kapitels umfasst die detaillierte Planung und Beschreibung der Schritte, die notwendig sind, um die Effektivität der verschiedenen Umgehungstechniken empirisch zu evaluieren. Der systematische Aufbau der empirischen Tests sowie die präzise Definition der Messparameter gewährleisten die Reproduzierbarkeit und Validität der Ergebnisse. Die Beantwortung der Forschungsfrage basiert auf einer fundierten wissenschaftlichen Grundlage und vertieft das Verständnis der Wirksamkeit von Umgehungstechnologien im Kontext von Österreich.

3.1. Ausgewähltes Forschungsdesign

Im Rahmen der Untersuchung der Wirksamkeit technischer Methoden zur Umgehung von Netzsperren in Österreich wird ein quantitativ-experimentelles Forschungsdesign gewählt. Dieses erlaubt die Generierung numerischer Daten, welche eine statistische Analyse der Erfolgsraten und der Antwortzeiten verschiedener Umgehungsmethoden ermöglichen. Das experimentelle Design wurde bewusst gewählt, um die Wirksamkeit der Technologien unter kontrollierten Bedingungen zu testen. Auf diese Weise können Zusammenhänge zwischen den eingesetzten Technologien und ihrer Fähigkeit, Netzsperren zu umgehen, untersucht werden. Dieser methodische Ansatz ist entscheidend, um valide und reproduzierbare Ergebnisse zu erzielen und fundierte Schlussfolgerungen über die Wirksamkeit der Umgehungstechniken ziehen zu können. Ziel ist es, die technischen Umgehungsmöglichkeiten von Netzsperren in Österreich quantitativ zu bewerten. Um

eine solide methodische Vorgehensweise zu gewährleisten, orientiert sich diese Arbeit an etablierten Forschungsarbeiten und Methoden aus verwandten Studienbereichen.

3.2. Methodenliteratur

Basierend auf den Erkenntnissen und Methoden der folgend genannten Literatur wird die methodische Vorgehensweise dieser Masterarbeit erweitert und an den spezifischen Kontext von Netzsperren in Österreich angepasst.

Die Arbeit greift auf die Studie "Understanding the Impact of Encrypted DNS on Internet Censorship" [Ji21] zurück, welche die Wirksamkeit von verschlüsseltem DNS (DNS über HTTPS (DoH) und DNS über TLS (DoT)) zur Umgehung von Zensurmaßnahmen in verschiedenen Ländern untersucht. Diese Studie dient als methodische Referenz für die Analyse von Umgehungstechnologien und ihrer Effektivität im Kontext der Internetzensur. Jin et al. bieten wertvolle Einblicke in die methodische Herangehensweise zur Bewertung der Effektivität von Technologien zur Umgehung von Zensur, einschließlich der Auswahl von Testfällen und der Durchführung von empirischen Tests.

Ein weiteres methodisches Vorbild ist die Arbeit von Master und Garman [Ma23], die mit "Disguiser" ein Framework zur Erkennung von Zensurmaßnahmen durch präzise End-to-End-Messungen vorstellt. Diese Arbeit zeigt Wege auf, um die Verbreitung und Effektivität von Zensurmechanismen global zu analysieren. Die technische Herangehensweise der Autor*innen zur Datenerhebung und -auswertung dient als Inspiration für die experimentelle Analyse in dieser Masterarbeit.

Die methodische Fundierung der eigenen Forschung kann durch eine vergleichende Analyse mit der Studie des Berkman Klein Center for Internet and Society an der Harvard University aus dem Jahr 2011 vertieft werden [RZP11]. Diese Studie evaluierte die Wirksamkeit verschiedener Umgehungstools gegen staatliche Internetzensur mittels eines umfassenden Mixed-Methods-Forschungsdesigns, das sowohl quantitative als auch qualitative Methoden integrierte. Die technische Bewertung der Tools erfolgte durch systematische Tests der Geschwindigkeit, Zuverlässigkeit und Sicherheit unter simulierten Netzwerkbedingungen. Spezifische Szenarien wurden entwickelt, um die Fähigkeit der Werkzeuge zu testen, verschiedene Zensurmaßnahmen effektiv zu umgehen. Zusätzlich zur technischen Bewertung wurde die Sicherheit jedes Tools eingehend analysiert, um potenzielle Risiken und die Wirksamkeit der implementierten Sicherheitsfunktionen zu ermitteln. Eine qualitative Dimension wurde durch das Sammeln von Nutzerfeedback mittels Umfragen und Interviews hinzugefügt, was wertvolle Einblicke in die Benutzerfreundlichkeit und die tatsächliche Nutzererfahrung lieferte. Die daraus resultierenden Daten wurden mit einer Kombination aus statistischen Methoden und qualitativer Inhaltsanalyse ausgewertet, um eine detaillierte Bewertung der Leistung des Tools und der Nutzererfahrung zu ermöglichen. Diese Herangehensweise verdeutlicht die Wichtigkeit einer methodisch fundierten Evaluation von Technologien zur Umgehung von Netzsperren und bildet eine wichtige Grundlage für die Entwicklung des Forschungsdesigns der vorliegenden

Arbeit, welches darauf abzielt, die Wirksamkeit spezifischer Methoden zur Umgehung von Netzsperren in Österreich zu untersuchen.

Zusätzlich zu den bereits besprochenen Studien fließen in diese Masterarbeit Erkenntnisse aus der Untersuchung "Measurement of Globally Visible DNS Injection" von Wander et al. [Wa14] ein. Diese Forschungsarbeit befasst sich mit der Implementierung und den Auswirkungen von DNS-Injektionen als Methode der Internetzensur und analysiert deren Einfluss auf globale Netzwerke. Wander et al. präsentieren eine umfassende Methodik zur Identifizierung und Messung von DNS-Injektionen aus der Perspektive außerhalb zensierter Netzwerke. Ihr Ansatz besteht darin, eine große Anzahl öffentlicher IPv4-Adressen auf das Vorhandensein von DNS-Injektionen zu untersuchen. Als Fallbeispiele dienen China und der Iran. Die Studie zeigt, wie DNS-Injektionen auch Dritte betreffen, deren Datenverkehr unbeabsichtigt über zensierte Netzwerke geleitet wird, und unterstreicht die globalen Auswirkungen lokaler Zensurmaßnahmen.

Wichtige methodische Komponenten von Wander et al., die für diese Masterarbeit relevant sind, umfassen

- Internetweite Messungen: Die Studie verwendet großflächige Abfragen, um Netzwerke zu identifizieren, die DNS-Injektionen einsetzen. Durch das Versenden von DNS-Anfragen an zahlreiche Ziele können die Forscher*innen feststellen, ob die Antworten manipuliert wurden, und bieten so einen skalierbaren Ansatz zur Erkennung von Zensurmaßnahmen.
- Algorithmus zur Erkennung gefälschter Adressen: Zur Verbesserung der Identifizierung gefälschter DNS-Antworten entwickeln die Autor*innen einen Algorithmus, um eine Liste von IP-Adressen zu sammeln, die in injizierten DNS-Antworten verwendet werden. Diese Technik ermöglicht die effiziente Erkennung von Zensur auch außerhalb der betroffenen Netzwerke.
- Granularität von DNS-Blacklists: Die Forschung untersucht die Spezifität und das Ausmaß der Domain-Blockierung und analysiert, wie verschiedene Domain-Name-Varianten Zensurmechanismen auslösen. Dieser Aspekt ist entscheidend, um das Ausmaß der DNS-Filterung und das Potenzial für Überblockierungen zu verstehen.
- Auswirkungen auf unbeteiligte Netzwerke: Durch das Abfragen von offenen Resolvern weltweit bewertet die Studie, wie DNS-Injektionen Netzwerke außerhalb der zensierenden Länder beeinflussen. Diese globale Perspektive ist entscheidend, um die unbeabsichtigten Konsequenzen nationaler Zensurmaßnahmen zu verstehen.

Durch die Integration dieser Methoden in die Analyse der Internetzensur in Österreich wendet die vorliegende Masterarbeit ähnliche großflächige Messtechniken an, um die Häufigkeit und Effektivität von DNS-basierten Zensurmaßnahmen und deren Umgehung zu evaluieren. Die Forschungsergebnisse von Wander et al. bieten einen robusten Rahmen für die Erkennung und Analyse von Zensuraktivitäten, der an den spezifischen Kontext von Netzsperren in Österreich angepasst wird. Durch die Kombination von empirischen Tests, algorithmischer Erkennung und umfassender Analyse zielt die Arbeit darauf ab, eine

fundierte Bewertung der Effektivität von Umgehungsmethoden von DNS-Sperren auf die Internetzugänglichkeit in Österreich zu liefern.

Des Weiteren stellt im Rahmen der Entwicklung einer Methodik zur Untersuchung von Internetzensur stellt der Web Connectivity Test des Open Observatory of Network Interference (OONI) [OO24] ein beispielhaftes Modell dar, an dem sich der eigene Forschungsansatz orientiert. Die umfangreiche Nutzung der OONI Probe Software, die bis März 2024 insgesamt 58.901.146 Messungen in 2.904 Netzwerken aus 173 Ländern dokumentiert hat, verdeutlicht die globale Relevanz und methodische Strenge des Tools. Die auf GitHub unter `https://github.com/ooni` (aufgerufen am 05.05.2024) verfügbare Open-Source-Software bietet einen transparenten Einblick in die technischen Mechanismen zur Erkennung von Netzsperren.

Der methodische Aufbau des Web Connectivity Tests von OONI umfasst mehrere wesentliche Komponenten, die auch für die eigene Forschung relevant sind:

- DNS-Abfragen zur Überprüfung von Domainnamen über lokale und öffentliche DNS-Resolver, die eine Grundlage zur Erkennung von DNS-Blockaden bieten.
- TCP-Verbindungstests, um festzustellen, ob eine Verbindung zu IP-Adressen möglich ist, was zur Erkennung von IP-basierten Blockaden dient.
- HTTP-GET-Requests, die an die Domains gesendet werden, um den Zugriff und das Antwortverhalten zu testen und so Rückschlüsse auf mögliche Blockaden zu ziehen.
- Vergleiche mit Kontrolldaten, die Abweichungen zwischen den Ergebnissen von gesperrten und nicht gesperrten Servern aufzeigen und damit auf Zensurmaßnahmen hinweisen können.

Obwohl der OONI-Test selbst in dieser Arbeit nicht direkt angewendet wird, dient das methodische Vorgehen und der Aufbau des Tests als wesentliche Inspiration und Orientierungshilfe für die Konzeption des eigenen Forschungsdesigns. Diese Orientierung ermöglicht eine methodisch fundierte und systematisch strukturierte Analyse der Wirksamkeit von Umgehungstechnologien für Netzsperren in einem regulierten Umfeld wie Österreich.

Für die statistische Auswertung der erhobenen Daten wird auf die in der Vorlesung "MT422 - Methoden der Datenanalyse" erlernten Methoden zurückgegriffen [Un10]. Diese umfassen grundlegende statistische Tests und Analysen, wie zum Beispiel Korrelationsanalysen und die Berechnung von Standardabweichungen. Diese Methoden ermöglichen es, Muster in den Daten zu erkennen, die Effektivität verschiedener Umgehungsmethoden objektiv zu bewerten und die Zuverlässigkeit der Techniken zu überprüfen.

3.3. Datenerhebungsverfahren

Das Datenerhebungsverfahren umfasst mehrere Schritte, die auf die Erfassung und Bewertung der verschiedenen technischen Umgehungsmethoden abzielen. Zunächst erfolgt die Auswahl von ISPs und die Definition der Zielwebseiten, die in Österreich aufgrund von DNS-Sperren nicht zugänglich sind.

Für jede Umgehungsmethode wird ein Testlauf durchgeführt, bei dem die Antwortzeit und die Erfolgsrate des Zugriffs auf die gesperrten Webseiten gemessen werden. Die Antwortzeit gibt dabei an, wie schnell eine Website trotz der Sperre erfolgreich aufgerufen werden kann, was ein wesentlicher Faktor für die Bewertung der Praktikabilität einer Umgehungsmethode ist.

Um die Effektivität der verschiedenen Umgehungsmethoden zu bewerten, werden die gesammelten Daten statistisch analysiert. Diese Analyse beinhaltet Vergleiche der Erfolgsraten und der Antwortzeiten unter verschiedenen Testbedingungen, um festzustellen, welche Methoden am konsistentesten und effektivsten Netzsperren umgehen können, um zuverlässige Aussagen über die Wirksamkeit der getesteten Methoden zuzulassen.

Diese methodische Herangehensweise stellt sicher, dass die Forschungsergebnisse nicht nur wissenschaftlich fundiert sind, sondern auch praxisrelevante Erkenntnisse zur Umgehung von Netzsperren in einem regulierten Umfeld wie Österreich liefern.

3.3.1. Auswahl der Umgehungsmethoden für die Analyse

Die Auswahl basiert auf der im Kapitel 2 dargestellten Erkenntnis, dass in Österreich DNS-Sperren eingesetzt werden. Um diese Sperren umgehen zu können, werden vier spezifische Methoden ausgewählt, die in der Tabelle 2.1 verglichen und bewertet wurden. Diese Methoden wurden ausgewählt, da sie sich zur Umgehung der in Österreich vorherrschenden DNS-Sperren eignen und somit die Forschungsfrage präzise adressieren.

Im Folgenden werden die ausgewählten Methoden beschrieben, die zur Umgehung von DNS-Sperren verwendet werden können und auf denen das Datenerhebungsverfahren aufbaut:

- **Methode 1, Verwendung einer alternativen IP-Adresse**: Diese Methode umgeht DNS-Sperren, indem direkt die IP-Adresse der Zielwebseite eingegeben wird, anstatt ihren DNS-Namen zu verwenden. Diese Methode ist effektiv, solange die IP-Adresse nicht ebenfalls blockiert ist und kein virtuelles Hosting betrieben wird (sieh auch Abschnitt 2.4.1).
- **Methode 2, Ändern des DNS-Resolvers:** Durch die Konfiguration eines alternativen DNS-Resolvers, der nicht von lokalen ISPs kontrolliert wird, können Nutzer*innen die DNS-Sperren umgehen. Resolver wie Google DNS oder Cloudflare DNS bieten Wege, um Zensurmaßnahmen zu umgehen (siehe auch Abschnitt 2.4.2).

- **Methode 3, VPN (Virtual Private Network):** VPNs verschlüsseln den gesamten Internetverkehr und leiten ihn über einen Server in einem anderen Land um. Dies nicht nur verschleiert die DNS-Anfragen, sondern ermöglicht auch den Zugriff auf Dienste und Webseiten, die regional gesperrt sind (siehe auch Abschnitt 2.4.3).
- **Methode 4, Tor-Netzwerk:** Das Tor-Netzwerk bietet eine hohe Anonymität, indem es den Internetverkehr über mehrere Server weltweit verteilt. Tor verwendet außerdem eine eigene Methode zur Auflösung von Domainnamen innerhalb des Netzwerks, wodurch es Nutzer*innen ermöglicht wird, DNS-Sperren zu umgehen, die von lokalen ISPs durchgeführt werden (siehe auch Abschnitt 2.4.4).

Diese Methoden werden im Rahmen des Experiments unter kontrollierten Bedingungen getestet, um ihre Wirksamkeit bei der Umgehung von DNS-Sperren zu bewerten.

3.3.2. Auswahl der ISPs

Die Auswahl der ISPs für die experimentellen Tests ist ein entscheidender Schritt, um die Generalisierbarkeit und Relevanz der Ergebnisse zu gewährleisten. Für die Untersuchung werden ISPs ausgewählt, die zusammen die Internetverbindungen für mehr als 80 Prozent der Internetnutzer*innen in Österreich bereitstellen. Die Datengrundlage für diese Auswahl bilden die aktuellen Berichte und Statistiken der Regulierungsbehörde RTR [RT24d], wie z. B. die Internet- oder Telekom-Monitor-Berichte. Diese Daten bieten eine aktuelle und umfassende Basis, die es ermöglicht, die relevantesten und marktführenden ISPs in die Tests einzubeziehen. Durch die Berücksichtigung dieser ISPs kann sichergestellt werden, dass die Testergebnisse eine breite Anwendbarkeit finden und die realen Gegebenheiten des österreichischen Internets widerspiegeln. Dieser methodische Ansatz ermöglicht es, die Wirksamkeit der verschiedenen Umgehungstechniken unter Bedingungen zu testen, die den Alltagserfahrungen der meisten Internetnutzer*innen in Österreich entsprechen. Die Auswahl der ISPs trägt somit wesentlich zur Validität und Aussagekraft der Ergebnisse bei.

3.3.3. Auswahl von Zielseiten

Für die experimentelle Untersuchung der Umgehungsmethoden von Netzsperren ist die Auswahl repräsentativer Zielseiten von entscheidender Bedeutung. Basierend auf der offiziellen Liste der von der RTR für gesperrte Webseiten werden die für das Experiment relevanten Seiten ausgewählt. Die Liste aller aktiven Netzsperren kann abgerufen werden unter: `https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_blockings.de.html` (abgerufen am 27.04.2024). Als Open Data ist die Liste an gesperrten Domains als .csv verfügbar unter: `https://www.data.gv.at/katalog/de/dataset/netzsperren` (abgerufen am 27.04.2024).

Für die Auswahl der Zielseiten werden jedoch Sperrlisten, die im Rahmen der EU-Sanktionsverordnung entstanden sind und ein EU-weites Verbreitungsverbot für bestimmte russische TV-Sender und Plattformen beinhalten, aus diversen Gründen ausgeschlossen.

Hierbei kommen ebenfalls DNS-Sperren zum Einsatz [WK24]. Damit unterscheiden sich technisch nicht von den Sperren, die in der Open Data-Liste dokumentiert sind. Aus technischer Sicht sind sie daher für die Analyse redundant und können aus der Untersuchung ausgeschlossen werden, ohne die Repräsentativität der Untersuchung zu verlieren.

Um eine breitere Datenbasis zu gewährleisten und die Relevanz sowie Effektivität der Umgehungsmethoden zu testen, wird zudem die Möglichkeit genutzt, zusätzliche Informationen über Netzsperren direkt von den Webseiten der Internet Service Provider zu recherchieren. Diese ISPs könnten eigene Listen oder Hinweise auf blockierte Dienste und Webseiten bieten, die nicht in der RTR-Liste enthalten sind.

Darüber hinaus wird die Nutzung externer Ressourcen, wie zum Beispiel der Citizen Lab Testlisten, in Betracht gezogen. Diese Listen bieten eine umfangreiche Sammlung von weltweit gesperrten oder zensierten URLs und können unter `https://github.com/citizenlab/test-lists` (abgerufen am 30.04.2024) eingesehen werden. Durch die Analyse dieser Listen kann die Untersuchung um eine internationale Perspektive erweitert werden, was besonders relevant ist, da DNS-Sperren nicht nur ein lokales, sondern auch ein globales Phänomen darstellen [La24].

3.3.4. Schritt 1: Überprüfung der gesperrten Webseiten

Das Ziel dieses Tests besteht in der Verifizierung der tatsächlichen Anwendung von DNS-Sperren in Österreich. Um eine solide Basis für die weiteren experimentellen Untersuchungen zu schaffen, ist es erforderlich, festzustellen, welche Webseiten tatsächlich durch Netzsperren blockiert sind. Die Verifizierungsmethode umfasst mehrere Schritte, die sicherstellen, dass die gesammelten Daten valide und zuverlässig sind. Diese Schritte werden im folgend in diesem Abschnitt vorgestellt.

Whois-Abfrage

Zuerst wird eine WHOIS-Abfrage durchgeführt, um die Top-Level-Domain (TLD) Nameserver für eine bestimmte Domain zu ermitteln. WHOIS ist ein Protokoll, das als Abfragedienst zur Ermittlung von Registrierungsinformationen zu Domainnamen, IP-Adressen und dem zugehörigen Netzwerk dient. Es liefert Details über den Registranten, den administrativen und technischen Kontakt sowie Statusinformationen zu einer Domain. Diese Informationen sind öffentlich zugänglich und bieten einen ersten Überblick darüber, wo eine Domain gehostet wird und wer sie verwaltet [Ch17].

TLD Nameserver

Aus den WHOIS-Daten werden die TLD-Nameserver (Top Level Domain) ermittelt, die für den nächsten Schritt, die Ermittlung der autoritativen Nameserver für die jeweilige

Domain, von entscheidender Bedeutung sind. Diese TLD-Nameserver sind kritisch, da sie die Verbindung zu den autoritativen Servern herstellen, die direkten Zugriff auf die gespeicherten DNS-Informationen der Domain haben.

Autoritative Nameserver

Sobald die TLD-Nameserver bekannt sind, wird der autoritative Nameserver für die Domain ermittelt. Dies ist der Server, der die A-Records der Domain enthält, das heißt er liefert die gültigen IP-Adressen, die der Domain zugeordnet sind. Die Abfrage dieser Nameserver ist entscheidend, um die tatsächlich verwendeten IP-Adressen frei von möglichen Manipulationen durch lokale DNS-Resolver oder ISPs zu erhalten.

3.3.5. Vergleich der Ergebnisse

Nach Erhalt der IP-Adressen aus den Abfragen der autoritativen Nameserver werden diese mit den Ergebnissen der DNS-Resolver der lokalen ISPs verglichen. Unterschiede zwischen den IP-Adressen können auf DNS-Manipulationen oder Blockierungen hindeuten, insbesondere wenn die Antworten der DNS-Resolver der ISP unterschiedlich ausfallen oder ganz fehlen. Diese Diskrepanzen werden als Indikator für das Vorhandensein von Netzsperren verwendet.

Dieser systematische Ansatz stellt sicher, dass die untersuchten DNS-Sperren tatsächlich existieren und dass die Ergebnisse der Umgehungsmethoden auf realen und genauen Bedingungen beruhen.

3.3.6. Umgehungsmethode 1: Verwendung der IP-Adresse

Eine grundlegende Technik zur Umgehung von DNS-Sperren ist die Verwendung von IP-Adressen für den Zugriff auf Inhalte. Um diese Methode zu evaluieren, wird die Liste von IP-Adressen und tatsächlich gesperrten Domains, welche in Schritt 1 ermittelt werden, verwendet (Abschnitt 3.3.4).

Es wird versucht, den Inhalt der Website direkt über diese IP-Adresse abzurufen. Mittels eigens entwickelter Skripte sollen systematisch HTTP(S)-Requests an die ermittelten IP-Adressen gesendet werden. Entscheidend ist, dass der abgerufene Inhalt tatsächlich der angeforderten Website entspricht und nicht vom ISP umgeleitet oder durch virtuelles Hosting unzugänglich gemacht wurde. Außerdem wird mittels Skript der HTTP(S)-Statuscode überprüft, um sicherzustellen, dass die tatsächliche Seite korrekt geladen wird. Diese Schritte sind notwendig, um die Wirksamkeit der Umgehung von DNS-Sperren mittels der Verwendung der IP-Adresse zu überprüfen und sicherzustellen, dass die Zugriffsversuche den tatsächlichen Inhalt der Zielwebseiten widerspiegeln.

3.3.7. Umgehungsmethode 2: Ändern des DNS-Resolvers

Die Verwendung eines alternativen DNS-Resolvers ist eine weitere Möglichkeit, DNS-basierte Sperren zu umgehen. Bei diesem Ansatz wird der DNS-Resolver auf einen unabhängigen Anbieter wie Cloudflare (1.1.1.1) oder Google (8.8.8.8) eingestellt. Diese unabhängigen Resolver sind nicht von möglichen Restriktionen der lokalen ISPs betroffen und bieten somit eine neutrale Basis für die DNS-Auflösung.

Um die Wirksamkeit dieser Methode zu überprüfen, wird ein eigens entwickeltes Skript verwendet, das HTTP(S)-Anfragen an eine Liste von Domains sendet, die zuvor als blockiert identifiziert wurden. Das Skript überprüft, ob die zurückgegebene IP-Adresse mit der zuvor durch DNS-Ergebnisse der autoritativen Nameserver ermittelten IP-Adresse übereinstimmt. Diese doppelte Überprüfung ist notwendig, um sicherzustellen, dass die Domain tatsächlich durch den alternativen Resolver aufgelöst und nicht durch den lokalen ISP umgeleitet wird. Die Automatisierung des Prozesses durch ein Skript ermöglicht eine effiziente und genaue Überprüfung, wobei jeder Testlauf konsistente und wiederholbare Ergebnisse liefert.

3.3.8. Umgehungsmethode 3: Verwendung eines VPN

Durch die Verwendung eines Virtual Private Network (VPN) können DNS-Sperren umgangen werden wie in Abschnitt 2.4.3. Sobald die VPN-Verbindung aufgebaut ist, ändert das VPN-Client-Programm in der Regel die DNS-Einstellungen des Geräts, sodass alle DNS-Anfragen über den VPN-Server geleitet werden. Dies ist ein kritischer Schritt, um DNS-Sperren zu umgehen. Um diese Methode zu testen, wird systematisch überprüft, ob die zuvor als gesperrt identifizierten Webseiten erreichbar sind, wenn eine VPN-Verbindung aufgebaut wird. Diese Überprüfung kann mit einem Skript ähnlich dem in Abschnitt 3.3.7 beschrieben durchgeführt werden, während die VPN-Verbindung aktiv ist. Das Hauptziel dieser Tests besteht darin, zu überprüfen, ob die Verbindung über das VPN tatsächlich in der Lage ist, die Einschränkungen zu umgehen und die Webseiten korrekt aufzurufen.

3.3.9. Umgehungsmethode 4: Verwendung des Tor-Netzwerks

Tor leitet den Datenverkehr durch ein weltweites Netzwerk, um die Herkunft und das Ziel der Daten zu verschleiern. Diese Technik ist nützlich, um DNS-Sperren zu umgehen und anonymen Zugriff auf das Internet zu ermöglichen.

Für die experimentellen Tests wird das Tor-Netzwerk eingesetzt, um die Zugänglichkeit der identifizierten gesperrten Domains zu überprüfen. Das Verfahren beinhaltet die Verwendung eines Skripts, ähnlich dem in Abschnitt 3.3.7 beschrieben, das aber noch zusätzlich eine Verbindung zum Tor-Netzwerk herstellt und Anfragen an die gesperrten Domains sendet. Das Hauptziel dieser Tests ist es, zu verifizieren, ob der Zugriff auf die Webseiten möglich ist.

3.4. Auswertungsmethodik

Die Auswertungsmethodik spielt eine entscheidende Rolle bei der Sicherstellung der Nachvollziehbarkeit der Ergebnisse dieser Forschungsarbeit. Es soll sichergestellt sein, dass die Forschungsergebnisse nicht nur wissenschaftlich fundiert, sondern auch praktisch relevant sind, und dazu beitragen, ein tieferes Verständnis der Wirksamkeit und der Anwendung von Umgehungstechnologien in einem regulierten Umfeld wie Österreich zu entwickeln.

Die Ergebnisse der Tests werden in Form von Tabellen und Grafiken dargestellt, um die Interpretation und das Verständnis der Daten zu vereinfachen. Abschließend werden die statistischen Ergebnisse im Kontext der Forschungsfrage und der theoretischen Grundlagen interpretiert, um zu prüfen, inwiefern die Ergebnisse mit bestehenden Erkenntnissen übereinstimmen oder neue Einsichten bieten.

3.4.1. Quantitative Auswertung

Die quantitative Analyse basiert auf der Sammlung numerischer Daten, die während der experimentellen Tests erfasst wurden. Diese Daten umfassen Antwortzeiten und Erfolgsraten des Zugriffs auf gesperrte Webseiten. Für die Auswertung dieser Informationen wird statistische Software verwendet, die es ermöglicht, komplexe Berechnungen wie Mittelwertbildung, Varianzanalyse und Korrelationsanalysen durchzuführen.

Erfolgsquote

Die Erfolgsquote wird definiert als der Prozentsatz der Tests, bei denen der Zugriff auf eine gesperrte Website erfolgreich war. Diese Rate ist ein direkter Indikator für die Wirksamkeit der jeweiligen Umgehungsmethode unter verschiedenen Netzwerkbedingungen.

Antwortzeit

Die Antwortzeit misst die Zeitdauer vom Senden der Anfrage bis zum Erhalt der Antwort. Dieser Wert ist besonders wichtig, um die Praktikabilität der Umgehungsmethoden zu beurteilen, da längere Wartezeiten die Benutzererfahrung negativ beeinflussen können. Antwortzeiten werden für jede Umgehungstechnik erfasst und analysiert, um festzustellen, ob signifikante Verzögerungen durch die Anwendung der Methoden entstehen.

3.4.2. Datenvalidierung und Reproduzierbarkeit

Um die Validität der Ergebnisse zu gewährleisten, werden die Tests unter kontrollierten Bedingungen durchgeführt und mehrmals wiederholt. Die Datenvalidierung erfolgt durch den Vergleich der Ergebnisse verschiedener Methoden und die Überprüfung der Konsistenz über verschiedene Testbedingungen hinweg. Die Reproduzierbarkeit der Ergebnisse wird durch die Dokumentation der Testverfahren und -einstellungen sichergestellt, die es anderen Forscher*innen ermöglicht, die Untersuchung unter gleichen Bedingungen zu wiederholen.

3.5. Mögliche Herausforderungen

Die Durchführung der Untersuchung zur Umgehung von Netzsperren in Österreich ist mit zahlreichen Herausforderungen verbunden, die sorgfältig adressiert werden müssen, um die Genauigkeit und Glaubwürdigkeit der Forschungsergebnisse zu gewährleisten. Eine der primären Herausforderungen stellt die technische Limitation der verwendeten Umgehungstechnologien dar. Technologien wie VPNs, DNS-Resolver oder das Tor-Netzwerk könnten unter bestimmten Netzwerkbedingungen ineffektiv sein. Um dies zu minimieren, wird eine robuste Validierung der Tools vor der Datenerhebung durchgeführt, einschließlich umfangreicher Vorabtests. Die Technologien werden während der Untersuchung überwacht und bei Bedarf aktualisiert, um auf Änderungen in den Sperrmethoden reagieren zu können. Wie in Kapitel 2 erörtert, ist jedoch nicht davon auszugehen, dass eine andere Sperrmethode als DNS-Sperren verwendet wird.

Eine weitere bedeutende Herausforderung ist die Entwicklung einer Methodik, um verlässliche und reproduzierbare Ergebnisse zu liefern, und gleichzeitig flexibel genug, um auf unvorhergesehene Ereignisse während der Untersuchung reagieren zu können. Diese Herausforderung wird durch die Gestaltung und das Testen eigener Skripte zur Überprüfung der Umgehungstechniken angegangen. Die Skripte werden so entwickelt, dass sie technisch korrekt funktionieren und konsistente Ergebnisse über verschiedene Testdurchläufe hinweg liefern. Durch die Minimierung menschlicher Fehler bei der Datenerhebung und die Maximierung der Automatisierung des Testverfahrens soll die Validität und Reproduzierbarkeit der Ergebnisse sichergestellt werden.

Durch den proaktiven Ansatz der Problemlösung und ständige Anpassungen soll sichergestellt werden, dass die Forschungsergebnisse nicht nur wissenschaftlich fundiert, sondern auch praktisch relevant sind und ein tieferes Verständnis der Wirksamkeit von Umgehungstechnologien in einem regulierten Umfeld wie Österreich bieten.

4. Experimentelle Analyse

In Kapitel 4 dieser Arbeit erfolt die Überprüfung der Effektivität von DNS-Sperren in Österreich. Der in Kapitel 3 vorgestellte Lösungsansatz wird dabei verfolgt. Der Schwerpunkt liegt auf der praktischen Anwendung von Python-Skripten, welche eine präzise Datensammlung und Auswertung ermöglichen. Das Ziel dieses Kapitels ist es, die Durchführbarkeit und Zuverlässigkeit dieser Methoden zu verstehen und ihre praktische Anwendbarkeit zu bewerten. Es richtet sich sowohl an technisch versierte Personen als auch an Entscheidungsträger*innen und Nutzer*innen, die ein tieferes Verständnis von Internetzensur suchen.

4.1. Hypothesen

Im Rahmen der empirischen Analyse dieser Arbeit werden folgende Hypothesen aufgestellt:

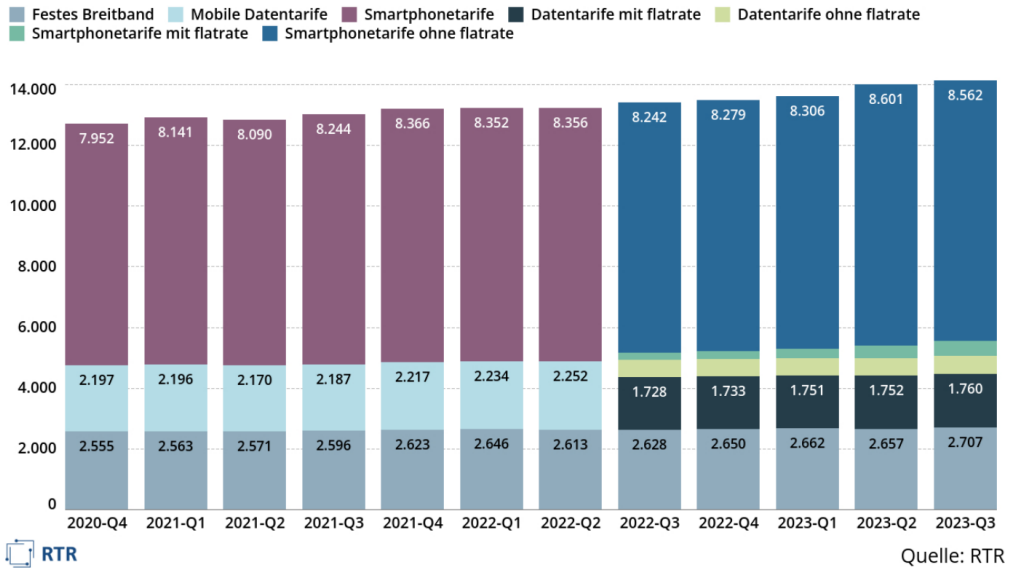
Hypothese H1 (Zusammenhangshypothese): Es besteht ein negativer Zusammenhang zwischen der Erfolgsrate der Umgehungsmethoden und der Antwortzeit. Das bedeutet, je höher die Erfolgsrate einer Methode, desto geringer tendenziell die Antwortzeit.

- **Analyseverfahren:** Korrelationsanalyse (Pearson oder Spearman je nach Datenverteilung).

Hypothese H2 (Unterschiedshypothese): Die Antwortzeiten von Tor sind signifikant höher als die der Umgehungsmethode VPN und DNS-Resolver ändern.

- **Analyseverfahren:** Varianzanalyse (ANOVA) wird verwendet, um zu testen, ob signifikante Unterschiede in den durchschnittlichen Antwortzeiten zwischen den Gruppen (VPNs, Tor und DNS-Resolver ändern) bestehen (mit Überprüfung der Voraussetzungen, alternativ Kruskal-Wallis-Test und anschließende post-hoc-Test zur Überprüfung der Signifikanz).

Diese Hypothesen zielen darauf ab, sowohl die Beziehung zwischen Erfolgsrate und Antwortzeit zu verstehen als auch spezifische Unterschiede zwischen den verschiedenen Technologien zu identifizieren, die zur Umgehung von DNS-Sperren genutzt werden. Sie basieren auf der Annahme, dass unterschiedliche Methoden unterschiedliche Eigenschaften aufweisen und dies zu unterschiedlichen Ergebnissen führt.



Abbildungsverzeichnis 4.1.: Breitbandanschlüsse im Fest- und Mobilnetz in Tausend. Quelle: [RT24e, S. 7]

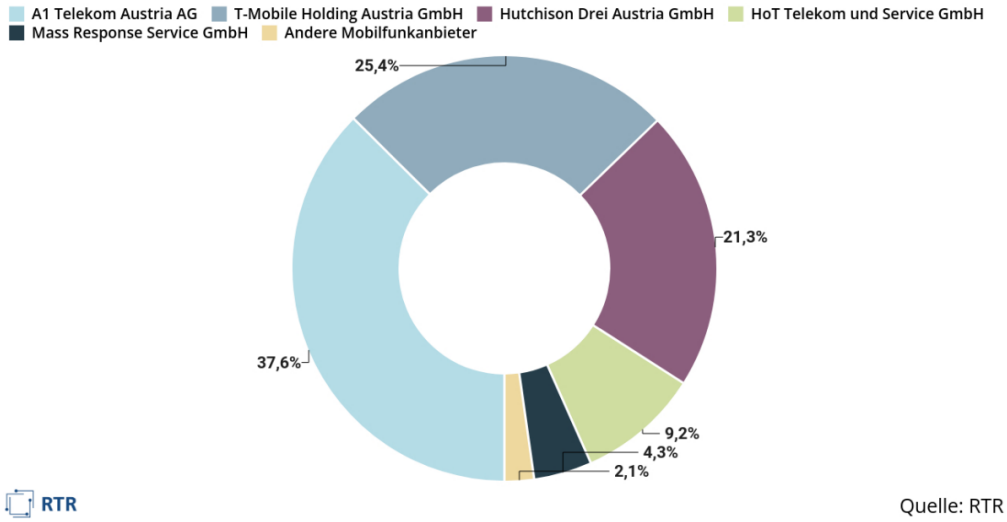
4.2. Testaufbau und Durchführung

Die Durchführung der Tests erfolgt mittels Python-Skripten. Im Vergleich zu Bash-Skripten weisen Python-Skripte Vorteile auf, da sie durch die Verfügbarkeit zahlreicher Bibliotheken eine größere Flexibilität und mehr Datenverarbeitungsoptionen bieten. Zudem sind Python-Skripte plattformübergreifend einsetzbar, was die Durchführung der Tests auf verschiedenen Betriebssystemen ohne zusätzliche Anpassungen ermöglicht. Die Python-Skripte wurden entwickelt und ausgeführt auf dem Betriebssystem `macOS Sonoma 14.3.1 (23D60)` mit Python Version `Python 3.12.3`.

4.2.1. Durchführung Auswahl der ISPs

Die Auswahl basiert auf den aktuellen Marktanteilen im Mobilfunkbereich, der für den Internetzugang in Österreich eine dominierende Rolle spielt. Die Abbildung 4.2 zeigt die Verteilung der Marktanteile basierend auf der Anzahl der aktiven SIM-Karten, wobei Anbieter mit mehr als 2 Prozent Marktanteil gesondert dargestellt werden. In der Kategorie „Andere Mobilfunkanbieter“ sind die Anteile aller nicht separat aufgeführten Anbieter zusammengefasst, die ebenfalls Mobilfunkdienste am österreichischen Markt anbieten.

Der Mobilfunkmarkt hat eine Anzahl von über 13 Millionen Breitbandanschlüssen, die über Mobilfunknetze bereitgestellt werden (ohne M2M-SIM-Karten für Machine-to-Machine-Kommunikation) [RT24e, S. 7]. Dadurch werden zur Untersuchung der Umgehungsmethoden von Netzsperren die führenden Mobilfunkbetreiber einbezogen. Im Jahr 2023 hatte in Österreich die drei größten Mobilfunkbetreiber (A1, Magenta und Drei) zusammen einen Marktanteil von 84,3 Prozent [RT24e, S. 22]. Die hohe Marktabdeckung der drei größten Mobilfunkbetreiber in Österreich macht sie zu zentralen Akteuren für die



Abbildungsverzeichnis 4.2.: Marktanteile der Mobilfunkanbieter in Österreich in Q3/2023. Quelle: [RT24e, S. 22]

Analyse der Umgehungsmethoden von Netzsperren. Aufgrund ihrer Marktdominanz haben die Ergebnisse weitreichende Implikationen.

Wie Abbildung 4.1 zeigt, überwiegen die mobilen Breitbandanschlüsse deutlich gegenüber den Festnetzanschlüssen, was die Bedeutung des mobilen Internets in Österreich unterstreicht. Dieser Überhang an mobilen Anschlüssen zeigt, dass ein großer Teil der Bevölkerung über mobile Internetzugänge verfügt. Dies unterstreicht die Relevanz der ausgewählten Mobilfunkbetreiber für die Untersuchung von Netzsperren in dieser Arbeit, da durch die Berücksichtigung von A1, Magenta und Drei die Situation von Netzsperren für mehr als 80 Prozent der Personen mit Internetzugang in Österreich untersucht werden kann.

In der weiteren Vorgehensweise der Untersuchung ist es essenziell, dass für die Tests jeweils eine SIM-Karte der drei größten Mobilfunkbetreiber A1, Magenta und Drei zur Verfügung steht. Mit diesen SIM-Karten können die Internetzugänge der Anbieter unter realen Bedingungen getestet werden. Jeder Test der jeweiligen Methode wird über die Internetverbindung eines dieser Anbieter durchgeführt, um sicherzustellen, dass die Ergebnisse die tatsächliche Fähigkeit zur Umgehung von Netzsperren unter den verschiedenen Netzbedingungen dieser Anbieter widerspiegeln. Diese Vorgehensweise ist entscheidend, um eine umfassende Analyse der verschiedenen Umgehungsmethoden durchführen zu können. Durch den direkten Zugang über die Netze der drei größten ISPs wird eine hohe Aussagekraft der Testergebnisse erreicht, da 84,3 Prozent der Internetnutzer*innen in Österreich deren Dienste in Anspruch nehmen. Der Einsatz dieser SIM-Karten bietet somit eine präzise Grundlage für die Bewertung der Effektivität von Umgehungstechniken im Kontext der österreichischen Internetlandschaft.

4.2.2. Durchführung Auswahl von Zielseiten

Der Fokus liegt auf der praktischen Anwendung der identifizierten Umgehungsmethoden auf eine gezielt ausgewählte Liste von gesperrten Webseiten. Die Grundlage dieser Auswahl bildet die Open Data-Liste der von den österreichischen ISPs gesperrten Domains (`https://www.data.gv.at/katalog/de/dataset/netzsperren` (abgerufen am 27.04.2024)). Es wurde eine spezifische Selektion vorgenommen, basierend auf den Netzsperren, die bei den drei führenden ISPs (A1, Drei und Magenta)im Einsatz sind. Diese Auswahl zeigt Unterschiede in der Anzahl der gesperrten URLs zwischen den ISPs:

- A1: 159 gesperrte Domains
- Drei: 184 gesperrte Domains
- Magenta: 179 gesperrte Domains

Die vollständige Liste dieser Zielseiten ist im Anhang unter Anhang A zu finden. Die in dieser Liste enthalten Zielseiten werden für die Untersuchung der Umgehungsmethoden verwendet.

Von den untersuchten ISPs lieferte nur Magenta auf deren Webseite spezifische Informationen zu deren Ansatz bei Netzsperren. Laut Magenta sollte sich die Anwendung von Netzsperren auf DNS-Sperren beschränken, um das Risiko des Overblockings zu minimieren. IP-Sperren oder eine Kombination aus IP- und DNS-Sperren wurden als nicht akzeptabel für die Kunden erachtet, da sie tiefgreifende Eingriffe in die Netzinfrastruktur erfordern und das Overblocking-Risiko unkalkulierbar machen [Ma22]. Bei A1 und Drei konnten keine spezifischen Informationen bezüglich Netzsperren auf deren Webseiten gefunden werden.

Die Analyse der Citizen Lab Testlisten ergab insgesamt sieben Einträge für Österreich, von denen jedoch zwei Einträge redundant zu den bereits aus den Open Data identifizierten Domains sind. Zwei weitere Einträge fielen unter das nicht berücksichtigte EU-Sanktionsverbot. Die übrigen drei Einträge erschienen irrtümlich, da sie tatsächlich von keiner Sperre betroffen sind. Diese Einträge umfassen `de.wiktionary.org`, `hu.wikipedia.org` und `https://www.sozialministerium.at/Informationen-zum-Coronavirus/Neuartiges-Coronavirus-(2019-n` abrufbar unter: `https://github.com/citizenlab/test-lists/blob/master/lists/at.csv` (abgerufen am 27.04.2024).

Um die Wirksamkeit der Umgehungsmethoden umfassend zu bewerten, wird jeder Test speziell auf die Liste der von den jeweiligen ISPs gesperrten Webseiten zugeschnitten. Diese spezifischen Listen sind entscheidend für die Evaluierung, da sie die tatsächlichen Bedingungen widerspiegeln, unter denen Internetnutzer in Österreich auf Inhalte zugreifen.

4.3. Schritt 1: Durchführung der Überprüfung der gesperrten Domains

Das Ziel dieses Abschnitts besteht darin, zu überprüfen, ob Domains tatsächlich gesperrt sind. Hierzu wird ermittelt, ob die über die ISP-DNS-Resolver erhaltenen IP-Adressen mit den über autoritative Nameserver ermittelten IPs übereinstimmen. Die autoritativen Nameserver sind dabei jene Server, die direkt von der Top-Level-Domain (TLD) verwaltet werden und die originalen Einträge der Domains besitzen. Im Gegensatz dazu sind die DNS-Resolver der ISPs rekursive Resolver, die ihre Daten von diesen autoritativen Quellen beziehen. Es wird ein Python-Skript eingesetzt, welches die Schritte zur Ermittlung der IP-Adressen durchführt und diese vergleicht. Das Python-Skript ist im Anhang B zu finden.

4.3.1. Ermittlung der IPs über autoritative Nameserver

Der Prozess der DNS-Sperrung beginnt mit einer WHOIS-Abfrage, um die Top-Level-Domain (TLD) einer bestimmten Domain zu ermitteln. Die WHOIS-Informationen enthalten wichtige Details über die TLD, die wiederum verwendet werden, um die autoritativen Nameserver zu identifizieren, die für die TLD zuständig sind [Mo20].

Diese autoritativen Nameserver sind die primären Quellen für die A-Records der Domain und liefern die genauesten, nicht manipulierten Informationen. Das für die WHOIS-Abfrage verwendete Skript (siehe Listing 4.1) und Code-Elemente aus einem Blogeintrag auf `binarytides.com` [Ka24a], extrahiert die TLD-Informationen und verwendet diese, um die entsprechenden autoritativen Nameserver zu ermitteln. Diese Schritte stellen sicher, dass die ermittelten IP-Adressen direkt von den autoritativen Quellen stammen und somit frei von ISP-Manipulationen sind.

Die WHOIS-Ausgabe, die im Listing 4.1 beispielhaft für `fernfh.ac.at` dargestellt wird, ist von zentraler Bedeutung, da sie entscheidende Informationen über die Domains liefert, die für weitere Untersuchungen herangezogen werden. Sie zeigt unter anderem den WHOIS-Server `whois.nic.at`, der für detaillierte Informationen über die Domain `fernfh.ac.at` konsultiert wird.

Neben allgemeinen Daten zur Domain und zur verwaltenden Organisation werden auch spezifische Informationen zu den autoritativen Nameservern aufgelistet. Die aufgelisteten Nameserver wie `D.NS.AT`, `J.NS.AT` und andere sind für die Verwaltung der DNS-Daten der Domain zuständig. Die Einträge enthalten sowohl IPv4- als auch IPv6-Adressen.

Listing 4.1: Beispiel WHOIS für `fernfh.ac.at`

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
```

```
4
5  refer:        whois.nic.at
6
7  domain:       AT
8
9  organisation: nic.at GmbH
10 address:      Jakob-Haringer-Strasse 8
11 address:      Salzburg 5020
12 address:      Austria
13
14 contact:      administrative
15 name:         Geschaeftsfuehrer NIC.AT
16 organisation: nic.at GmbH
17 address:      Jakob-Haringer-Strasse 8
18 address:      Salzburg 5020
19 address:      Austria
20 phone:        +43 662 4669-14
21 fax-no:       +43 662 4669-19
22 e-mail:       gf@nic.at
23
24 contact:      technical
25 name:         Technik NIC.AT
26 organisation: nic.at GmbH c/o Vienna University Computer Center
27 address:      Universitaetsstrasse 7
28 address:      Vienna 1010
29 address:      Austria
30 phone:        +43 1 4277 14035
31 fax-no:       +43 1 4277 9140
32 e-mail:       tech-nic-at@nic.at
33
34 nserver:      D.NS.AT 2a02:568:20:1:0:0:0:d 81.91.161.98
35 nserver:      J.NS.AT 194.146.106.50 2001:67c:1010:12:0:0:0:53
36 nserver:      N.NS.AT 2a02:568:281:0:0:0:0:130 81.91.173.130
37 nserver:      NS1.UNIVIE.AC.AT 2001:628:2030:4301:0:0:0:2
       78.104.144.2
38 nserver:      NS2.UNIVIE.AC.AT 192.92.125.2 2001:678:1c:0:0:0:0:2
39 nserver:      NS9.UNIVIE.AC.AT 194.0.10.100 2001:678:d:0:0:0:0:
       cafe
40 nserver:      R.NS.AT 194.0.25.10 2001:678:20:0:0:0:0:10
41 nserver:      U.NS.AT 185.102.12.2 2a02:850:ffff:0:0:0:0:2
42 ds-rdata:     1253 13 2
       ba17c1bacb3fb49f7760ad1f7e71e17ab39ee0df3e9d3bf23fd3d70d6cf1719e

43 ds-rdata:     18942 13 2
```

```
ae5f0bd73c8f48f3d55cdc4070f9407873176c364de4bc92bf96887685e6e55f

whois:          whois.nic.at

status:         ACTIVE
remarks:        Registration information: http://www.nic.at/

created:        1988-01-20
changed:        2023-04-25
source:         IANA
```

Nachdem der Top Level Domain (TLD) Nameserver durch eine WHOIS-Abfrage wie im Listing 4.1 dargestellt ermittelt wurde, wird dieser verwendet, um die autoritativen Nameserver für die spezifische Domain zu ermitteln. Dieser Vorgang ist für die korrekte Identifizierung der IP-Adressen einer Domain entscheidend. Die Ermittlung der autoritativen Nameserver erfolgt über einen DNS-Lookup-Befehl. Im Falle der Domain `fernfh.ac.at` wird beispielsweise der Nameserver `d.ns.at` verwendet, der zuvor durch die WHOIS-Abfrage 4.1 ermittelt wurde. Der entsprechende Befehl, der auch im Python-Skript B implementiert ist, lautet `nslookup -type=NS fernfh.ac.at d.ns.at`. Die Ausgabe dieses Befehls, die im Listing 4.2 gezeigt wird, enthält die autoritativen Nameserver. Das Listing 4.2 zeigt, dass `fernfh.ac.at` von den autoritativen Nameservern `ns1.edis.global.` und `ns2.edis.global.` verwaltet wird. Diese Nameserver sind die primären Quellen für die DNS-Daten der Domain und daher entscheidend für die Ermittlung der tatsächlichen, nicht manipulierten IP-Adressen.

Listing 4.2: Beispiel autoritativer Nameserver Ermittlung für `fernfh.ac.at`

```
Server:         d.ns.at
Address:        81.91.161.98#53

Non-authoritative answer:
*** Can't find fernfh.ac.at: No answer

Authoritative answers can be found from:
fernfh.ac.at    nameserver = ns1.edis.global.
fernfh.ac.at    nameserver = ns2.edis.global.
```

Ein konkretes Beispiel für die Ermittlung der IP durch die Verwendung des autoritativen

Nameservers wird durch die Abfrage der Domain `fernfh.ac.at` mittels des autoritativen Nameservers `ns1.edis.global.` illustriert. Der entsprechende Befehl, der verwendet wird, ist `dig @ns1.edis.global. fernfh.ac.at`. Die Ausgabe ist im Listing 4.3 dargestellt. In der Antwort-Sektion wird die tatsächliche IP-Adresse `5.132.190.70` für die Domain `fernfh.ac.at` aufgeführt. Diese IP ist die offizielle Adresse, die auf den autoritativen Servern registriert ist.

Listing 4.3: Beispiel IP über autoritativen Nameserver für `fernfh.ac.at` ermitteln

```
; <<>> DiG 9.10.6 <<>> @ns1.edis.global. fernfh.ac.at
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30205
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
    1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1400
;; QUESTION SECTION:
;fernfh.ac.at.                  IN      A

;; ANSWER SECTION:
fernfh.ac.at.           600     IN      A       5.132.190.70

;; Query time: 55 msec
;; SERVER: 192.174.68.12#53(192.174.68.12)
;; WHEN: Sun May 05 13:39:57 CEST 2024
;; MSG SIZE  rcvd: 57
```

4.3.2. Ermitteln ISP-Resolver IP-Adresse und Vergleich der IP-Adressen

Nach der Ermittlung der IP-Adressen über die autoritativen Nameserver, die als zuverlässigste und unveränderte Quelle für die A-Records einer Domain gelten, werden diese mit den vom DNS-Resolver des ISP gelieferten IP-Adressen verglichen. Dieser Vergleich erfolgt durch DNS-Abfragen, die standardmäßig über den im Netz der Nutzer*innen konfigurierten DNS-Server des ISP durchgeführt werden. Für diese Abfragen wird kein bestimmter Nameserver angegeben, sodass automatisch der vom ISP voreingestellte DNS-

Server verwendet wird. Alle ermittelten IPs werden protokolliert und anschließend verglichen. Im Python-Skript (siehe Anhang B), das diese Abfragen durchführt, wird in der Ausgabe, die eine CSV-Datei ist, in der Spalte `DNS-Sperre` das Ergebnis des Vergleichs festgehalten. Wenn mindestens eine IP-Adresse aus beiden Abfragen übereinstimmt, wird davon ausgegangen, dass keine DNS-Sperre vorliegt. Andernfalls wird von einer DNS-Sperre ausgegangen.

Das Python-Skript (siehe Anhang B), das diesen gesamten Prozess durchführt, stellt sicher, dass die Untersuchung der DNS-Sperren auf präzisen und unverfälschten Daten beruht. Durch den Vergleich dieser Daten mit denen, die durch ISP-Resolver erhalten wurden, kann effektiv festgestellt werden, ob und in welchem Ausmaß DNS-Sperren in Österreich Anwendung finden.

Die korrekte und unmanipulierte Ermittlung der IP-Adressen ermöglicht es, die Wirksamkeit von Maßnahmen zur Umgehung von DNS-Sperren zu testen und trägt somit zur Genauigkeit und Zuverlässigkeit der Forschungsergebnisse bei.

4.3.3. Ergebnisse Schritt 1

Der in diesem Abschnitt beschriebene Prozess stellt eine systematische und technisch fundierte Methode dar, um DNS-Sperren zu überprüfen. Dieser Ansatz trägt wesentlich zur Genauigkeit und Zuverlässigkeit der Forschungsergebnisse bei.

Die Ausgabe des Skripts werden in einer CSV-Datei mit folgenden Spalten festgehalten:

Listing 4.4: Spalten .CSV-Datei Ausgabe für Schritt 1

```
1 Timestamp;Domain;Whois-Nameserver;Authorative-Nameserver;Auth.-
    Nameserver IP-Adressen;ISP-Nameserver IP-Adressen;DNS-Sperre
```

Es gibt je einen Zeileneintrag für jede Domain aus der Liste der Zielwebseiten, die für die Untersuchung festgelegt wurden (siehe Anhang A). Die Ausgaben sind in den Anhängen zu finden.

- Anhang C.1 für A1
- Anhang C.2 für Drei
- Anhang C.3 für Magenta

Es ergibt sich folgende Anzahl an tatsächlichen Webseiten bzw. Domains, die einer DNS-Sperre unterliegen (Liste Zielwebseiten siehe Anhang A):

- A1: Tatsächlich 155 gesperrte Domains von 159 aus der Liste der Zielwebseiten.

- Drei: Tatsächlich 182 gesperrte Domains von 184 aus der Liste der Zielwebseiten.
- Magenta: Tatsächlich 176 gesperrte Domains von 179 aus der Liste der Zielwebseiten.
- Gesamt: Tatsächlich 513 gesperrte Domains von Gesamt 522 aus der Liste der Zielwebseiten.

4.4. Umgehungsmethode 1: IP-Adresse verwenden

In der theoretischen Diskussion um Netzsperren erscheint die Verwendung von IP-Adressen zur Umgehung von DNS-Sperren durch direkte IP-Adressanfragen, wie im Abschnitt 2.4.1 dargestellt, als geeignet. In der Praxis stößt dieser Ansatz jedoch auf erhebliche technische und sicherheitsrelevante Probleme, die seine Anwendung insbesondere im Kontext von HTTPS-Anfragen stark einschränken.

Es zeigt sich, dass zwar Zugriffe erfolgen, die Verwendung der IP-Adresse jedoch, nicht geeignet ist. Das erstellte Python-Skript, welches zur Überprüfung der Umgehungsmethode (siehe Anhang D) dient, führt eine systematische Überprüfung der Erreichbarkeit von Webseiten über ihre IP-Adressen durch, indem es sowohl HTTP- als auch HTTPS-Anfragen an die jeweilige IP-Adresse sendet. Die IP-Adressen werden aus der Ausgabe von Schritt 1 (siehe Anhang A) verwendet, welche von den autoritativen Nameservern stammen. Für jede Anfrage werden der HTTP- und HTTPS-Statuscode sowie die daraus resultierende Erreichbarkeit dokumentiert.

Die Funktion `test_access_via_ip`, zu sehen in Listing 4.5, ist zentral für die Untersuchung der Erreichbarkeit von Webseiten über IP-Adressen und spielt eine wichtige Rolle bei der Bewertung der Wirksamkeit von Methoden zur Umgehung von DNS-Sperren. Sie nimmt zwei Hauptparameter entgegen: `domain`, den Domainnamen der zu testenden Website, und `ip_addresses`, eine durch Beistrichen getrennte Liste von IP-Adressen. Für jede IP-Adresse führt die Funktion systematische HTTP- und HTTPS-Anfragen durch. Die korrekte Einbindung des Host-Headers ist entscheidend, um sicherzustellen, dass der Server das richtige SSL/TLS-Zertifikat zuweist und somit den korrekten Inhalt über IP-Adressen ausliefert. Trotz dieser Maßnahme zeigt es sich in der Praxis, dass es zu SSL/TLS-Fehlern beim Aufrufen von Webseiten mittels IP kommt, was die Herausforderungen dieser Umgehungsmethode verdeutlicht.

Jede Anfrage wird protokolliert, wobei Ergebnisse wie Zeitstempel, getestete Domain, IP-Adresse und erhaltene HTTP- bzw. HTTPS-Statuscodes gespeichert werden. Fehler, insbesondere SSL/TLS-Fehler, werden protokolliert, um eine gründliche Analyse möglicher Schwachstellen zu ermöglichen. Die Ergebnisse aller Tests werden in einer .csv Datei zusammengefasst und bieten eine solide Grundlage für die anschließende Auswertung der Erreichbarkeit über die getesteten IP-Adressen.

Durch die Anwendung dieser Funktion können die Grenzen und Potentiale von der IP Verwendung als Umgehungsmethoden systematisch evaluiert und dokumentiert werden.

Listing 4.5: Auszug Python-Skript für Umgehungsmethode 1: IP-Adresse verwenden

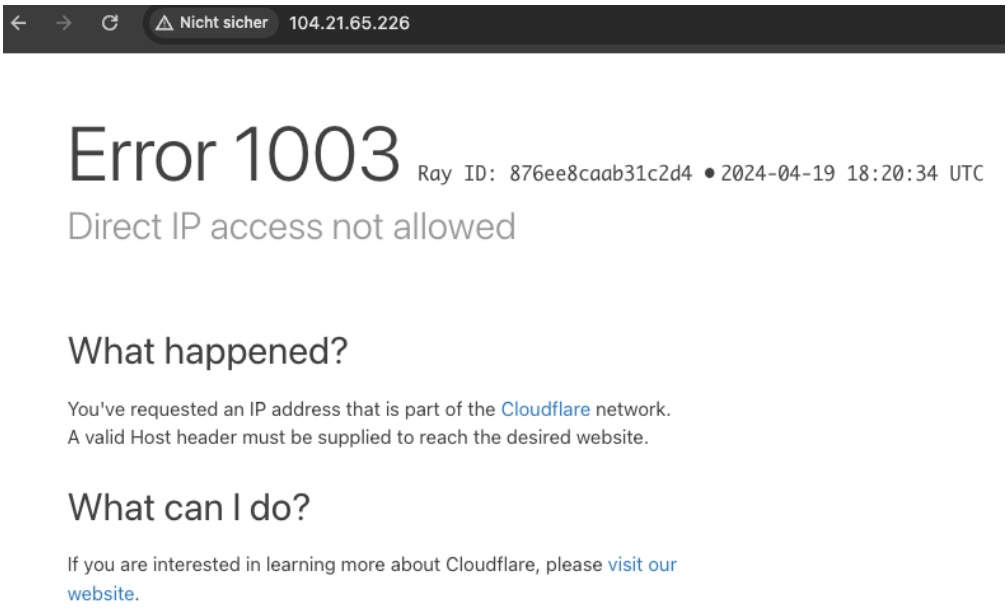
```
# Funktion zum Testen der Erreichbarkeit einer Domain über deren IP-Adresse
def test_access_via_ip(domain, ip_addresses):
    results_list = []  # Liste zum Speichern der Ergebnisse jeder getesteten IP
    for ip_address in ip_addresses.split(','):  # Zerlegt die IP-Adressen-String und iteriert über jede IP-Adresse
        ip_address = ip_address.strip()  # Entfernt überflüssige Leerzeichen
        results = {
            'Timestamp': datetime.now().strftime('%Y-%m-%d %H:%M:%S'),  # Setzt den aktuellen Zeitstempel
            'Domain': domain,  # Die Domain, die getestet wird
            'IP': ip_address,  # Die IP-Adresse, die getestet wird
            'Erreichbar über HTTP?': 'Nein',  # Initialisiert den HTTP-Erreichbarkeitsstatus als 'Nein'
            'HTTP Statuscode': '',  # Leeres Feld für den HTTP-Statuscode
            'Erreichbar über HTTPS?': 'Nein',  # Initialisiert den HTTPS-Erreichbarkeitsstatus als 'Nein'
            'HTTPS Statuscode': ''  # Leeres Feld für den HTTPS-Statuscode
        }
        # Dictionary zur Abbildung von Protokollen zu ihren Ergebnisschlüsseln im results-Dictionary
        protocols = {'http': ('Erreichbar über HTTP?', 'HTTP Statuscode'), 'https': ('Erreichbar über HTTPS?', 'HTTPS Statuscode')}
        for protocol in protocols:  # Testet sowohl HTTP als auch HTTPS
            url = f"{protocol}://{ip_address}"  # Bildet die URL
            try:
                # Führt den GET-Request aus mit einem spezifischen Host-Header
                response = requests.get(url, headers={'Host': domain}, timeout=10, verify=True)
                status_code = response.status_code  # Speichert den Statuscode der Antwort
                results[protocols[protocol][1]] = f"{status_code} {response.reason}"  # Speichert Statuscode und Grund
                if status_code == 200:
                    results[protocols[protocol][0]] = 'Ja'  #
```

```
    Setzt den Erreichbarkeitsstatus auf 'Ja', wenn 200 OK
26                  else:
27                      results[protocols[protocol][0]] = 'Nein'
28              except SSLError:
29                  results[protocols[protocol][1]] = "SSL/TLS Error"
     # Speichert einen SSL-Fehler
30                  logging.warning(f"SSL/TLS error encountered while
    accessing {url}")  # Loggt eine Warnung bei SSL-Fehlern
31              except RequestException as e:
32                  error_message = " ".join(str(e).split()[:2])  #
    Reduziert die Fehlermeldung auf die ersten zwei Wörter
33                  results[protocols[protocol][1]] = f"Error: {
    error_message}"  # Speichert die Fehlermeldung
34                  logging.error(f"Request failed for {url}: {
    error_message}")  # Loggt einen Fehler bei Request-Fehlern
35
36          results_list.append(results)  # Fügt die Ergebnisse der
    Liste hinzu
37      return results_list  # Gibt die Liste der Ergebnisse zurück
```

Folgenden Informationen werden in eine CSV-Datei geschrieben:

- Timestamp: Der genaue Zeitpunkt der Anfrage.
- Domain: Die Domain, die getestet wird.
- IP: Die IP-Adresse, die für die Anfrage verwendet wird.
- Erreichbar über HTTP?: Ein Indikator, der angibt, ob die HTTP-Anfrage erfolgreich war (Ja) oder nicht (Nein).
- HTTP Statuscode: Der Statuscode der HTTP-Anfrage.
- Erreichbar über HTTPS?: Ein Indikator, der angibt, ob die HTTPS-Anfrage erfolgreich war (Ja) oder nicht (Nein).
- HTTPS Statuscode: Der Statuscode der HTTPS-Anfrage oder eine Kurzbeschreibung des Fehlers, z. B. SSL/TLS Error.

Diese Methode ermöglicht es, systematisch zu evaluieren, ob die direkte IP-Anfrage eine potenzielle Lösung zur Umgehung von DNS-Sperren darstellen kann. Des Weiteren wurde in Praxistests versucht, die IP-direkt in die Browser-Suchleiste einzugeben, wie Abbildung 4.3 zeigt. Beim virtuellen Hosting kann der Zugriff auf eine Website über deren IP-Adresse ohne zugehörigen Hostnamen dazu führen, dass der Server nicht die gewünschte Website lädt, sondern eine Fehlermeldung ausgibt oder auf eine Standard- oder Platzhalterseite



Abbildungsverzeichnis 4.3.: Abrufen einer Website über deren IP-Adresse, direkter IP-Aufruf nicht gestattet.

umleitet. Dies geschieht, weil der Server ohne den spezifischen Hostnamen nicht feststellen kann, welche der gehosteten Webseiten der Anfrage entspricht.

Folgend werden noch die Herausforderungen, die sich durch das Aufrufen einer Website mit der IP-Adresse ergeben, aufgezeigt. Der Test hat diese bestätigt und das Verwenden der IP-Adresse, um DNS-Sperren zu umgehen, ist damit nicht geeignet.

Herausforderungen bei HTTPS-Anfragen
Die Sicherheit von HTTPS-Verbindungen basiert maßgeblich auf dem SSL/TLS-Zertifikat, welches die Authentizität des Servers bestätigt. Diese Zertifikate werden typischerweise auf Domainnamen, nicht auf IP-Adressen, ausgestellt. Folglich resultiert eine HTTPS-Anfrage an eine IP-Adresse in einem Zertifikatsfehler, da der im Zertifikat spezifizierte Domainname nicht mit der angeforderten IP übereinstimmt. Des Weiteren ermöglicht virtuelles Hosting die Verwaltung mehrerer SSL/TLS-Zertifikate auf einem einzigen Server. Während des TLS-Handshake muss der Client den gewünschten Hostnamen übermitteln, damit der Server das korrekte Zertifikat auswählen kann. Bei Anfragen, die sich direkt an eine IP-Adresse richten, ist es also unwahrscheinlich, dass der Server ein passendes Zertifikat zuordnen kann, was zu weiteren Fehlern im Prozess führt [Lö23].

Herausforderungen bei HTTP-Anfragen
Obwohl HTTP-Anfragen die SSL/TLS-Zertifikatsproblematik nicht haben, da kein SSL/TLS verwendet wird, sind sie aus Sicherheitsperspektive nicht unproblematisch. HTTP-Anfragen sind unverschlüsselt und können daher leicht abgefangen oder manipuliert werden, was sie für Abhör- und Man-in-the-Middle-Angriffe anfällig macht, da keine Gewährleistung für die Integrität und Vertraulichkeit der Datenübertragung besteht. Viele Webseiten implementieren Maßnahmen, die den Datenverkehr automatisch von HTTP auf HTTPS

umleiten oder die Nutzung von HTTPS erzwingen. Die genannten Mechanismen verhindern effektiv die Nutzung von HTTP als zuverlässige Alternative für den Zugang zu beschränkten Inhalten [Ga24].

Deshalb ist die Nutzung von IP-Adressen zur Umgehung von DNS-Sperren ist für HTTPS-Anfragen aufgrund von SSL/TLS-Zertifikatsproblemen keine praktikable Methode und wird auch für HTTP-Anfragen aufgrund von erheblichen Sicherheitsbedenken nicht empfohlen. In kontrollierten Umgebungen kann die SSL/TLS-Validierung für Entwicklungs- und Testzwecke deaktiviert werden, doch birgt dies in Produktionsumgebungen unvertretbare Risiken.

Die Tests wurden mit SIM-Karten und damit in der Netzumgebung der ausgewählten ISPs durchgeführt. Jeder Testlauf wurde dokumentiert und die Ausgabe ist in den Anhängen zu finden:

- Anhang E.1 für A1
- Anhang E.2 für Drei
- Anhang E.3 für Magenta

Die Ergebnisse werden in Abschnitt 5.1.1 präsentiert.

4.5. Umgehungsmethode 2: DNS-Resolver ändern

In diesem Abschnitt wird eine Methode zur Umgehung von DNS-Sperren diskutiert, die sich durch den Wechsel des DNS-Resolvers auszeichnet. Die Effektivität verschiedener öffentlicher DNS-Resolver wie Google Public DNS, Cloudflare DNS und OpenNIC wird untersucht, um festzustellen, ob sie eine zuverlässige Umgehung von DNS-basierten Zugriffsbeschränkungen ermöglichen.

Die Wahl fiel auf den Google Public DNS (8.8.8.8) [Go24], den Cloudflare DNS (1.1.1.1) [Cl24] und OpenNIC (37.252.191.197) [Op24] als Vergleichs-Resolver gegenüber dem ISP-Resolver. Diese öffentlichen DNS-Dienste sind bekannt für ihre Unabhängigkeit von lokalen ISPs, was bedeutet, dass sie potenziell nicht den lokalen Zensurrichtlinien unterliegen. Diese Eigenschaft macht sie zu idealen Kandidaten für die Überprüfung ihrer Fähigkeit, DNS-Sperren zu umgehen. In dieser Analyse wurde OpenNIC in die Tests einbezogen, um seine Effektivität im Vergleich zu etablierteren Diensten wie Google und Cloudflare zu bewerten. OpenNIC ist ein alternativer DNS-Resolver, der sich durch seine Unabhängigkeit von typischen kommerziellen Routen auszeichnet. OpenNIC zielt darauf ab, eine weniger zentralisierte Version des Internets zu fördern [Op24].

Im Rahmen der Untersuchung wurde ein Python-Skript (siehe Anhang F) entwickelt, das automatisch DNS-Abfragen über diese drei Resolver ausführt und die Ergebnisse mit den autoritativen Nameserver-IPs vergleicht, die in Schritt 1 (siehe 4.3) identifiziert wurden.

Nur Domains, für die eine DNS-Sperre laut Methode in Schritt 1 existiert, werden in die Analyse einbezogen.

Die spezifischen Parameter und Funktionen des Skripts umfassen (siehe Listing 4.6):

- **DNS-Abfragefunktion** (`query_dns`): Diese Funktion nimmt eine Domäne und einen DNS-Server als Argumente und führt den Befehl `dig` aus, um die DNS-Abfrage durchzuführen. Sie misst die Dauer der Abfrage und speichert die vom DNS-Resolver zurückgegebenen IP-Adressen. Die Funktion gibt die gesammelten IP-Adressen und die Antwortzeit zurück.
- **Vergleichsfunktion** (`compare_dns_results`): Diese Funktion führt einen Vergleich zwischen den IP-Adressen durch, die von einem DNS-Resolver zurückgegeben wurden, und den bekannten IP-Adressen, die von autoritativen Nameservern bereitgestellt werden. Sie bestimmt, ob eine DNS-Sperre effektiv umgangen wurde, indem sie überprüft, ob es eine Überschneidung zwischen beiden IP-Adresssets gibt.

Listing 4.6: Auszug Python-Skript für Umgehungsmethode 2: DNS-Resolver ändern.

```
#Führt eine DNS-Abfrage für die angegebene Domain über den spezifizierten DNS-Server aus.
def query_dns(domain, dns_server):
    start_time = time.time()  # Startzeit der Messung
    try:
        # Führt den 'dig'-Befehl aus und fängt die Ausgabe auf.
        output = subprocess.run(['dig', '+short', '@' + dns_server, domain], capture_output=True, text=True)
        duration = time.time() - start_time  # Berechnet die Dauer der Anfrage
        # Überprüft, ob der Prozess erfolgreich war und gibt die Antwort als Liste zurück.
        if output.returncode == 0 and output.stdout.strip():
            return output.stdout.strip().split('\n'), duration
    except Exception as e:
        # Gibt eine Fehlermeldung aus, wenn ein Fehler auftritt.
        print(f"Fehler bei DNS-Anfrage für {domain} über {dns_server}: {e}")
    # Gibt eine leere Liste zurück, wenn keine Daten gefunden wurden oder ein Fehler auftrat.
    return [], time.time() - start_time

#Vergleicht zwei Listen von IP-Adressen und gibt zurück, ob eine DNS-Sperre umgangen wurde.
def compare_dns_results(known_ips, new_ips):
```

```
19      # Konvertiert die Liste der bekannten IPs in ein Set, um
    eindeutige und schnelle Vergleichsoperationen zu ermöglichen.
20      known_set = set(known_ips)
21      # Konvertiert die Liste der neuen, überprüften IPs in ein Set.
22      new_set = set(new_ips)
23      # Überprüft, ob eine direkte Überschneidung zwischen den
    bekannten IPs und den neuen IPs besteht.
24      if known_set.intersection(new_set):
25          return "Ja"  # Gibt "Ja" zurück, wenn mindestens eine IP
    in beiden Sets übereinstimmt.
26      # Überprüft, ob die ersten drei Oktette der IP-Adressen ü
    bereinstimmen, was auf eine geografische Nähe hindeuten könnte.
27      elif any(ip.rsplit('.', 1)[0] == new_ip.rsplit('.', 1)[0] for
    ip in known_ips for new_ip in new_ips):
28          return "Ja-Geolokalisiert"  # Gibt "Ja-Geolokalisiert" zur
    ück, wenn IPs geografisch ähnlich sind.
29      else:
30          return "Nein"  # Gibt "Nein" zurück, wenn keine der obigen
     Bedingungen erfüllt ist.
```

Die Ergebnisse werden in eine CSV-Datei geschrieben, die Spalten dieser Datei siehe Listing 4.7.

Listing 4.7: Spalten CSV-Datei Ausgabe für Umgehungsmethode 2: DNS-Resolver ändern

```
1 Timestamp;Domain;Authorative Nameserver IPs;Google IPs;Google
    Antwortzeit;Google DNS-Sperre umgangen?;Cloudflare IPs;
    Cloudflare Antwortzeit;Cloudflare DNS-Sperre umgangen?;OpenNIC
    IPs;OpenNIC Antwortzeit;OpenNIC DNS-Sperre umgangen?
```

Ein kritischer Aspekt, der in der Analyse berücksichtigt werden muss, ist das Caching von DNS-Anfragen. DNS-Resolver speichern Antworten auf frühere Anfragen, um die Antwortzeit zu verbessern. Dieses Verhalten kann jedoch dazu führen, dass veraltete oder manipulierte Daten verwendet werden, was die Wirksamkeit der Umgehungsmethode beeinflusst. Verschiedene Resolver haben unterschiedliche Cache-Ablaufzeiten und -Strategien, was bedeutet, dass ein Resolver möglicherweise aktuellere oder unterschiedliche Informationen liefert als ein anderer. Darüber hinaus können sich IP-Adressen aufgrund geografischer Unterschiede unterscheiden, insbesondere da DNS-Dienste

geografisch verteilte Server verwenden können, die je nach Standort der Nutzer*innen unterschiedliche IP-Adressen zurückgeben können. Um geografisch bedingte Unterschiede zu berücksichtigen, wurde in der Funktion `compare_dns_results` eine erweiterte Prüfung implementiert. Diese prüft nicht nur, ob die IP-Adressen exakt übereinstimmen, sondern auch, ob die ersten drei Oktette der IP-Adressen übereinstimmen. Dies ermöglicht die Identifizierung von partiellen Übereinstimmungen, die auf geografische Variationen hinweisen, und erweitert somit unser Verständnis darüber, wie geografische Aspekte die DNS-Auflösung beeinflussen können.

Diese partiellen Übereinstimmungen, die als `Ja-Geolokalisiert` gekennzeichnet werden, tragen dazu bei, ein vollständigeres Bild der Effektivität von DNS-Resolvern zu zeichnen. Die Berücksichtigung dieser geolokalisierten Antworten ist entscheidend für das Verständnis der Herausforderungen, die mit geografischen Unterschieden verbunden sind, und unterstreicht die Notwendigkeit, mehrere Resolver zu testen.

Die Tests wurden mit SIM-Karten und damit in der Netzumgebung der ausgewählten ISPs durchgeführt. Jeder Testlauf wurde dokumentiert und die Ausgabe ist in den Anhängen zu finden:

- Anhang G.1 für A1
- Anhang G.2 für Drei
- Anhang G.3 für Magenta

Die Ergebnisse werden in Abschnitt 5.1.2 präsentiert.

4.6. Umgehungsmethode 3: VPN

Die Verwendung eines VPN (Virtual Private Network) ist eine weitere Möglichkeit, DNS-basierte Zugriffsbeschränkungen zu umgehen. In diesem Abschnitt wird untersucht, wie effektiv die Verwendung eines VPN-Dienstes, insbesondere Psiphon, zur Umgehung von DNS-Sperren sein kann. Psiphon [Ps24] ist eine Software, die entwickelt wurde, um Internetzensur zu umgehen, indem sie Nutzern den Zugriff auf Inhalte über eine verschlüsselte Verbindung ermöglicht. Dazu werden verschiedene Technologien wie VPN, SSH und HTTP-Proxy verwendet.

Für diese Untersuchung wurde Psiphon ausgewählt, da es weit verbreitet ist und eine kostenlose Version zur Verfügung steht, was es zu einem beliebten Werkzeug in der Forschung macht. Psiphon verwendet automatisch einen durch die VPN-Verbindung vorgegebenen DNS-Resolver, wodurch der lokale DNS-Resolver des ISP umgangen wird. Dies ist wichtig, da der ISP nicht in der Lage ist, DNS-Anfragen zu überwachen oder zu protokollieren, was eine potentielle Umgehung von DNS-Sperren ermöglicht.

Um DNS-Abfragen während einer aktiven VPN-Verbindung durchführen zu können, wurde ein Python-Skript (siehe H) entwickelt. Dieses Skript ermittelt die vom VPN-DNS-Resolver

aufgelösten IP-Adressen für Domains, von denen bekannt ist, dass sie einer DNS-Sperre unterliegen (siehe Schritt 1 4.3). Dabei unterscheidet sich das Skript gegenüber dem bei Umgehungsmethode 2 (DNS-Resolver ändern) in der Funktion textttquery_dns (siehe Listing 4.8), dass kein spezifischer DNS-Resolver angegeben wird, da der Resolver durch die VPN-Software konfiguriert wird.

Listing 4.8: Auszug Python-Skript für Umgehungsmethode 3: VPN

```
#Führt eine DNS-Abfrage für die angegebene Domain über den Netzwerk-DNS-Resolver (bei VPN-Verbindung, Resolver von VPN) aus.
def query_dns(domain):
    start_time = time.time()
    try:
        # Führt den 'dig'-Befehl aus, ohne einen spezifischen DNS-Server zu spezifizieren.
        output = subprocess.run(['dig', '+short', domain], capture_output=True, text=True)
        duration = time.time() - start_time
        if output.returncode == 0 and output.stdout.strip():
            return output.stdout.strip().split('\n'), duration
    except Exception as e:
        print(f"Fehler bei DNS-Anfrage für {domain} über den Netzwerk-DNS-Resolver: {e}")
    return [], time.time() - start_time
```

Die Ergebnisse dieser Abfragen werden in einer CSV-Datei gespeichert, die Spalten dieser Datei siehe Listing 4.9.

Listing 4.9: Spalten CSV-Datei Ausgabe für Umgehungsmethode 3: VPN

```
Timestamp; Domain; Aufgelöste IP-Adresse von Authorative Nameserver; Aufgelöste IP-Adresse bei aktiver VPN-Verbindung; Antwortzeit VPN-Verbindung Resolver; DNS-Sperre umgangen mit VPN?
```

Die Verwendung eines Virtual Private Network (VPN) bietet mehrere entscheidende

Vorteile, insbesondere in Bezug auf Sicherheit, Privatsphäre und Zugangsfreiheit, wie bereits in der Theorie diskutiert (siehe 2.4.3). Ein VPN verschlüsselt den gesamten Datenverkehr, einschließlich DNS-Anfragen. Dies erhöht die Sicherheit in öffentlichen Netzen erheblich und schützt effektiv vor Man-in-the-Middle-Angriffen. Zudem verbirgt ein VPN die tatsächliche IP-Adresse der Nutzer*innen, sodass die Anonymität gegenüber den besuchten Webseiten und Diensten gewahrt bleibt. Darüber hinaus ermöglicht das Routing des Datenverkehrs über Server in verschiedenen geografischen Regionen die Umgehung geografischer Sperren und Zensur, was den Zugang zu globalen Ressourcen erleichtert.

Trotz dieser Vorteile gibt es auch spezifische Herausforderungen bei der Verwendung von VPNs. Die Konsistenz der IP-Adressen kann variieren, da unterschiedliche VPN-Server unterschiedliche IPs liefern können. Dies kann zu variierenden Ergebnissen führen, besonders wenn Serverstandorte wechseln. Für diese Untersuchung wurde daher ein VPN-Server in Österreich verwendet, um die Konsistenz der Testumgebung zu gewährleisten.

Die Tests wurden mit SIM-Karten und damit in der Netzumgebung der ausgewählten ISPs durchgeführt. Jeder Testlauf wurde dokumentiert und die Ausgabe ist in den Anhängen zu finden:

- Anhang I.1 für A1
- Anhang I.2 für Drei
- Anhang I.3 für Magenta

Die Ergebnisse werden in Abschnitt 5.1.3 präsentiert.

4.7. Umgehungsmethode 4: Tor

In diesem Abschnitt wird die Effektivität von Tor bei der Umgehung von DNS-basierten Zugangsbeschränkungen untersucht. Tor [To24] ist ein Netzwerk zur Anonymisierung von Verbindungsdaten, das den Datenverkehr über mehrere Knoten leitet, um die Quelle und das Ziel der Daten zu verschleiern.

Für diese Untersuchung wurde Tor ausgewählt, da es nicht nur die IP-Adresse der Nutzer*innen verbirgt, sondern auch die Möglichkeit bietet, DNS-Anfragen über sein Netzwerk zu leiten. Dies verhindert, dass der ISP die DNS-Anfragen überwachen oder manipulieren kann, was eine potentielle Umgehung von DNS-Sperren ermöglicht.

Um DNS-Abfragen während einer aktiven Tor-Verbindung durchführen zu können, wurde ein Python-Skript (siehe Anhang J) entwickelt. Dieses Skript verwendet die Tor-Bibliothek, um eine sichere und anonyme Verbindung aufzubauen, bevor DNS-Anfragen gesendet werden. Das Skript liefert somit wichtige empirische Daten für die Forschung über Internetzensur und die Wirksamkeit von Anonymisierungstools. Zur Ermittlung der IPs über Tor wird `tor-resolve` verwendet, ein Tool speziell für die Auflösung von DNS über

Tor, welches sicherstellt, dass alle Anfragen anonym und durch das Tor-Netzwerk geroutet werden. Die Funktion zur Auflösung der IP ist in Listing 4.10 dargelegt.

Listing 4.10: Auszug Python-Skript für Umgehungsmethode 4: Tor

```
#Verwendet tor-resolve, um eine DNS-Abfrage für die angegebene Domain über Tor auszuführen.
def tor_resolve(domain):
    start_time = time.time()  # Startzeit für die Zeiterfassung der Funktion
    try:
        # Führt tor-resolve Befehl aus
        output = subprocess.run(['tor-resolve', domain], capture_output=True, text=True)
        duration = time.time() - start_time  # Berechnet die Dauer der Anfrage
        # Überprüft, ob der Prozess erfolgreich war
        if output.returncode == 0:
            return [output.stdout.strip()], duration
        else:
            raise Exception(output.stderr.strip())
    except Exception as e:
        print(f"Fehler bei der DNS-Anfrage für {domain} über Tor: {e}")
        return [], time.time() - start_time
```

Die Ergebnisse dieser Abfragen werden in einer CSV-Datei gespeichert, die Spalten dieser Datei siehe Listing 4.11.

Listing 4.11: Spalten CSV-Datei Ausgabe für Umgehungsmethode 4: Tor

```
Timestamp;Domain;Authorative Nameserver IPs;Aufgelöste IP-Adresse bei aktiver Tor-Verbindung;Antwortzeit Tor-Verbindung Resolver;DNS-Sperre umgangen mit Tor?
```

Die Nutzung von Tor bietet mehrere Vorteile in Bezug auf Anonymität und Zugangsfreiheit. Durch die Verschlüsselung und das Routing des Datenverkehrs über mehrere Knoten auf der

ganzen Welt bietet Tor eine robuste Plattform, um Zensur und Überwachung zu umgehen. Allerdings kann die Nutzung von Tor auch Herausforderungen mit sich bringen, wie z. B. langsamere Verbindungsgeschwindigkeiten und die Möglichkeit, dass einige Dienste den Zugang von Tor-Exit-Knoten blockieren.

Trotz dieser Herausforderungen bleibt Tor eine effektive Methode zur Umgehung von DNS-Sperren, insbesondere in Umgebungen mit strenger Internetzensur. Die Ergebnisse dieser Untersuchung werden die Effektivität von Tor im Vergleich zu anderen Methoden wie VPNs beleuchten und zeigen, inwieweit Tor DNS-Sperren umgehen kann.

Die Tests wurden mit SIM-Karten und damit in der Netzumgebung der ausgewählten ISPs durchgeführt. Jeder Testlauf wurde dokumentiert und die Ausgabe ist in den Anhängen zu finden:

- Anhang K.1 für A1
- Anhang K.2 für Drei
- Anhang K.3 für Magenta

Die Ergebnisse werden in Abschnitt 5.1.4 präsentiert.

4.8. Auswertungsmethodik

Die Auswertung der gesammelten Daten zu den verschiedenen Umgehungsmethoden der DNS-Sperre, direkter Zugriff auf IP-Adressen, verschiedene DNS-Resolver, VPN-Verbindungen und Tor-Nutzung, erfolgt durch eine Kombination aus deskriptiven Statistiken und visuellen Darstellungen. Diese Methoden helfen dabei, die Effektivität der einzelnen Umgehungsmethoden zu bewerten und vergleichende Einblicke zu gewinnen.

4.8.1. Erfolgsrate

Die Erfolgsrate jeder Methode zur Umgehung von DNS-Sperren wird quantifiziert und als Prozentsatz ausgedrückt. Dabei wird die Anzahl der erfolgreichen Umgehungen ins Verhältnis zur Gesamtzahl der Versuche gesetzt. Diese Methode ermöglicht einen direkten Vergleich der Effektivität der verschiedenen Techniken und basiert auf der Formel

$$\text{Erfolgsrate} = \left(\frac{\text{Anzahl erfolgreicher Umgehungen}}{\text{Gesamtzahl der Versuche}} \right) \times 100\%$$

4.8.2. Antwortzeiten

Zur Analyse der Haupttendenzen und Streuungen der Antwortzeiten werden deskriptive Statistiken verwendet. Mittelwert und Median der Antwortzeiten werden berechnet, um die Haupttendenzen zu identifizieren. Außerdem werden die Standardabweichung und der Variationskoeffizient bestimmt, um die Variabilität der Antwortzeiten zwischen den verschiedenen Methoden zu quantifizieren.

4.8.3. Korrelationsanalyse

Zur Untersuchung der Hypothese H1, *Es besteht ein negativer Zusammenhang zwischen der Erfolgsrate der Umgehungsmethoden und der Antwortzeit. Das bedeutet, je höher die Erfolgsrate einer Methode, desto geringer tendenziell die Antwortzeit*, wird eine Korrelationsanalyse durchgeführt.

4.8.4. Varianzanalyse

Zur Untersuchung der Hypothese H2, *Die Antwortzeiten von Tor sind signifikant höher als die der Umgehungsmethode VPN und DNS-Resolver ändern.*, wird eine Varianzanalyse durchgeführt. Diese Analyse testet die Mittelwertunterschiede der Antwortzeiten zwischen den Gruppen. Falls die Voraussetzungen der ANOVA (Normalverteilung und Homogenität der Varianzen) nicht erfüllt sind, wird der Kruskal-Wallis-Test als nicht-parametrische Alternative verwendet. Bei signifikanten Ergebnissen werden Post-hoc-Tests durchgeführt, um zu bestimmen, welche Gruppen sich unterscheiden.

4.8.5. Visuelle Datenanalyse

Für eine intuitive Darstellung der gesammelten Daten werden verschiedene Diagrammtypen verwendet:

- Balkendiagramme: Visualisierung der Erfolgsraten der Umgehungsmethoden, um effektive von weniger effektiven Methoden zu unterscheiden.
- Boxplots: Visualisierung der Verteilungen der Antwortzeiten für jede Methode, um Ausreißer zu identifizieren und die Konsistenz jeder Methode zu bewerten.

4.8.6. Vergleichende Analyse basierend auf der Forschungsfrage

Im Rahmen der abschließenden Analyse erfolgt ein direkter Vergleich der verschiedenen technischen Umgehungsmethoden von Netzsperren in Österreich. Dabei liegt der Fokus auf der Untersuchung der Zuverlässigkeit und Effektivität jeder einzelnen Methode, basierend auf den gesammelten Daten zu Erfolgsraten und Antwortzeiten. Die Forschungsfrage lautet: *Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen?* Die Beantwortung der Forschungsfrage erfordert

eine detaillierte Analyse, welche die Effektivität und Zuverlässigkeit jeder Methode bewertet. Dabei werden sowohl die spezifischen Stärken und Schwächen der einzelnen Methoden als auch die effizienteste Methode identifiziert. Die Ergebnisse sollen dazu beitragen, ein umfassendes Verständnis der verschiedenen Techniken zu entwickeln und auf dieser Basis fundierte Empfehlungen für die Praxis abzuleiten, die auf wissenschaftlichen Erkenntnissen basieren.

Durch die Anwendung dieser statistischen und analytischen Methoden wird eine umfassende Auswertung der gesammelten Daten angestrebt, um Schlussfolgerungen über die Wirksamkeit der untersuchten DNS-Umgehungsmethoden zu ziehen. Die Ergebnisse dieser Auswertung dienen als Grundlage für weiterführende Diskussionen und Empfehlungen in den folgenden Abschnitten der Masterarbeit.

5. Analyse der Ergebnisse

In diesem Kapitel erfolgt die detaillierte Auswertung und Interpretation der empirischen Daten, die im Rahmen der experimentellen Analyse gesammelt wurden, um die Effektivität verschiedener Methoden zur Umgehung von DNS-Sperren zu bewerten.

5.1. Ergebnisse der Umgehungsmethoden

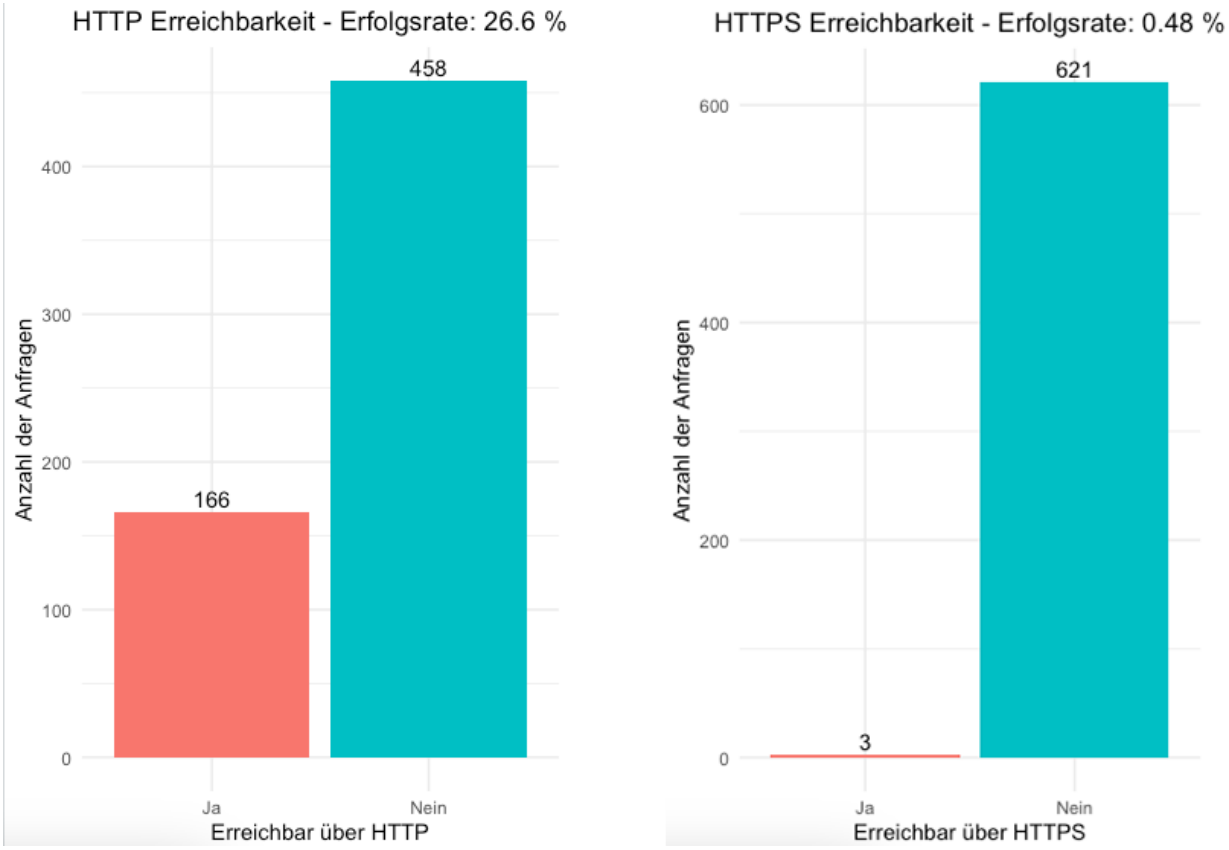
Um ein umfassendes Bild der Wirksamkeit dieser Umgehungstechniken in der österreichischen Internetlandschaft zu erhalten, wurden die Daten der drei größten österreichischen Internet Service Provider (ISP) zusammengetragen und analysiert. Folgend werden die Ergebnisse je Umgehungsmethode präsentiert.

5.1.1. Umgehungsmethode 1: IP-Adresse verwenden

Die dargestellten Diagramme und Statistiken wurden mithilfe von `R` erstellt, das verwendete R-Skript ist im Anhang L zu finden.

Die visuelle Darstellung in Abbildung 5.1 präsentiert zwei Balkendiagramme, welche die Resultate der Tests zur Ermittlung der Fähigkeit von Webseiten, über IP-Adressen unter Verwendung der Protokolle HTTP und HTTPS erreicht zu werden, veranschaulichen. Die Diagramme demonstrieren die Anzahl der Anfragen, bei denen der Zugriff erfolgreich (Ja) und nicht erfolgreich (Nein) war.

- **HTTP Erreichbarkeit:**
  - Der linke Balken zeigt, dass 166 Anfragen über HTTP erfolgreich waren, was einer Erfolgsrate von 26,6 % entspricht.
  - Der rechte Balken zeigt, dass bei 458 Anfragen der Zugriff über HTTP nicht erfolgreich war.
- **HTTPS Erreichbarkeit:**
  - Der linke Balken zeigt, dass nur drei Anfragen über HTTPS erfolgreich waren, was einer Erfolgsrate von 0,48 % entspricht.
  - Der rechte Balken zeigt, dass bei 621 Anfragen der Zugriff über HTTPS nicht erfolgreich war.

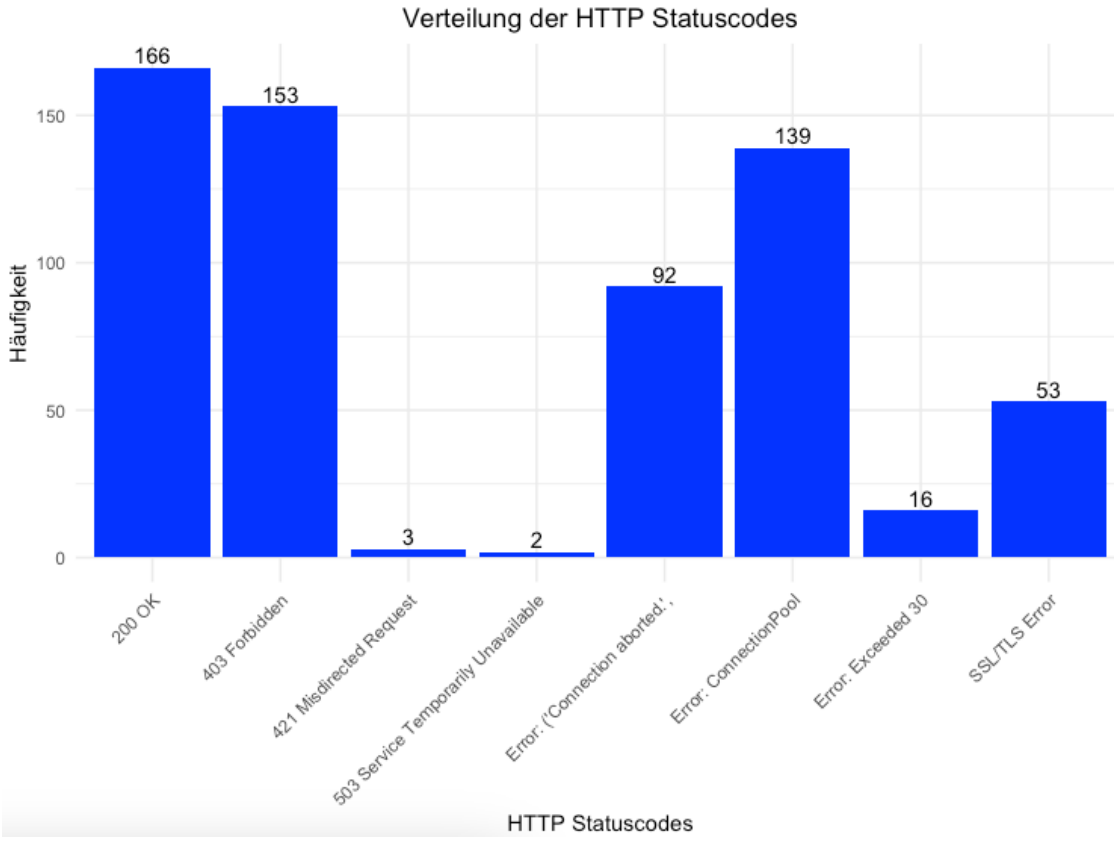


Abbildungsverzeichnis 5.1.: Ergebnisse Umgehungsmethode 1: IP-Adresse verwenden. Erfolgsrate HTTP-Erreichbarkeit

Diese Diagramme verdeutlichen, dass der Zugriff auf Webseiten über ihre IP-Adressen bei Nutzung von HTTPS fast vollständig blockiert war und diese Methode nicht geeignet ist.

Die Abbildung 5.2 zeigt die Verteilung der HTTP-Statuscodes, die bei Webanfragen über IP-Adressen mittels des HTTP-Protokolls während der Untersuchung erhalten wurden. Die einzelnen Balken repräsentieren die Häufigkeit verschiedener Statuscodes und Fehlermeldungen, die aufgetreten sind. Folgend eine Übersicht der Ergebnisse:

- **200 OK**: Dieser Statuscode wurde 166 Mal zurückgegeben und zeigt erfolgreiche Anfragen an.
- **403 Forbidden**: 153 Vorkommen dieses Codes bedeuten, dass der Zugriff wegen fehlender Zugriffsrechte vom Server verweigert wurde.
- **Error: Connection aborted**: Dieser Status erschien 92 Mal und wird vermutlich durch Netzwerkfehler oder Unterbrechungen der Verbindung zwischen Client und Server verursacht.
- **Error: Connection Pool**: Dieser Fehler trat 139 Mal auf und zeigt Probleme im Server-Verbindungspool an. Ein Verbindungspool, der eine limitierte Anzahl



Abbildungsverzeichnis 5.2.: Ergebnisse Umgehungsmethode 1: IP-Adresse verwenden. Verteilung HTTP-Statuscodes

wiederverwendbarer Verbindungen verwaltet, kann erschöpft sein, wenn durch hohes Anfragevolumen oder Verbindungslecks keine freien Verbindungen mehr verfügbar sind. Dies resultiert in Verzögerungen oder dem Scheitern von Anfragen, wenn keine Verbindung aufgebaut werden kann.

- **SSL/TLS Error**: 43 Mal festgestellt, zeigt Probleme mit SSL/TLS-Verschlüsselung oder Zertifikatsvalidierung an, die sicheren Zugang über HTTPS beeinträchtigen.
- **Error: Exceeded 30**: Mit 16 Fällen könnte dies auf das Überschreiten eines festgelegten Limits wie Zeitüberschreitung hinweisen.
- **421 Misdirected Request**: Erschien dreimal und deutet darauf hin, dass die Anfrage an einen ungeeigneten Server gerichtet wurde.
- **503 Service Temporary Unavailable**: Dieser Statuscode trat zweimal auf und zeigt, dass der Server temporär nicht verfügbar war, möglicherweise aufgrund von Überlastung oder Wartungsarbeiten.

Die vorliegende Analyse der Statuscodes erlaubt es, wichtige Einblicke in die technischen Barrieren bei direkten IP-Zugriffen auf Webressourcen zu gewinnen.

Abbildung 5.3 zeigt die Verteilung der HTTPS-Statuscodes, die während der Untersuchung der Erreichbarkeit von Webseiten über IP-Adressen mittels des HTTPS-Protokolls aufgezeichnet wurden. Die Balken repräsentieren die Häufigkeit spezifischer Statuscodes oder Fehlermeldungen, die in der Testserie auftraten.

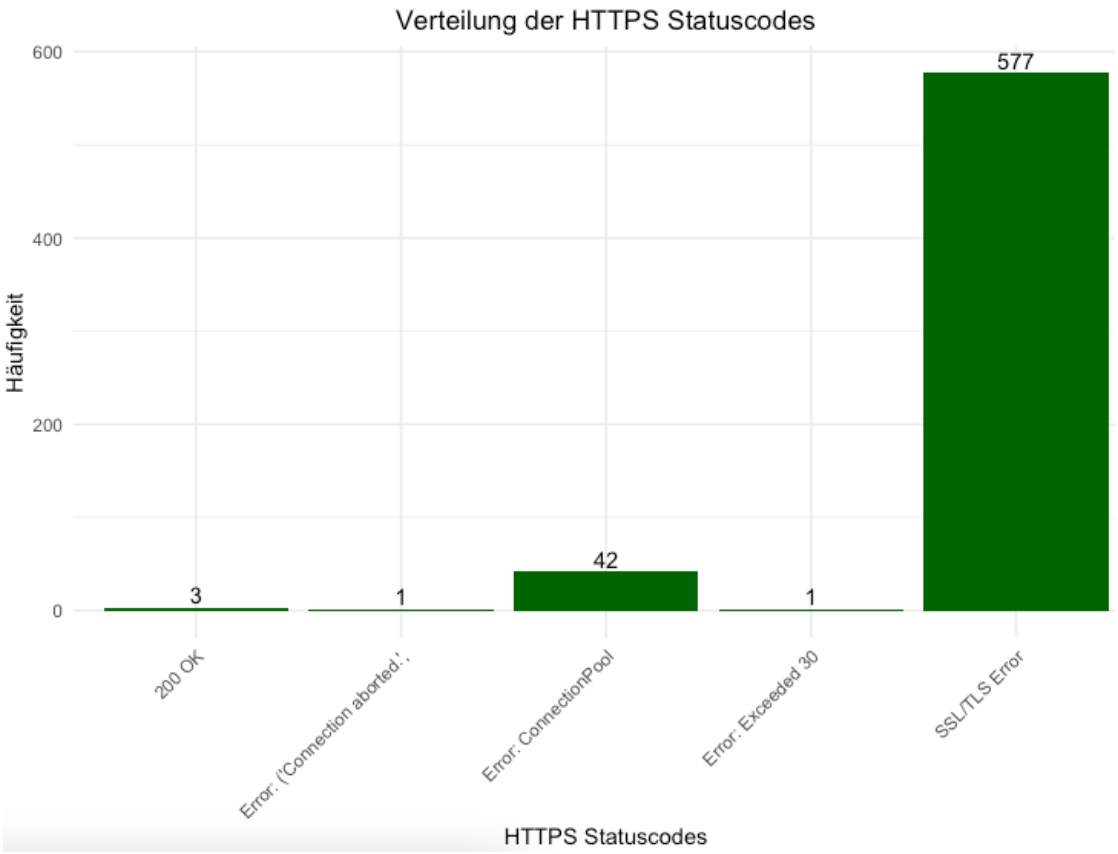
- **200 OK**: Dieser Statuscode wurde nur dreimal registriert, was auf eine sehr geringe Erfolgsrate bei HTTPS-Anfragen hinweist.
- **Error: Connection aborted**: Der Fehler wurde einmal gemeldet und deutet auf eine Unterbrechung der Verbindung hin.
- **Error: Connection Pool**: 42 Mal aufgetreten, weist dieser Fehler auf Probleme im Server-Verbindungspool hin, möglicherweise durch ein hohes Anfragevolumen oder Verbindungslecks.
- **Error: Exceeded 30**: Auch dieser Fehler wurde einmal erfasst und könnte auf das Überschreiten eines Zeitlimits hinweisen.
- **SSL/TLS Error**: Mit 577 Vorkommen ist dies der häufigste Fehler, der Probleme mit der SSL/TLS-Verschlüsselung oder Zertifikatsvalidierung anzeigt, die einen sicheren Zugang über HTTPS verhinderten.

Diese Ergebnisse verdeutlichen die Herausforderungen, die mit HTTPS-Anfragen verbunden sind, insbesondere im Hinblick auf Verschlüsselungs- und Zertifikatsprobleme, die den Zugang deutlich stärker beeinträchtigen als bei HTTP.

Herausforderungen bei der Verwendung von IP-Adressen zur Umgehung von Netzsperren

Die Verwendung direkter IP-Adressen zur Umgehung von DNS-Sperren stößt auf technische Herausforderungen und Sicherheitsprobleme, insbesondere bei HTTPS-Anfragen. Die Sicherheit von HTTPS-Verbindungen hängt maßgeblich von SSL/TLS-Zertifikaten ab, die die Authentizität des Servers bestätigen. Diese Zertifikate sind üblicherweise auf Domainnamen und nicht auf IP-Adressen ausgestellt. Eine HTTPS-Anfrage an eine IP-Adresse resultiert häufig in einem Zertifikatsfehler, da der im Zertifikat spezifizierte Domainname nicht mit der angeforderten IP übereinstimmt. Weiterhin erfordert virtuelles Hosting, dass während des TLS-Handshake der Client den gewünschten Hostnamen übermittelt, damit der Server das korrekte Zertifikat auswählen kann. Bei direkten IP-Anfragen ist der Server folglich oft nicht in der Lage, ein adäquates Zertifikat zuzuordnen, was zu weiteren Fehlern im Prozess führt, obwohl die Anfragen mit Host-Header, welcher die Domain beinhaltet, versendet wurden.

Auch bei HTTP-Anfragen, die ohne die Komplexität von SSL/TLS auskommen, bestehen erhebliche Sicherheitsrisiken. Da HTTP-Anfragen unverschlüsselt sind, können diese abgefangen oder manipuliert werden, was sie anfällig für Abhör- und Man-in-the-Middle-Angriffe macht. Viele Webseiten implementieren Sicherheitsmaßnahmen, die den Datenverkehr automatisch von HTTP auf HTTPS umleiten oder ausschließlich die Nutzung von HTTPS erlauben, um die Integrität und Vertraulichkeit der übertragenen



Abbildungsverzeichnis 5.3.: Ergebnisse Umgehungsmethode 1: IP-Adresse verwenden. Verteilung HTTPS-Statuscodes

Daten zu gewährleisten. Diese Mechanismen verhindern effektiv die Nutzung von HTTP als zuverlässige Alternative für den Zugriff auf beschränkte Inhalte.

Aufgrund der genannten Probleme mit SSL/TLS-Zertifikaten und der inhärenten Sicherheitsrisiken von HTTP ist die Nutzung von IP-Adressen zur Umgehung von DNS-Sperren keine empfohlene Methode. In Produktionsumgebungen birgt die Deaktivierung der SSL/TLS-Validierung, auch wenn sie für Entwicklungs- und Testzwecke manchmal praktiziert wird, unvertretbare Risiken. Daher sollten sicherere und effizientere Methoden zur Umgehung von DNS-Sperren in Betracht gezogen werden, die sowohl die Sicherheit als auch die Zugänglichkeit der Dienste nicht gefährden.

5.1.2. Umgehungsmethode 2: DNS-Resolver ändern

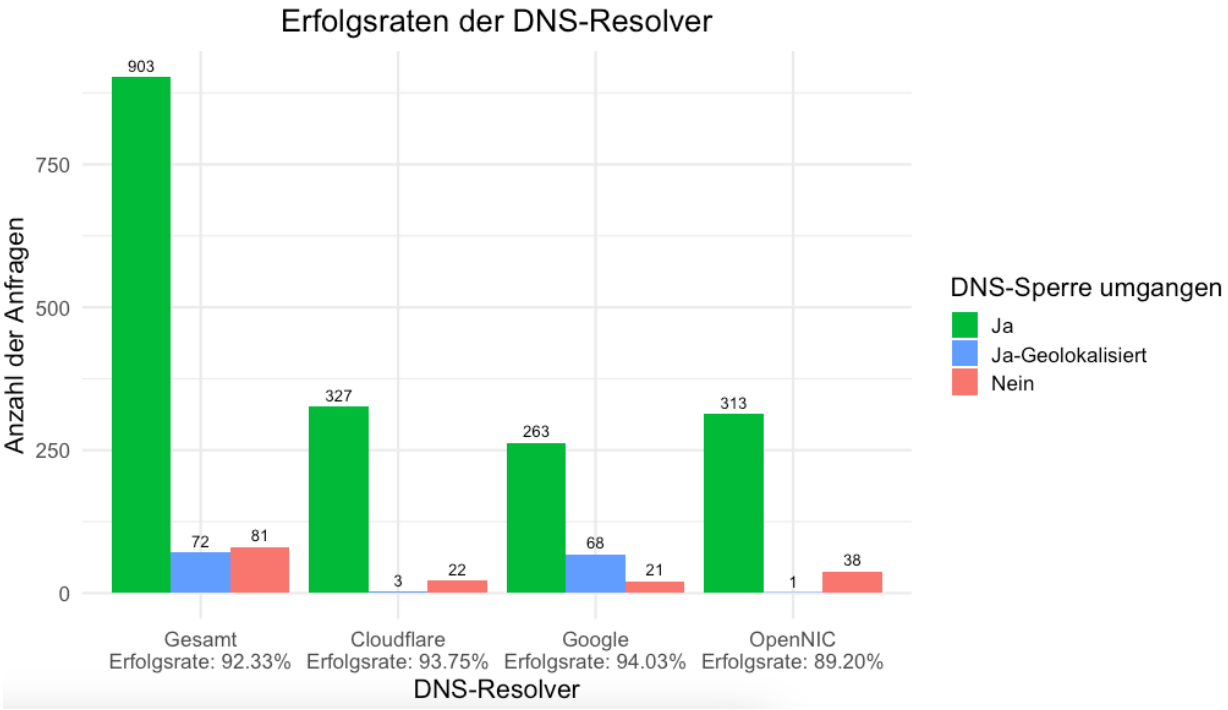
Die Fähigkeit, DNS-Sperren mithilfe alternativer DNS-Resolver zu umgehen, wurde untersucht. In Abbildung 5.4 werden die Ergebnisse von Google DNS, Cloudflare DNS und OpenNIC dargestellt. Das Balkendiagramm zeigt die Erfolgsrate der DNS-Resolver sowie die Gesamterfolgsrate. Die vertikale Achse repräsentiert die Anzahl der Anfragen, und die horizontale Achse die einzelnen Resolver. Diese Grafik verdeutlicht nicht nur die Anzahl der vollständig erfolgreichen Anfragen (grün dargestellt), sondern auch die Anfragen, die aufgrund geografischer Unterschiede ähnliche IP-Adressen lieferten (blau dargestellt), sowie jene, die scheiterten (rot dargestellt). Bei den sogenannten ähnlichen IP-Adressen stimmt der letzte Teil der IP-Adresse (Host-Teil) nicht überein. Dies ist besonders relevant, da die ursprünglichen Anfragen an die autoritativen Nameserver von Österreich aus gestellt wurden und die Antworten der internationalen Public DNS die Informationen zu den IP-Adressen von anderen Standorten bezogen haben können und somit ein geografischer Unterschied besteht und unterschiedliche IP-Adressen zurückgegeben werden können.

Die Gesamterfolgsrate beträgt 92,33 %, was eine hohe Wirksamkeit der eingesetzten DNS-Resolver bei der Umgehung von Zugriffsbeschränkungen hervorhebt. Diese Rate setzt sich aus 903 vollständigen Erfolgen und 72 teilweisen Erfolgen zusammen. Der rote Bereich markiert 81 Anfragen, bei denen die DNS-Sperren nicht umgangen werden konnten.

Google DNS erzielte mit 94,03 % die höchste Erfolgsquote bei der Umgehung von DNS-Sperren. Dieser Resolver lieferte in 68 Fällen Antworten mit geografisch ähnlichen IPs, was die höchste Zahl unter den untersuchten Diensten darstellt. Darüber hinaus gab es 21 Fälle, in denen die Antworten nicht mit denen der autoritativen Nameserver übereinstimmten.

Cloudflare DNS zeigte ebenfalls eine hohe Effizienz mit einer Erfolgsrate von 93,75 %, wobei 330 von 352 Anfragen die DNS-Sperren erfolgreich umgingen. Im Gegensatz zu Google DNS wurden jedoch nur 3 Anfragen als geografisch ähnlich klassifiziert. Weitere 22 Anfragen lieferten Ergebnisse, die von den autoritativen Serverantworten abwichen, was die robuste, aber nicht perfekte Leistung von Cloudflare DNS im internationalen Einsatz unterstreicht.

OpenNIC erreichte eine Erfolgsrate von 89,20 % und konnte 314 der 352 Anfragen erfolgreich bearbeiten, lieferte aber in 38 Fällen keine übereinstimmenden IP-Adressen.

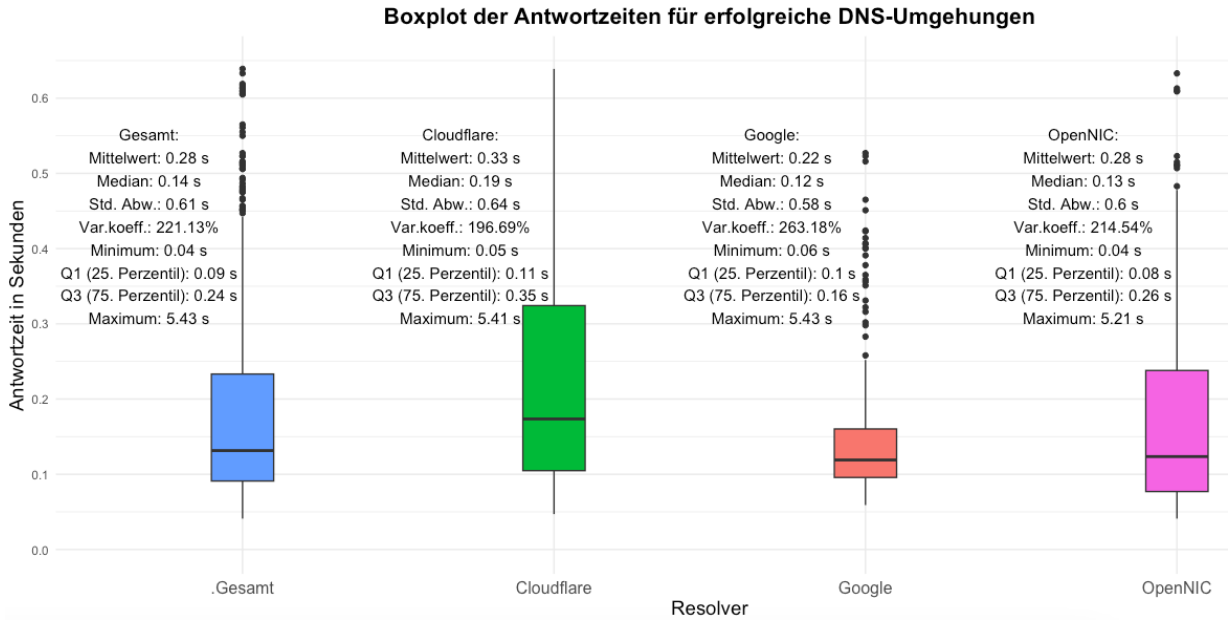


Abbildungsverzeichnis 5.4.: Ergebnisse Umgehungsmethode 2: DNS-Resolver ändern, Erfolgsratenberechnung.

Interessanterweise wurde nur eine Anfrage als nur geografisch korrekt identifiziert, was möglicherweise darauf zurückzuführen ist, dass dieser OpenNIC-Resolver in Österreich betrieben wird. Dies deutet darauf hin, dass OpenNIC eine geeignete Alternative darstellt für Nutzer*innen in Österreich.

Abbildung 5.5 stellt die Antwortzeiten für erfolgreiche DNS-Umgehungen mittels Boxplots dar. Die Antwortzeit ist auf der Y-Achse in Sekunden angegeben und auf der X-Achse werden die einzelnen Resolver aufgelistet.

Die Antwortzeiten der verschiedenen DNS-Resolver sind in Tabelle 5.1 zusammengefasst, um einen direkten Vergleich der Leistungsdaten zu ermöglichen. Der Boxplot "Gesamt" zeigt, dass 75 % der Antwortzeiten unter 0,24 Sekunden liegen, mit einem Median von 0,14 Sekunden. Die Daten weisen jedoch eine Variabilität auf, wie der Variationskoeffizient von 221,13 % und die Spanne von 5,39 Sekunden zwischen Minimum und Maximum zeigen. Cloudflare DNS zeigt eine etwas längere durchschnittliche Antwortzeit von 0,33 Sekunden gegenüber Google und OpenNIC an, aber dafür eine geringere Variation der Antwortzeiten, wie der Variationskoeffizient von 196,69 % zeigt. Mit einem Median von 0,19 Sekunden und höheren Werten für Q1 und Q3 im Vergleich zu Google DNS kann Cloudflare DNS dennoch als effizient eingestuft werden, auch wenn es zu verzögerten Antworten neigt. Google DNS hat die kürzeste durchschnittliche Antwortzeit von 0,22 Sekunden. Mit einem Median von 0,12 Sekunden und einer relativ geringen Streuung, die durch das 25. Perzentil (Q1) von 0,10 Sekunden und das 75. Perzentil (Q3) von 0,16 Sekunden belegt wird, zeigt Google DNS eine konsistente Leistung. Dennoch deutet der Variationskoeffizient von 263,18 %

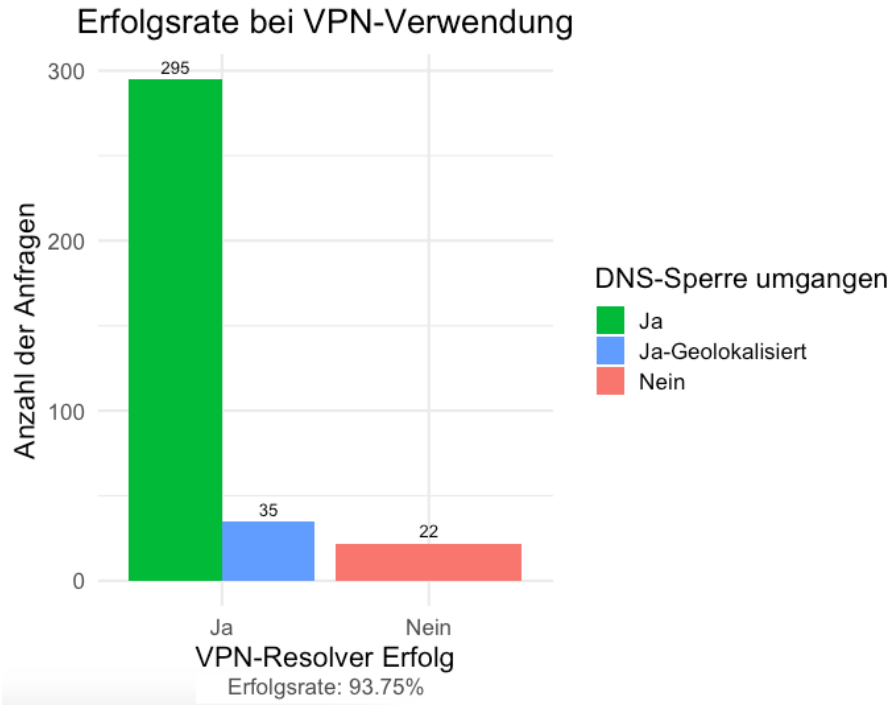


Abbildungsverzeichnis 5.5.: Ergebnisse Umgehungsmethode 2: DNS-Resolver ändern, Antwortzeiten und statistische Auswertung.

auf gelegentliche Ausreißer bei den Antwortzeiten hin. OpenNIC liegt mit einer mittleren Antwortzeit von 0,28 Sekunden in einem ähnlichen Bereich wie Google und Cloudflare, zeigt aber mit einem Variationskoeffizienten von 214,54 % eine geringere Variabilität als Google. Dies könnte darauf hindeuten, dass OpenNIC stabilere Antwortzeiten bietet, aber insgesamt etwas langsamer ist als Google. Jeder dieser Boxplots liefert wichtige Informationen über die Konsistenz und Zuverlässigkeit der Antwortzeiten der DNS-Resolver, die für die Bewertung ihrer Eignung zur Umgehung von DNS-Blockaden entscheidend sind.

Stat. Parameter	**Gesamt**	**Cloudflare**	**Google**	**OpenNIC**
Mittelwert	0.28 s	0.33 s	**0.22 s**	0.28 s
Median	0.14 s	0.19 s	**0.12 s**	0.13 s
Std.abw.	0.61 s	0.64 s	**0.58 s**	0.60 s
Var.koeff.	221.13%	**196.69%**	263.18%	214.54%
Minimum	0.04 s	0.05 s	0.06 s	**0.04 s**
25. Perzentil (Q1)	0.09 s	0.11 s	0.10 s	**0.08 s**
75. Perzentil (Q3)	0.24 s	0.35 s	**0.16 s**	0.26 s
Maximum	5.43 s	5.41 s	5.43 s	**5.21 s**

Tabelle: 5.1.: Antwortzeiten für erfolgreiche DNS-Umgehungen der verschiedenen Resolver. Fett hervorgehoben sind die jeweils besten Werte je Statistikparameter.



Abbildungsverzeichnis 5.6.: Ergebnisse Umgehungsmethode 3: VPN, Erfolgsratenberechnung.

5.1.3. Umgehungsmethode 3: VPN

Abbildung 5.6 zeigt die Erfolgsraten der Verwendung des VPN Psiphon zur Umgehung von DNS-Sperren. Die Grafik präsentiert die Anzahl der Anfragen in drei Kategorien: Erfolgreich umgangene DNS-Sperren (grün dargestellt), die aufgrund geografischer Unterschiede ähnliche IP-Adressen lieferten (blau dargestellt) und erfolglose Versuche (rot dargestellt).

- **Vollständig erfolgreich (grün):** 295 Anfragen konnten dieselbe IP-Adresse als der autoritative Nameserver zurückgeben.
- **Geolokalisiert erfolgreich (blau):** 35 Anfragen lieferten ähnliche IP-Adressen, was darauf hinweist, dass der VPN-Resolver IP-Adressen aus einer anderen geografischen Region lieferte, aber nicht genau die erwartete IP.
- **Nicht erfolgreich (rot):** 22 Anfragen waren nicht erfolgreich, was die Grenzen der VPN-Technologie unter bestimmten Bedingungen aufzeigt.

Die Gesamterfolgsrate der VPN-Nutzung beträgt 93,75 %, was die Wirksamkeit von Psiphon bei der Umgehung von DNS-basierten Zugriffsbeschränkungen unterstreicht. Diese Daten verdeutlichen, dass ein VPN wie Psiphon ein effektives Mittel sein kann, um die Kontrolle und Überwachung durch lokale ISPs zu umgehen.

Abbildung 5.7 illustriert die Antwortzeiten, die bei der Nutzung eines VPN-Dienstes zur Umgehung von DNS-Sperren beobachtet wurden. Der Boxplot gibt einen Einblick in die Variabilität und Konsistenz der Antwortzeiten des VPN-Resolvers.

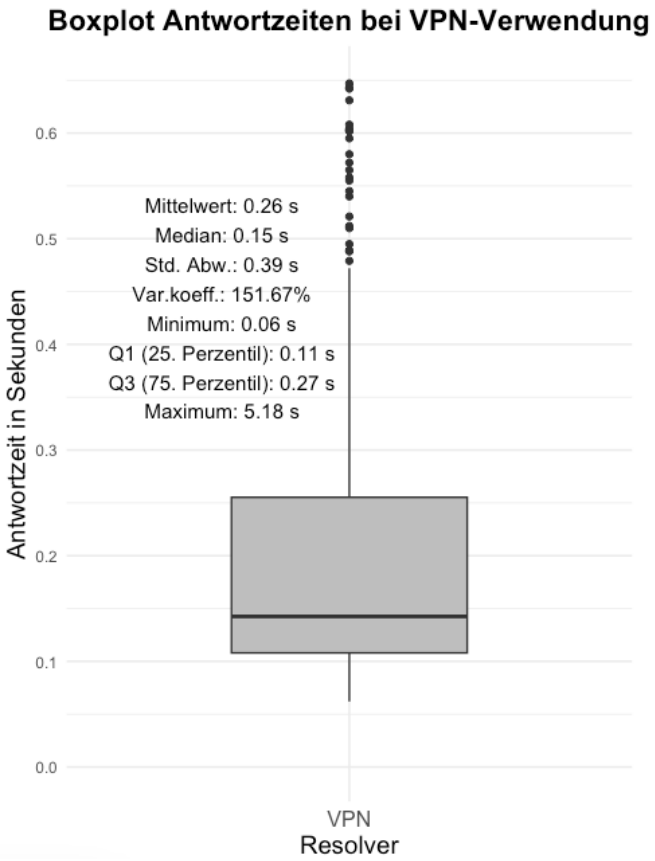
Die zentralen statistischen Maße sind wie folgt:

- **Mittelwert (0,26 Sekunden):** Der durchschnittliche Wert der Antwortzeiten beträgt 0,26 Sekunden. Dieser Wert gibt eine allgemeine Vorstellung von der typischen Antwortgeschwindigkeit des VPN-Resolvers.
- **Median (0,15 Sekunden):** Der Medianwert liegt bei 0,15 Sekunden. Da der Median weniger anfällig für extreme Werte ist als der Mittelwert, bietet dieser eine verlässlichere Aussage über die zentrale Tendenz der Antwortzeiten. Dass der Median niedriger als der Mittelwert ist, deutet auf eine rechtsschiefe Verteilung hin, was bedeutet, dass die meisten Antwortzeiten geringer als der Mittelwert sind, jedoch einige wenige sehr lange Antwortzeiten das Mittel nach oben ziehen.
- **Standardabweichung (0,39 Sekunden):** Eine Standardabweichung von 0,39 Sekunden zeigt an, dass die Antwortzeiten um den Mittelwert herum gestreut sind, was auf eine Variabilität in den Antwortzeiten hinweist.
- **Variationskoeffizient (151,67 %):** Mit einem Variationskoeffizienten von 151,67 % ist ersichtlich, dass die Antwortzeiten relativ zur Größe des Mittelwerts variieren, was auf eine ungleichmäßige Leistung des VPN-Resolvers hinweist.
- **Minimum (0,06 Sekunden) und Maximum (5,18 Sekunden):** Die Spannweite der Daten, von einem Minimum von 0,06 Sekunden bis zu einem Maximum von 5,18 Sekunden, illustriert die Unterschiede in den Antwortzeiten.
- **Interquartilsabstand (Q1 und Q3):** Das erste Quartil (25. Perzentil) liegt bei 0,11 Sekunden und das dritte Quartil (75. Perzentil) bei 0,27 Sekunden. Der Interquartilsabstand zeigt, dass 50 % der Antwortzeiten zwischen diesen beiden Werten liegen. Dieser Bereich gibt die somit typische Antwortzeit wider, frei von Ausreißern.

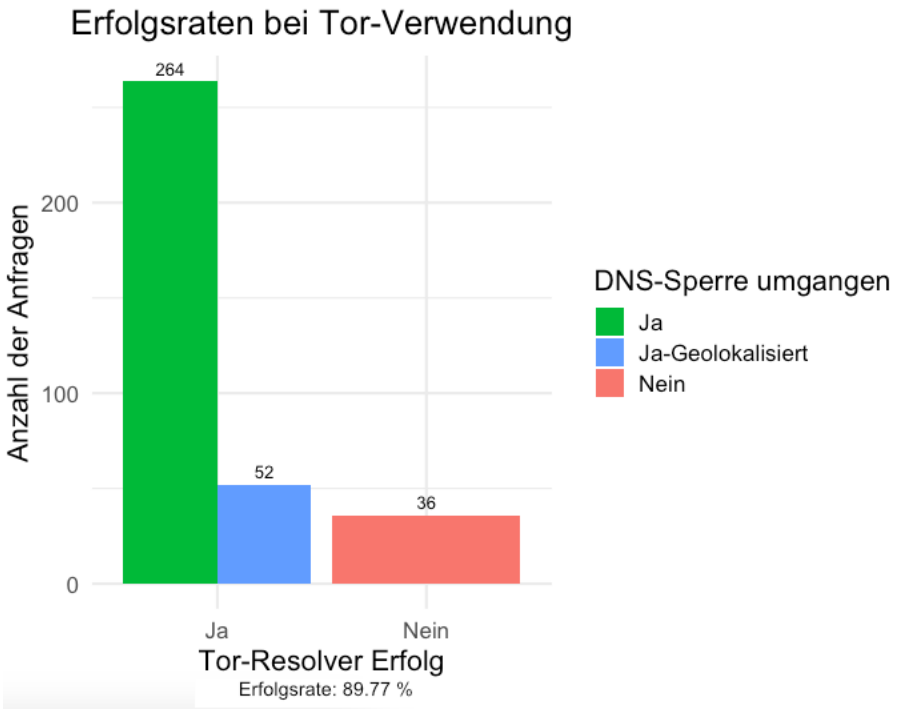
Insgesamt zeigt der Boxplot, dass zwar viele Anfragen schnell beantwortet werden, aber eine nicht unerhebliche Anzahl von Anfragen deutlich länger dauert, wie die Ausreißer oberhalb des 75. Perzentil zeigen. Diese Ausreißer könnten auf Netzwerklatenzen, Routingprobleme oder die geografische Entfernung der VPN-Server von den Nutzer*innen zurückzuführen sein. Die Varianz und der Variationskoeffizient könnten auch ein Hinweis auf die Qualität des VPN-Dienstes oder auf Inkonsistenzen in der Netzwerkleistung sein.

5.1.4. Umgehungsmethode 4: Tor

Abbildung 5.8 zeigt die Erfolgsraten der Verwendung von Tor, um DNS-Sperren zu umgehen. Diese Ergebnisse wurden durch umfangreiche Tests gewonnen, bei denen Tor eingesetzt



Abbildungsverzeichnis 5.7.: Ergebnisse Umgehungsmethode 3: VPN, Antwortzeiten und statistische Auswertung.



Abbildungsverzeichnis 5.8.: Ergebnisse Umgehungsmethode 4: Tor, Erfolgsratenberechnung.

wurde, um Anfragen zu senden, deren Zieladressen normalerweise durch DNS-Sperren blockiert sind.

Die Grafik stellt die Anzahl der Anfragen in drei Kategorien dar:

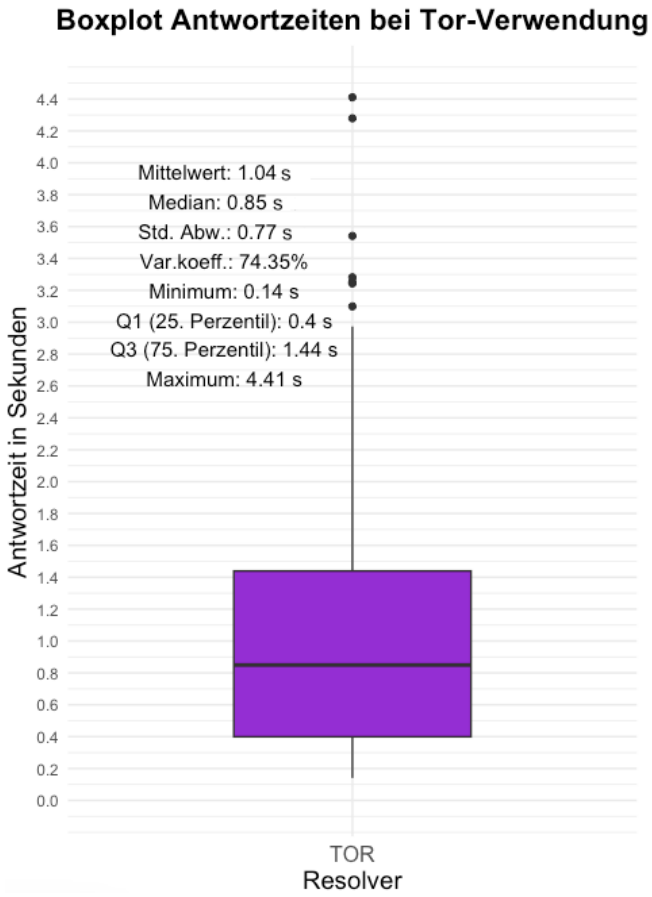
- **Vollständig erfolgreich (grün):** 264 Anfragen konnten die DNS-Sperren komplett umgehen, wobei die durch Tor aufgelösten IP-Adressen mit den erwarteten autoritativen Nameserver-Antworten übereinstimmten.
- **Geolokalisiert erfolgreich (blau):** 52 Anfragen lieferten IP-Adressen aus einer anderen geografischen Region. Dies weist auf die Fähigkeit von Tor hin, Anfragen über internationale Knoten zu leiten, was zu Abweichungen bei den gelieferten IPs führen kann.
- **Nicht erfolgreich (rot):** 36 Anfragen konnten die DNS-Sperren nicht umgehen, was auf potenzielle Netzwerkeinschränkungen oder die Erkennung und Blockierung von Tor-Verkehr hinweisen könnte.

Die Gesamterfolgsrate von Tor bei der Umgehung von DNS-Sperren liegt bei 89,77 %, was die Effektivität von Tor als Werkzeug zum Schutz der Online-Privatsphäre und zur Umgehung von Internetzensur unterstreicht. Die Daten zeigen, dass Tor nicht nur die Identität der Nutzer*innen schützt, sondern auch ein effektives Mittel sein kann, um Zugang zu ansonsten eingeschränkten Ressourcen zu erhalten.

Die Abbildung 5.9 zeigt die Antwortzeiten, die bei der Nutzung von Tor zur Umgehung von DNS-Sperren gemessen wurden. Dieser Boxplot gibt einen Überblick über die Verteilung der Antwortzeiten und hilft dabei, die Leistungsfähigkeit und Zuverlässigkeit des Tor-Netzwerks in Bezug auf DNS-Auflösungen zu verstehen.

- **Mittelwert (1,04 Sekunden):** Der Mittelwert gibt die durchschnittliche Antwortzeit aller gemessenen Anfragen an. Bei einem Wert von etwas über einer Sekunde zeigt dieser, dass Anfragen über das Tor-Netzwerk generell innerhalb einer angemessenen Zeit beantwortet werden. Der Mittelwert ist nützlich, um einen Gesamteindruck von der Leistung zu bekommen, wird aber durch extreme Werte (sowohl sehr schnelle als auch sehr langsame Antworten) beeinflusst.
- **Median (0,85 Sekunden):** Der Median stellt den mittleren Wert der Datensatzes dar und teilt die Antwortzeiten in zwei Hälften. Da er weniger empfindlich gegenüber Ausreißern ist als der Mittelwert, bietet er ein realistischeres Bild der typischen Antwortzeit. Dass der Median niedriger ist als der Mittelwert, deutet auf eine asymmetrische Verteilung hin, bei der einige sehr hohe Antwortzeiten den Durchschnitt erhöhen.
- **Standardabweichung (0,77 Sekunden):** Dieses Maß zeigt, wie breit die Antwortzeiten um den Mittelwert gestreut sind. Eine Standardabweichung von 0,77 Sekunden in diesem Kontext zeigt eine Variabilität in den Antwortzeiten, was auf die variablen Pfade hinweist, die durch das Tor-Netzwerk genommen werden.
- **Variationskoeffizient (74,35 %):** Der Variationskoeffizient ist ein Maß für die relative Variabilität und zeigt die Schwankungen der Antwortzeiten im Verhältnis zum Mittelwert. Dies weist auf eine inkonsistente Leistung des Tor-Netzwerks hin, was typisch für Anonymisierungsnetzwerke mit dynamisch wechselnden Routen ist.
- **Minimum (0,14 Sekunden) und Maximum (4,41 Sekunden):** Diese Werte zeigen die Spannweite der Antwortzeiten von der schnellsten bis zur langsamsten. Sie verdeutlichen, dass unter optimalen Bedingungen Anfragen in 0,14 Sekunden bearbeitet werden können und unter ungünstigen Umständen Verzögerungen von 4,41 Sekunden entstehen können.
- **Interquartilsabstand (Q1 und Q3):** Diese Quartile zeigen, dass 50 % der Antwortzeiten zwischen 0,4 und 1,44 Sekunden liegen. Der Interquartilsabstand bietet einen Einblick in die zentrale Tendenz der Daten, frei von den extremen Ausreißern, die das Bild verzerren könnten.

Diese statistischen Maße geben einen wichtigen Einblick in das Verhalten von Tor bei der DNS-Umgehung. Die hohe Variabilität und die Ausreißer in den Antwortzeiten sind kritische Faktoren, die bei der Verwendung von Tor für zeitkritische Anwendungen berücksichtigt werden müssen.



Abbildungsverzeichnis 5.9.: Ergebnisse Umgehungsmethode 4: Tor, Antwortzeiten und statistische Auswertung.

5.2. Vergleich der Ergebnisse

In dieser Sektion werden die Leistung und die Effektivität der verschiedenen Methoden zur Umgehung von DNS-Sperren, einschließlich Cloudflare DNS, Google DNS, OpenNIC, VPNs und Tor, eingehend analysiert und verglichen. Diese Analyse berücksichtigt verschiedene Leistungsindikatoren wie Antwortzeiten, Variabilität, Erfolgsraten und spezifische Vorteile und Nachteile jeder Methode. Zu sehen sind die Parameter jeder Umgehungsmethode in Tabelle 5.2.

Parameter	**Cloudflare** 1.1.1.1	**Google** 8.8.8.8	**OpenNIC** 37.252.191.197	**VPN** Psiphon	**Tor**
Mittelwert	0.33 s	**0.22 s**	0.28 s	0.26 s	1.04 s
Median	0.19 s	**0.12 s**	0.13 s	0.15 s	0.85 s
Std.abw.	0.64 s	0.58 s	0.60 s	**0.39 s**	0.77 s
Var.koeff.	196.69%	263.18%	214.54%	151.67%	**74.35%**
Minimum	0.05 s	0.06 s	**0.04 s**	0.06 s	0.14 s
Q1	0.11 s	0.10 s	**0.08 s**	0.11 s	0.40 s
Q3	0.35 s	**0.16 s**	0.26 s	0.27 s	1.44 s
Maximum	5.41 s	5.43 s	5.21 s	5.18 s	**4.41 s**
Erfolgsrate	93.75%	**94.03%**	89.20%	93.75%	89.77%

Tabelle: 5.2.: Vergleich der Statistiken und Erfolgsraten für Cloudflare DNS, Google DNS, OpenNIC, VPN und Tor. Fett hervorgehoben sind die jeweils besten Werte je Statistikparameter.

5.2.1. Analyse der Antwortzeiten

Die Analyse der Antwortzeiten der verschiedenen Umgehungsmethoden zeigt Unterschiede in der Leistungsfähigkeit zwischen den untersuchten Diensten. Die in der Vergleichstabelle dargestellten Daten belegen, dass Google DNS mit einer durchschnittlichen Antwortzeit von 0,22 Sekunden und einem Median von 0,12 Sekunden die schnellste Performance unter den getesteten Verfahren aufweist. Der Variationskoeffizient von 263,18 % weist dabei die höchste gemessene Variabilität der Antwortzeiten auf, was potenzielle Inkonsistenzen in der Performance impliziert.

Cloudflare DNS erreicht eine minimale Antwortzeit von nur 0,05 Sekunden. Die durchschnittliche Antwortzeit liegt bei 0,33 Sekunden und der Median bei 0,19 Sekunden. Obgleich diese Werte auf schnelle Antwortzeiten hindeuten, lässt sich anhand des Variationskoeffizienten von 196,69 % eine erhöhte Variabilität der Antwortzeiten ableiten, was potenzielle Inkonsistenzen in der Performance impliziert.

Die durchschnittliche Antwortzeit von OpenNIC beträgt 0,28 Sekunden, der Median liegt bei 0,13 Sekunden. Damit bietet OpenNIC eine ähnlich gute Performance wie Cloudflare DNS und übertrifft diesen sogar in beiden Kategorien. Interessant ist die kleinste gemessene Latenz von 0,04 Sekunden, die zeigt, dass OpenNIC unter idealen Bedingungen schnell

reagieren kann. Die im Vergleich zu Cloudflare DNS geringere Standardabweichung von 0,60 Sekunden lässt auf eine gewisse Konstanz in der Antwortgeschwindigkeit schließen, obwohl eine merkliche Schwankungsbreite durch den Variationskoeffizienten von 214,54 % angezeigt wird.

Die durchschnittliche Antwortzeit von VPN, repräsentiert durch Psiphon, beträgt 0,26 Sekunden, während der Median bei 0,15 Sekunden liegt. Dies entspricht einer konkurrenzfähigen Performance mit den DNS-Resolvern. Der vergleichsweise geringste Standardabweichung von 0,39 Sekunden lässt auf eine stabilere Performance im Vergleich zu den reinen DNS-Diensten schließen.

Die längsten Antwortzeiten wurden für Tor mit einem Mittelwert von 1,04 Sekunden und einem Median von 0,85 Sekunden ermittelt. Diese längeren Zeiten für das Tor-Netzwerk, ergeben sich wohl durch sein mehrstufiges, global verteiltes Routing, welches zur Anonymisierung beiträgt. Der im Vergleich ermittelte Variationskoeffizient von 74,35 % ist der niedrigste und zeigt an, dass die Antwortzeiten zwar langsamer, aber konsistenter sind, was auf eine vorhersehbare Leistung trotz der inhärenten Latenz hinweist.

Zusammenfassend zeigt diese Analyse, dass Google DNS und OpenNIC optimale Optionen für Anwender*innen darstellen, die schnelle DNS-Auflösungen priorisieren. OpenNIC bietet eine ausgewogene Performance mit einem guten Gleichgewicht zwischen Geschwindigkeit und geringer Variabilität der Antwortzeiten. VPN und Tor eignen sich besonders für Nutzer*innen, welche Wert auf Sicherheit und Anonymität legen, wobei Tor trotz langsamerer Antwortzeiten eine ausgeglichenere Performance bietet. Die Analyse der Variabilität der Antwortzeiten zeigt, dass die Wahl des DNS-Resolvers sorgfältig auf die spezifischen Bedürfnisse der Endnutzer*innen und die technischen Anforderungen der jeweiligen Anwendung abgestimmt werden sollte.

5.2.2. Zuverlässigkeit und Erfolgsraten

Die Erfolgsraten der Umgehungsmethoden sind ein entscheidender Faktor, wie effektiv diese Methoden bei der Umgehung von DNS-Sperren sind. Ein Vergleich dieser Metrik zeigt Unterschiede in den Erfolgsraten der verschiedenen Methoden.

Google DNS zeigt mit einer Erfolgsrate von 94,03 % die beste Leistung unter den betrachteten DNS-Resolving-Diensten. Diese hohe Erfolgsrate bestätigt die Effizienz von Google DNS bei der Lösung von DNS-Anfragen unter verschiedenen Netzwerkbedingungen. Diese Eigenschaften machen Google DNS besonders geeignet für Nutzer*innen, die auf einen zuverlässigen Zugriff auf weltweit verfügbare Inhalte angewiesen sind.

Die VPN-Methode, repräsentiert durch Psiphon, weist eine Erfolgsrate von 93,75 % auf und liegt damit gleichauf mit Cloudflare, nahe an der Erfolgsrate von Google DNS. VPNs unterscheiden sich jedoch dadurch, dass sie nicht nur DNS-Anfragen auflösen, sondern auch den gesamten Datenverkehr verschlüsseln. Die Verschlüsselung bietet zusätzlichen Schutz vor Überwachung und Zensur. VPNs wie Psiphon sind daher ideal für Benutzer*innen, die

ihre Privatsphäre schützen und gleichzeitig Zugang zu regional blockierten oder zensierten Inhalten suchen.

Die Erfolgsrate von OpenNIC liegt bei 89,20 %. Trotz dieser geringfügig niedrigeren Rate bietet OpenNIC den Vorteil, unabhängig von den bekannten und etablierten DNS-Resolvern zu sein, sodass keine persönlichen Daten an diese übermittelt werden müssen.

Tor weist mit einer Erfolgsrate von 89,77 % eine hohe Effektivität auf und legt dabei besonderen Wert auf Anonymität und Sicherheit. Obwohl Tor nicht die schnellste oder effektivste Methode gegen DNS-Sperren darstellt, kann es Vorteile bieten in dem es die Privatsphäre der Nutzer*innen schützen kann.

5.3. Hypothesenprüfung

In diesem Abschnitt werden die Ergebnisse der statistischen Tests zur Überprüfung der aufgestellten Hypothesen dargestellt und interpretiert. Hierzu wurde das in Anhang P befindliche R-Skript für die statistische Analyse verwendet.

5.3.1. Ergebnisse Hypothese H1

Um die Hypothese H1 zu prüfen, dass ein negativer Zusammenhang zwischen der Erfolgsquote der Umgehungsmethoden und der Antwortzeit besteht, wurde eine Korrelationsanalyse mit dem Rangkorrelationskoeffizienten nach Spearman durchgeführt. Der Spearman-Rangkorrelationskoeffizient wurde gewählt, da die Verteilung der Antwortzeiten asymmetrisch ist. Im Gegensatz zum Pearson-Korrelationskoeffizienten, der lineare Zusammenhänge zwischen zwei metrischen Variablen misst und empfindlich auf Ausreißer und Verteilungsannahmen reagiert, wertet der Spearman-Korrelationskoeffizient monotone Zusammenhänge aus, ohne dass die Verteilung der Daten normal sein muss. Er ist daher robuster gegenüber Ausreißern und nicht normalverteilten Daten.

Der Spearman-Rangkorrelationskoeffizient berechnet die Korrelation zwischen den Rängen der Werte, anstatt direkt mit den Werten zu arbeiten. Die Berechnung erfolgt in folgenden Schritten: Jedem Wert der beiden Variablen wird sein Rang im Datensatz zugeordnet. Dann werden die Differenzen zwischen den Rängen der entsprechenden Werte berechnet. Die Quadrate der Rangunterschiede werden addiert und der Spearman-Koeffizient wird nach folgender Formel berechnet

$$r_s = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)}$$

berechnet, wobei d_i die Differenz zwischen den Rängen jedes Datenpaares und n die Anzahl der Datenpaare ist.

Der Spearman-Rangkorrelationskoeffizient (r_s) zwischen der Erfolgsrate und dem Median der Antwortzeit beträgt -0.359 ($p = 0.553$). Dies deutet auf eine leichte negative Korrelation hin, die jedoch statistisch nicht signifikant ist. Ein p-Wert von weniger als 0,05 würde

als statistisch signifikant gelten, was bedeutet, dass die Wahrscheinlichkeit, dass das beobachtete Ergebnis zufällig ist, weniger als 5 % beträgt. Im vorliegenden Fall ist der p-Wert jedoch deutlich höher, was darauf hinweist, dass der beobachtete Zusammenhang nicht stark genug ist, um als statistisch signifikant angesehen zu werden, was bedeutet, dass höhere Erfolgsraten nicht zuverlässig mit kürzeren Antwortzeiten verbunden sind.

5.3.2. Ergebnisse Hypothese H2

Zur Überprüfung der Hypothese U2, dass die Antwortzeiten von Tor signifikant höher sind als die von VPN und der DNS-Resolver-Änderungsmethode, wurde zunächst eine Varianzanalyse (ANOVA) in Betracht gezogen. Die ANOVA setzt voraus, dass die Varianzen der Antwortzeiten in den verschiedenen Gruppen homogen sind.

Um die Homogenität der Varianzen zu überprüfen, wurde der Levene-Test durchgeführt. Die Ergebnisse des Levene-Tests zeigten jedoch, dass die Varianzen zwischen den Gruppen signifikant unterschiedlich sind ($F(4, 1343) = 14.614$, $p < 1.089 \times 10^{-11}$). Ein p-Wert kleiner als 0.05 deutet darauf hin, dass die Varianzen zwischen den Gruppen nicht homogen sind, was die Voraussetzung für die ANOVA verletzt. Aufgrund dieser Verletzung der Varianz-Homogenität ist die ANOVA nicht geeignet, um die Unterschiede zwischen den Gruppen zu analysieren.

Stattdessen wurde der Kruskal-Wallis-Test gewählt, um die Antwortzeiten zwischen den Gruppen zu vergleichen. Der Kruskal-Wallis-Test ist ein nicht-parametrischer Test, der keine Annahmen über die Homogenität der Varianzen oder die Normalverteilung der Daten erfordert und somit robuster gegenüber Verletzungen dieser Voraussetzungen ist.

Der Kruskal-Wallis-Test ergab signifikante Unterschiede zwischen den Gruppen ($\chi^2 = 437.49$, $df = 4$, $p < 2.2 \times 10^{-16}$). Der sehr hohe Wert der Teststatistik (χ^2 = 437.49) deutet darauf hin, dass es erhebliche Unterschiede in den Antwortzeiten zwischen den untersuchten Methoden gibt. Freiheitsgrade von 4 entsprechen der Anzahl der Methoden minus eins, was in diesem Fall bedeutet, dass die Unterschiede in den Daten über alle fünf Methoden hinweg analysiert wurden. Ein p-Wert kleiner als 0.05 weist darauf hin, dass mindestens eine der Gruppen signifikant unterschiedlich ist. Dies deutet darauf hin, dass die Antwortzeiten zwischen den verschiedenen Methoden unterschiedlich sind.

Um herauszufinden, welche spezifischen Gruppen sich unterscheiden, wurden anschließend paarweise Vergleiche mit dem Dunn-Test durchgeführt, wobei die Bonferroni-Korrektur angewendet wurde, um die Wahrscheinlichkeit von Typ-I-Fehlern zu verringern.

Der Dunn-Test ist ein nicht-parametrischer Post-hoc-Test, der verwendet wird, um paarweise Vergleiche nach einem Kruskal-Wallis-Test durchzuführen. Dieser Test hilft, festzustellen, welche spezifischen Gruppen sich signifikant voneinander unterscheiden.

Die Bonferroni-Korrektur wird angewendet, um die Wahrscheinlichkeit von Typ-I-Fehlern (fälschlicherweise als signifikant erkannte Unterschiede) zu verringern. Bei der Bonferroni-Korrektur wird das Signifikanzniveau (gewöhnlich 0.05) durch die Anzahl der Vergleiche

geteilt. Dies führt zu strengeren Kriterien für die Signifikanz und reduziert die Wahrscheinlichkeit, dass ein zufälliger Unterschied als signifikant angesehen wird.

Die paarweisen Vergleiche zeigten die folgenden Ergebnisse:

- **Tor vs. Cloudflare DNS:** Es gibt einen signifikanten Unterschied ($p < 2.2 \times 10^{-34}$). Dies bedeutet, dass die Antwortzeiten von Tor signifikant höher sind als die von Cloudflare DNS.
- **Tor vs. Google DNS:** Es gibt einen signifikanten Unterschied ($p < 1.39 \times 10^{-79}$). Dies bedeutet, dass die Antwortzeiten von Tor signifikant höher sind als die von Google DNS.
- **Tor vs. OpenNIC DNS:** Es gibt einen signifikanten Unterschied ($p < 9.11 \times 10^{-60}$). Dies bedeutet, dass die Antwortzeiten von Tor signifikant höher sind als die von OpenNIC.
- **Tor vs. VPN:** Es gibt einen signifikanten Unterschied ($p < 4.45 \times 10^{-49}$). Dies bedeutet, dass die Antwortzeiten von Tor signifikant höher sind als die vom VPN.

Diese Ergebnisse zeigen, dass die Antwortzeiten von Tor signifikant höher sind als die der VPN- und DNS-Resolver-Änderungsmethode. Dies bestätigt die Hypothese, dass Tor längere Antwortzeiten hat.

5.4. Interpretation der Ergebnisse

Die empirischen Daten in Tabelle 5.2 untermauern die theoretischen Vor- und Nachteile der verschiedenen Umgehungstechniken, die in Tabelle 2.1 im Kapitel 2 diskutiert wurden. Diese Daten ermöglichen eine Analyse, wie effektiv die theoretisch diskutierten Techniken in der Praxis tatsächlich sind und welche spezifischen Herausforderungen dabei auftreten. Die Erkenntnisse aus dieser Analyse wurden genutzt, um die Wirksamkeit dieser Techniken in der Praxis zu überprüfen. Die Verknüpfung der praktischen Ergebnisse dieser Arbeit mit den theoretischen Grundlagen ermöglicht eine umfassende Bewertung der Anwendbarkeit und Effektivität technischer Methoden zur Umgehung von Netzsperren in Österreich.

Die Analyse und der Vergleich der unterschiedlichen Umgehungstechniken für Netzsperren offenbaren eine klare Differenzierung in der Eignung dieser Methoden abhängig von den spezifischen Anforderungen der Nutzer*innen. Hervorzuheben sind hier DNS-basierte Methoden wie Google DNS, Cloudflare DNS und OpenNIC. Diese zeichnen sich durch ihre Median Antwortzeit von 0,14 Sekunden, was sie als geeignet für Nutzer*innen macht, die einen schnellen und ununterbrochenen Zugang zu Online-Inhalten benötigen. In DNS-gesperrten Umgebungen wie in Österreich, zeigen sie somit schnellen und umfangreichen Zugang zu Internetressourcen ohne Zensurgefahr durch lokale ISPs. Die Änderung des DNS-Resolvers ist nicht nur aufgrund der hohen Geschwindigkeit, sondern auch aufgrund der 92,33 % Erfolgsquote bei der Auflösung von DNS-Anfragen ein zuverlässiges Werkzeug zur

Überwindung von DNS-basierten Zugangsbeschränkungen. Die Fähigkeit dieser Dienste, schnell auf Anfragen zu reagieren und dabei eine hohe Erfolgsrate zu erzielen, unterstützt die theoretische Annahme, dass eine effiziente DNS-Auflösung zentral für die Umgehung von Sperren ist. OpenNIC bietet eine interessante Alternative, da es den Nutzer*innen eine gewisse Unabhängigkeit von etablierten Akteuren wie Google und Cloudflare im Internet bietet.

Auf der anderen Seite stehen Technologien wie VPN und das Tor-Netzwerk, deren Stärken in stark regulierten oder überwachten Umgebungen zum Tragen kommen könnten, da diese Technologien nicht nur in der Lage sind, den gesamten Datenverkehr zu verschlüsseln, sondern auch die IP-Adressen der Nutzer*innen zu anonymisieren, was für die Wahrung der Privatsphäre und Anonymität von entscheidender Bedeutung sein sollte. Es wäre interessant in weiteren Studien zu Untersuchung, inwieweit der in der Theorie beschrieben Verschlüsselungs- und Sicherheitsaspekt in der Praxis zum Tragen kommt. Obwohl die Verwendung dieser Methoden in der Regel mit langsameren Antwortzeiten verbunden ist, stellen diese voraussichtlich einen akzeptablen Kompromiss für Nutzer*innen dar, die besonderen Wert auf die Sicherheit ihrer Online-Kommunikation legen. Die langsameren Verbindungsgeschwindigkeiten sind eine direkte Folge der komplexen Verschlüsselungsprotokolle und des mehrfachen Routings über verschiedene Server, die erforderlich sind, um Anonymität und Sicherheit zu gewährleisten.

Die empirischen Ergebnisse der praktischen Überprüfung verschiedener Umgehungsmethoden spiegeln die in der Konzeption des Lösungsansatzes geäußerten Bedenken gegen die Verwendung von IP-Adressen wider, insbesondere bei HTTPS-Anfragen. Bei dieser Methode treten häufig Zertifikatsfehler auf, da SSL/TLS-Zertifikate typischerweise an Domainnamen und nicht direkt an IP-Adressen gebunden sind. Wenn also eine HTTPS-Anfrage direkt an eine IP-Adresse gesendet wird, kann es zu einer Diskrepanz zwischen der IP-Adresse und dem im Zertifikat angegebenen Domainnamen kommen. Dies führt zu Warnungen oder Fehlern im Browser, da die Authentizität der Verbindung nicht überprüft werden kann. Diese Problematik zeigt sich deutlich in der erhöhten Anfälligkeit für Sicherheitsrisiken. Ohne korrekte Zertifikatsvalidierung ist der Datenverkehr über HTTPS nicht sicher vor Man-in-the-Middle-Angriffen, bei denen Angreifer*innen Daten abfangen, einsehen oder manipulieren können. In Umgebungen, in denen die Sicherheit der Kommunikation von Bedeutung ist, würde die Verwendung von IP-Adressen zur Umgehung von DNS-Sperren daher ein erhebliches Risiko darstellen.

Zusammenfassend lässt sich festhalten, dass die theoretischen Diskussionen in Kapitel 2 durch die empirischen Daten weitgehend bestätigt werden, was die Wichtigkeit einer sorgfältigen Auswahl der Umgehungsmethode basierend auf den spezifischen Anforderungen und Risiken der Nutzer*innen unterstreicht.

6. Schlussfolgerungen

In diesem Kapitel werden die Ergebnisse der Untersuchung zusammengefasst und interpretiert. Es wird analysiert, inwieweit die Ziele der Arbeit erreicht wurden und welche neuen Erkenntnisse gewonnen werden konnten. Darüber hinaus werden die Methodik und die Ergebnisse kritisch reflektiert und ihre Bedeutung für den Stand der Forschung diskutiert.

6.1. Beantwortung der Forschungsfrage

Die Forschungsfrage lautet: *Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen?*

Die durchgeführten Tests und Analysen haben gezeigt, dass die verschiedenen Methoden zur Umgehung von DNS-Sperren unterschiedlich effektiv sind. Die DNS-Resolver-Methoden (Google DNS, Cloudflare DNS und OpenNIC) zeigten insgesamt eine hohe Erfolgsquote bei der Umgehung von DNS-Sperren. Insbesondere Google DNS erzielte mit 94,03 % die höchste Erfolgsrate, gefolgt von Cloudflare DNS mit 93,75 % und OpenNIC mit 89,20 %. Diese Ergebnisse bestätigen, dass Änderungen am DNS-Resolver eine effektive Methode zur Umgehung von DNS-Sperren darstellen.

VPNs und das Tor-Netzwerk zeigten ebenfalls hohe Erfolgsraten, wobei VPNs eine Erfolgsrate von 93,75 % und Tor eine Erfolgsrate von 89,77 % erreichten. Diese Methoden können neben der Umgehung von DNS-Sperren zusätzliche Vorteile hinsichtlich der Anonymität und Sicherheit der Nutzer*innen bieten. Insbesondere Tor könnte sich durch ein hohes Maß an Anonymität und Schutz der Privatsphäre der Nutzer*innen auszeichnen, auch wenn es im Vergleich zu den anderen Methoden längere Antwortzeiten aufweist.

Die Methode der direkten Verwendung einer IP-Adresse zur Umgehung von DNS-Sperren hat sich als ungeeignet erwiesen. Empirische Analysen haben gezeigt, dass die direkte Verwendung von IP-Adressen erhebliche Einschränkungen aufweist. Eines der Hauptprobleme dieser Methode besteht darin, dass Webseiten virtuelle Hosts verwenden können, die mehrere Domainnamen unter einer einzigen IP-Adresse hosten. Ohne die Verwendung des Domainnamens kann der Server die angeforderte Website nicht richtig zuordnen, was zu einem Fehler führt. Dies ist besonders problematisch bei Websites, die HTTPS verwenden, da das Zertifikat dem Domainnamen und nicht der IP-Adresse entsprechen muss. Diese Diskrepanz führt zu Zertifikatsfehlern und verhindert den Zugriff auf die Website.

Zusammengefasst lassen sich die Ergebnisse wie folgt darstellen:

Methode	**Eignung zur Umgehung von Netzsperren**	**Erfolgsrate**
Google DNS	Ja	94,03 %
Cloudflare DNS	Ja	93,75 %
OpenNIC DNS	Ja	89,20 %
VPN	Ja	93,75 %
Tor	Ja	89,77 %
Direkte IP-Adressen-Verwendung	Nein	N/A

Tabelle: 6.1.: Erfolgsraten und Eignung der verschiedenen Umgehungsmethoden von Netzsperren in Österreich.

Diese Ergebnisse in Tabelle 6.1 zeigen, dass DNS-Resolver-Änderungen, VPNs und das Tor-Netzwerk effektive Methoden zur Umgehung von DNS-Sperren in Österreich sind. Die direkte Verwendung von IP-Adressen ist nicht geeignet.

6.2. Bewertung der Hypothese

Des Weiteren werden an dieser Stelle der Arbeit die in der empirischen Analyse aufgestellten Hypothesen bewertet.

Hypothese H1, *Es besteht ein negativer Zusammenhang zwischen der Erfolgsrate der Umgehungsmethoden und der Antwortzeit. Das bedeutet, je höher die Erfolgsrate einer Methode, desto geringer tendenziell die Antwortzeit.*, kann nicht bestätigt werden.

Es besteht ein negativer Zusammenhang zwischen der Erfolgsrate der Umgehungsmethoden und der Antwortzeit. Dies wurde durch eine Korrelationsanalyse untersucht, wobei der Spearman-Rangkorrelationskoeffizient (r_s) berechnet wurde. Der Wert von $r_s = -0.359$ ($p = 0.553$) deutet auf einen moderaten negativen Zusammenhang hin, der jedoch statistisch nicht signifikant ist.

Hypothese H2, *Die Antwortzeiten von Tor sind signifikant höher als die der Umgehungsmethode VPN und DNS-Resolver ändern.*, wurde bestätigt.

Die Antwortzeiten von Tor sind signifikant höher als die von VPN und der DNS-Resolver-Änderungsmethode. Diese Hypothese wurde zunächst mittels ANOVA untersucht, jedoch zeigte der Levene-Test, dass die Varianzen nicht homogen sind ($F(4, 1343) = 14.614$, $p < 1.089 \times 10^{-11}$). Daher wurde der Kruskal-Wallis-Test verwendet, der signifikante Unterschiede zwischen den Gruppen ergab ($\chi^2 = 437.49$, $df = 4$, $p < 2.2 \times 10^{-16}$). Die Dunn-Tests mit Bonferroni-Korrektur zeigten signifikante Unterschiede zwischen den Antwortzeiten von Tor und den verglichenen Methoden, was Hypothese H2 bestätigt.

6.3. Bezug der Ergebnisse zum Forschungsstand

In diesem Abschnitt werden die empirischen Ergebnisse mit dem aktuellen Forschungsstand verknüpft. Es wird untersucht, welche neuen Erkenntnisse durch diese Arbeit gewonnen wurden, wie sich diese in den bestehenden theoretischen Kontext einfügen und welche praktischen Implikationen sich daraus ergeben. Dabei wird ein Vergleich mit bestehenden Studien und Theorien vorgenommen, um die Position dieser Arbeit innerhalb der wissenschaftlichen Diskussion zu verdeutlichen und die spezifischen Beiträge zur Weiterentwicklung des Forschungsfeldes herauszuarbeiten.

6.3.1. Theoretischer Hintergrund

Im theoretischen Teil dieser Arbeit wurde untersucht, welche Arten von Netzsperren in Österreich eingesetzt werden und welche Umgehungsmethoden sich dafür eignen. Dabei hat sich herausgestellt, dass in Österreich DNS-Sperren zur Zensur von Internetinhalten verwendet werden. Diese Erkenntnis wurde durch eine umfassende Literaturrecherche und die Analyse regulatorischer Dokumente bestätigt.

DNS-Sperren funktionieren, indem Internet Service Provider (ISPs) DNS-Anfragen zu bestimmten Domainnamen blockieren oder manipulieren, sodass die entsprechenden Webseiten für die Nutzer*innen nicht erreichbar sind. Diese Form der Zensur wird häufig eingesetzt, um den Zugang zu illegalen oder unerwünschten Inhalten zu verhindern.

Vier spezifische Umgehungsmethoden wurden identifiziert und im theoretischen Teil ausführlich diskutiert:

- **Verwendung einer alternativen IP-Adresse:** Diese Methode umgeht DNS-Sperren, indem direkt die IP-Adresse der Zielwebseite eingegeben wird, anstatt ihren DNS-Namen zu verwenden.
- **Ändern des DNS-Resolvers:** Durch die Konfiguration eines alternativen DNS-Resolvers, der nicht von lokalen ISPs kontrolliert wird, können Nutzer*innen die DNS-Sperren umgehen.
- **VPN (Virtual Private Network):** VPNs verschlüsseln den gesamten Internetverkehr und leiten ihn über einen Server in einem anderen Land um, wodurch DNS-Anfragen verschleiert werden und ein eigener DNS-Resolver des VPN-Anbieters verwendet werden kann.
- **Tor-Netzwerk:** Das Tor-Netzwerk bietet Anonymität, indem es den Internetverkehr über mehrere Server weltweit verteilt und eine eigene Methode zur Auflösung von Domainnamen innerhalb des Netzwerks verwendet.

Diese Umgehungsmethoden wurden auf der Grundlage der verfügbaren Literatur hinsichtlich ihrer Vor- und Nachteile bewertet. Die theoretische Analyse ergab, dass jede Methode spezifische Stärken und Schwächen aufweist, die je nach Anwendungsszenario variieren können. Beispielsweise bieten VPNs und das Tor-Netzwerk Anonymität und

Sicherheit, jedoch auch längere Antwortzeiten, während die Änderung des DNS-Resolvers eine schnellere und einfachere Lösung darstellt.

Die empirische Untersuchung dieser Arbeit hat diese theoretischen Erkenntnisse bestätigt. Es wurde festgestellt, dass DNS-Manipulationen von ISPs in Österreich tatsächlich durchgeführt werden. Die Vor- und Nachteile der theoretisch identifizierten Umgehungsmethoden wurden in der Praxis nachvollzogen und validiert, was die Robustheit der theoretischen Modelle und Annahmen unterstreicht, wobei die Wahl der Methode von den spezifischen Anforderungen und Nutzungskontexten abhängt.

6.3.2. Vergleich mit bestehender Literatur

Die Forschung zu Umgehungsmethoden von Netzsperren hat eine Vielzahl Studien, insbesondere in Ländern mit strenger Internetzensur wie China und Iran, hervorgebracht. In anderen Ländern durchgeführte Studien liefern wertvolle Einblicke in die verschiedenen Techniken, die von Regierungen und ISPs zur Durchsetzung von Netzsperren verwendet werden, sowie in die Methoden, die Nutzer*innen anwenden können, um diese Sperren zu umgehen. Im Gegensatz zu den meisten bisherigen Studien, die sich auf Länder mit strenger Zensur konzentrieren, untersucht diese Arbeit die Umgehungsmethoden von DNS-Sperren im spezifischen österreichischen Kontext. Bisher gab es in Österreich vor allem Studien zu den rechtlichen Aspekten von Netzsperren und theoretische Erörterungen zu Umgehungsmethoden, jedoch keine umfassende empirische Analyse der praktischen Anwendung dieser Methoden. Die vorliegende Arbeit schließt diese Lücke, indem sie eine detaillierte Bewertung der Effektivität und Effizienz verschiedener Umgehungsmethoden unter realen Bedingungen in Österreich liefert.

Eine der umfassendsten Studien zur DNS-Injektion wurde von Wander et al. durchgeführt. In ihrer Arbeit „Measurement of Globally Visible DNS Injection“ [Wa14] untersuchten sie, wie DNS-Injektionen als Zensurmaßnahme eingesetzt werden, insbesondere in China und Iran. Diese Studie zeigte, dass DNS-Injektion eine weit verbreitete Methode ist, die Deep Paket Inspection verwendet, um gefälschte DNS-Antworten zu erzeugen, und dabei auch unbeteiligte Dritte beeinträchtigt, wenn deren Datenverkehr durch zensierte Netzwerke geleitet wird. Beispielsweise konnte die Studie von Wander et al. die Wirksamkeit von DNS-Resolver-Änderungen wie der Nutzung von Google DNS und OpenDNS zeigen, um DNS-Sperren zu umgehen. Diese Erkenntnisse wurden durch die vorliegende Arbeit bestätigt, da sowohl Google DNS als auch Cloudflare DNS erfolgreich bei der Umgehung von DNS-Sperren in Österreich sind.

Eine weitere wichtige Studie stammt von Halderman et al. [AAH13], die sich mit der Internetzensur im Iran beschäftigt und herausgefunden hat, dass neben der DNS-Injektion auch die HTTP-Filterung eine zentrale Rolle spielt. Dies bestätigt die Beobachtung, dass DNS-basierte Sperren häufig durch zusätzliche Maßnahmen ergänzt werden, um eine umfassendere Zensur zu gewährleisten. Darüber hinaus zeigt die vorliegende Arbeit, dass VPNs und das Tor-Netzwerk effektive Mittel zur Umgehung von Netzsperren sind, was im Einklang mit den Studien von Halderman et al. steht, die die Bedeutung von

Verschlüsselung und Anonymisierung zur Umgehung von Zensur betonen. Die Ergebnisse der vorliegenden Arbeit zeigen aber auch, dass diese Methoden mit längeren Antwortzeiten verbunden sind, was in anderen Studien oft nur am Rande erwähnt wird.

Die Ergebnisse dieser Arbeit bestätigen und erweitern die bestehenden Theorien und Modelle über Umgehungsmethoden.

6.3.3. Neue Erkenntnisse

Durch diese Arbeit konnten fundierte wissenschaftliche Erkenntnisse über die Erfolgsraten und Antwortzeiten verschiedener Umgehungsmethoden von Netzsperren gewonnen werden. Diese Erkenntnisse tragen maßgeblich zur bestehenden Forschung bei und liefern eine detaillierte Analyse der praktischen Anwendbarkeit dieser Methoden unter den spezifischen Bedingungen in Österreich.

Ein bedeutender Beitrag dieser Arbeit ist die Bestätigung, dass DNS-Resolver-Änderungsmethoden, wie Google DNS, Cloudflare DNS und OpenNIC, effektive Lösungen für die Umgehung von DNS-Sperren darstellen. Die empirischen Daten zeigen, dass diese Methoden Erfolgsraten von 92,33 % haben und Median-Antwortzeiten von 0,14 Sekunden aufweisen. Diese Ergebnisse stützen die theoretischen Annahmen, die in der bestehenden Literatur diskutiert wurden, und bieten eine solide empirische Grundlage, die die praktische Anwendbarkeit dieser Techniken unterstreicht.

Die Methode der direkten Verwendung von IP-Adressen hat sich als weniger geeignet erwiesen, was auf die häufigen Zertifikatsfehler bei HTTPS-Anfragen zurückzuführen ist. Diese Erkenntnis verdeutlicht die Risiken und Einschränkungen dieser Technik, da SSL/TLS-Zertifikate typischerweise an Domainnamen gebunden sind. Diese Ergebnisse bestätigen die theoretischen Bedenken und liefern wichtige Hinweise für die praktische Anwendung dieser Methode.

Ein weiteres wichtiges Ergebnis ist die Feststellung, dass VPNs und das Tor-Netzwerk trotz ihrer längeren Antwortzeiten robuste Werkzeuge zur Wahrung der Privatsphäre und zur Umgehung von Zensur darstellen. Diese Erkenntnisse ergänzen die bestehende Forschung und bieten wertvolle Einblicke in die praktischen Vorteile und Herausforderungen der Nutzung von VPNs und Tor.

Die Untersuchung der Auswirkungen von der Geolokalisation und Content Delivery Networks (CDNs) auf die Effektivität der Umgehungsmethoden stellt einen wichtigen Aspekt in der Forschung dar. Die Ergebnisse zeigen, dass geografische Unterschiede und die Nutzung von CDNs zu variierenden Erfolgsraten führen können. Diese Unterschiede können sich erheblich auf die Wirksamkeit der Umgehungsmethoden auswirken, je nachdem, wo die Anfragen gestellt werden. Diese Erkenntnisse erweitern das Verständnis der bestehenden Forschung und heben die Komplexität der Umgehung von Netzsperren in verschiedenen geografischen und technischen Kontexten hervor.

Zusätzlich zu den empirischen Erkenntnissen über die spezifischen Umgehungsmethoden bietet diese Arbeit auch methodische Beiträge zur Forschung. Die Verwendung von anerkannten Tools wie Psiphon, Google DNS, Cloudflare DNS, OpenNIC und dem Tor-Netzwerk, kombiniert mit einer statistischen Analyse, stellt sicher, dass die Ergebnisse sowohl zuverlässig als auch aussagekräftig sind. Diese methodischen Ansätze können als Grundlage für zukünftige Studien dienen und die Forschung in diesem Bereich weiter vorantreiben.

6.3.4. Praktische Implikationen

Die Ergebnisse dieser Arbeit haben mehrere wichtige praktische Implikationen für die Anwendung von Umgehungsmethoden in Österreich und allgemein.

Erstens können Nutzer*innen, die sich durch Netzsperren in Österreich eingeschränkt fühlen, die Ergebnisse dieser Arbeit nutzen, um fundierte Entscheidungen darüber zu treffen, welche Umgehungsmethoden für sie am effektivsten sind. Die empirischen Daten zeigen, dass DNS-Resolver-Änderungsmethoden wie Google DNS und Cloudflare DNS schnelle und zuverlässige Lösungen bieten. Für Nutzer*innen, die Wert auf Anonymität und Sicherheit legen, bieten VPNs und das Tor-Netzwerk effektive Alternativen, auch wenn diese mit längeren Antwortzeiten verbunden sind. Diese Informationen ermöglichen es den Nutzer*innen, die für ihre spezifischen Bedürfnisse und Kontexte geeignetste Methode auszuwählen.

Zweitens können die entwickelten Python-Skripte von weiteren Forscher*innen eingesetzt werden, um DNS-Sperren in anderen lokalen oder globalen Kontexten zu analysieren. Die Skripte sind so gestaltet, dass sie flexibel und anpassbar sind, wodurch sie in verschiedenen Netzwerkkonfigurationen und geografischen Regionen verwendet werden können. Dies fördert die Weiterentwicklung der empirischen Forschung zu Netzsperren und Umgehungsmethoden und unterstützt die Erstellung vergleichbarer Datensätze, die eine breitere Analyse ermöglichen.

Drittens bieten die Ergebnisse dieser Arbeit wertvolle Einblicke für politische Entscheidungsträger*innen und Regulierungsbehörden. Die Erkenntnisse über die Wirksamkeit und die Grenzen von DNS-Sperren und deren Umgehung können genutzt werden, um bestehende Zensurmaßnahmen zu bewerten und zu verbessern. Darüber hinaus können sie dazu beitragen, die Diskussion über die Balance zwischen Internetzensur und freiem Zugang zu Informationen zu informieren und zu bereichern.

Schließlich haben die Erkenntnisse dieser Arbeit auch Implikationen für die technische Entwicklung und Verbesserung von Umgehungstechnologien. Die identifizierten Schwächen und Herausforderungen bei der Verwendung bestimmter Methoden, wie beispielsweise Zertifikatsherausforderungen bei der Verwendung von IP-Adressen, können Entwickler*innen helfen, neue Lösungen zu entwickeln, die diese Einschränkungen überwinden und die Effizienz und Benutzerfreundlichkeit von Umgehungstechnologien erhöhen.

Zusammenfassend bieten die praktischen Implikationen dieser Arbeit wertvolle Leitlinien für Nutzer*innen, Forscher*innen, politische Entscheidungsträger*innen und Entwickler*innen. Sie unterstützen die Anwendung und Weiterentwicklung von Umgehungsmethoden, fördern die empirische Forschung und tragen zur informierten Gestaltung von Internetregulierungen bei.

6.4. Kritische Reflexion der Methodik

In diesem Abschnitt werden die verwendeten methodischen Ansätze sowie die Qualität und Zuverlässigkeit der erhobenen Daten bewertet. Die folgende Diskussion gibt einen Einblick in die Stärken und Grenzen der Untersuchung und stellt die gewonnenen Erkenntnisse in den Kontext ihrer praktischen Anwendbarkeit und Relevanz.

6.4.1. Methodische Überlegungen

Der methodische Ansatz dieser Arbeit kombiniert eine theoretische Fundierung mit einer empirischen Untersuchung, um die Wirksamkeit von Umgehungsmethoden von Netzsperren in Österreich umfassend zu evaluieren. Im Kapitel 2 wurde geklärt, dass DNS-Sperren in Österreich zur Zensur eingesetzt werden, darauf aufbauend wurden die relevanten Umgehungstechniken identifiziert.

Die empirische Analyse konzentriert sich auf die Frage, ob die verschiedenen Umgehungsmethoden korrekte IP-Adressen zurückgeben, was für die Beurteilung der Wirksamkeit der einzelnen Methoden von entscheidender Bedeutung ist. Für die Untersuchung wurden die drei größten ISPs in Österreich ausgewählt, um ein repräsentatives Bild der durchschnittlichen Internetnutzung in Österreich zu erhalten. Diese Auswahl der ISPs zielt darauf ab, ein breites Spektrum an Netzwerkumgebungen zu erfassen und sicherzustellen, dass die Ergebnisse für einen Großteil der österreichischen Internetnutzer*innen relevant sind.

Dieser methodische Ansatz ermöglicht es, nicht nur die technische Funktionsweise der verschiedenen Umgehungstechniken zu evaluieren, sondern auch ihre praktische Anwendbarkeit in realen Netzwerkszenarien zu überprüfen. Durch die Kombination von theoretischen Untersuchungen und gezielten empirischen Tests wird eine solide Basis geschaffen, um fundierte Aussagen über die Wirksamkeit der untersuchten Umgehungsmethoden treffen zu können.

6.4.2. Datenqualität und Zuverlässigkeit

Die Sicherstellung der Datenqualität und Zuverlässigkeit spielte eine entscheidende Rolle für die Glaubwürdigkeit der Ergebnisse dieser Arbeit. Die Datenquellen wurden sorgfältig ausgewählt, um nur zuverlässige und anerkannte Informationsquellen zu verwenden. Die verwendeten Daten zu gesperrten Webseiten stammen von `data.gv.at`,

einer vertrauenswürdigen Plattform, die öffentlich zugängliche Daten zur Verfügung stellt. Zusätzliche Informationen über die Anzahl und den Marktanteil der größten ISPs in Österreich wurden von der Regulierungsbehörde RTR eingeholt, wodurch eine hohe Zuverlässigkeit und Relevanz dieser Daten gewährleistet ist.

Für die empirischen Messungen wurden anerkannte Tools wie Psiphon, Google DNS, Cloudflare DNS, OpenNIC und das Tor-Netzwerk verwendet. Diese Tools wurden ausgewählt, da sie in realen Nutzungsszenarien weit verbreitet sind und somit eine praxisnahe Bewertung der Umgehungsmethoden ermöglichen. Um die Genauigkeit der Datenerhebung weiter zu erhöhen, wurden die Skripte zur Erfassung der IP-Daten mehrfach überprüft und validiert. Diese Schritte stellen sicher, dass die erhobenen Daten korrekt sind und die tatsächlichen Bedingungen der Internetnutzung in Österreich widerspiegeln.

Zusätzlich wurde eine statistische Auswertung durchgeführt, um eine objektive Interpretation der erhobenen Daten zu ermöglichen. Diese methodischen Maßnahmen stellen sicher, dass die Ergebnisse dieser Studie sowohl zuverlässig als auch aussagekräftig sind und somit wertvolle Erkenntnisse über die Wirksamkeit der untersuchten Umgehungsmethoden liefern.

6.4.3. Einschränkungen und Herausforderungen

Die Untersuchung unterliegt einigen Einschränkungen und Herausforderungen, die ihre Aussagekraft und Verallgemeinerbarkeit beeinflussen können. Eine wesentliche Einschränkung ist die dynamische Natur des Internets, die zu ständigen Veränderungen in der Struktur und Verwaltung des Netzes führt. Diese Dynamik kann die langfristige Gültigkeit der Ergebnisse beeinträchtigen, da sich die Bedingungen, unter denen die Daten erhoben wurden, ändern können.

Eine weitere Herausforderung stellt der Einsatz von Content Delivery Networks (CDNs) und Geolocation-Technologien dar. Diese Technologien optimieren die Auslieferung von Inhalten auf der Grundlage des geografischen Standorts der Nutzer*innen. In der Praxis bedeutet dies, dass Nutzer*innen, die über einen Tor Exit Node oder VPN in Österreich verbunden sind, möglicherweise andere IP-Auflösungen erhalten als Nutzer*innen in anderen Ländern. Diese geografischen Unterschiede können zu unterschiedlichen Suchergebnissen führen, je nachdem, wo die Anfragen gestellt werden.

Ein weiterer Aspekt der methodischen Reflexion betrifft die Fokussierung auf IPv4-DNS-Ergebnisse, während IPv6-Daten nicht berücksichtigt wurden. Diese Entscheidung basiert auf der weiterhin weit verbreiteten Nutzung von IPv4-Adressen. Die empirische Tests haben gezeigt, dass bei DNS-Abfragen es nicht aufgetreten ist, dass nur IPv6-Adressen und keine IPv4-Adressen für die untersuchten Domains zurückgegeben wurde. Die Nichtberücksichtigung von IPv6 stellt eine Einschränkung dar, da potenziell relevante Daten über die Effektivität von Umgehungsmethoden im Zusammenhang mit IPv6-DNS-Sperren fehlen. Die Generalisierbarkeit der Ergebnisse ist somit eingeschränkt, dennoch sind die Erkenntnisse aus der Untersuchung der IPv4-DNS-Sperren wertvoll und bieten eine solide Grundlage für zukünftige Forschungen, die IPv6 einbeziehen könnten.

Diese Einschränkungen unterstreichen die Notwendigkeit, die Ergebnisse der Studie mit Vorsicht zu interpretieren und die spezifischen Bedingungen der Datenerhebung bei der Bewertung der Anwendbarkeit und Effektivität der untersuchten Umgehungsmethoden zu berücksichtigen.

Insgesamt betrachtet, zeichnet sich die Untersuchung durch eine hohe methodische Sorgfalt aus. Die gewählten Ansätze und Werkzeuge ermöglichten es, fundierte Erkenntnisse über die Effektivität von Umgehungsmethoden unter den spezifischen Bedingungen in Österreich zu gewinnen. Zukünftige Forschungen könnten von einer Erweiterung der geografischen und technischen Reichweite der Tests profitieren, um die Robustheit der Ergebnisse weiter zu erhöhen.

7. Zusammenfassung und Ausblick

Dieses Kapitel fasst die Arbeit zusammen und gibt einen Ausblick auf zukünftige Forschungsrichtungen. Dabei werden die wichtigsten Erkenntnisse und deren Bedeutung sowohl für die Wissenschaft als auch für die Praxis hervorgehoben.

7.1. Zusammenfassung

Kapitel 1 der Masterarbeit bietet eine Einführung in das Thema Netzsperren in Österreich. Es wird dargelegt, dass Netzsperren zunehmend kontrovers diskutiert werden, da sie nicht nur den Zugang zu unerwünschten Inhalten blockieren, sondern auch legitime Dienste beeinträchtigen können. Außerdem wird die zentrale Forschungsfrage vorgestellt, welche lautet: *Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen?* Das Kapitel definiert die Hauptziele der Arbeit, darunter die Identifikation und Bewertung verschiedener Umgehungsmethoden und deren empirische Untersuchung. Nicht-Ziele, wie die rechtliche und politische Analyse, werden ebenfalls klar abgegrenzt, um den Fokus auf die technischen Aspekte zu schärfen. Für die Beantwortung der Forschungsfrage wird das Forschungsdesign der experimentellen Analyse angewandt. Dabei wird zuerst ein Konzept für die Untersuchung entwickelt, das anschließend in die Praxis umgesetzt wird.

Kapitel 2 dieser Arbeit behandelt die Mechanismen und Methoden von Netzsperren sowie deren Umgehung im spezifischen Kontext Österreichs. Es wird beschrieben, dass DNS-Sperren von ISPs eingesetzt werden, um den Zugang zu bestimmten Internetinhalten zu blockieren. Diese Maßnahmen werden technisch durch DNS-Manipulationen umgesetzt. Es werden die Vor- und Nachteile verschiedener Umgehungsmethoden wie IP-Adressen verwenden, DNS-Resolver-Änderungen, VPNs und das Tor-Netzwerk thematisiert.

Historische Entwicklungen des Internets in Österreich und die Rolle der ISPs werden ebenso behandelt wie grundlegende Internetstandards und -protokolle. Netzneutralität und Internetfreiheit, die im Zusammenhang mit Netzsperren von großer Bedeutung sind, werden diskutiert.

Der rechtliche Rahmen für Netzsperren in Österreich basiert auf Gesetzen wie dem Urheberrechtsgesetz und EU-Vorschriften. Schließlich werden bestehende Forschungslücken identifiziert, insbesondere das Fehlen empirischer Analysen der praktischen Anwendung von Umgehungsmethoden in Österreich.

Kapitel 3 beschreibt den methodischen Ansatz zur Untersuchung der Wirksamkeit von Umgehungsmethoden für Netzsperren in Österreich. Die Arbeit kombiniert eine theoretische Fundierung mit einer empirischen Untersuchung, um ein umfassendes Verständnis der DNS-Sperren und deren Umgehung zu gewinnen.

Der Testaufbau umfasst die Auswahl der Internet Service Provider (ISPs), der Zielseiten und der Umgehungsmethoden. Die drei größten ISPs (A1, Drei und Magenta) in Österreich, welche gemeinsam 84 % Marktanteil haben, werden für die Untersuchung ausgewählt. Zielseiten werden auf Basis der Daten zu Netzsperren von ISPs, welche von der RTR auf `https://www.data.gv.at/katalog/de/dataset/netzsperren` zur Verfügung gestellt werden, ausgewählt. Vier Umgehungsmethoden werden für die experimentelle Analyse ausgewählt: IP-Adresse verwenden, DNS-Resolver ändern, VPN und Tor.

Kapitel 4 beschreibt die experimentelle Analyse, welche die detaillierte Durchführung der Tests beinhaltet. In diesem Kapitel werden außerdem die zwei zentralen Hypothesen formuliert:

- Hypothese H1: *Es besteht ein negativer Zusammenhang zwischen der Erfolgsrate der Umgehungsmethoden und der Antwortzeit. Das bedeutet, je höher die Erfolgsrate einer Methode, desto geringer tendenziell die Antwortzeit.*
- Hypothese H2: *Die Antwortzeiten von Tor sind signifikant höher als die der Umgehungsmethode VPN und DNS-Resolver ändern.*

Zur Untersuchung der Hypothese H1, die einen negativen Zusammenhang zwischen der Erfolgsrate der Umgehungsmethoden und der Antwortzeit postuliert, wird eine Korrelationsanalyse durchgeführt. Zur Untersuchung der Hypothese H2, die signifikant höhere Antwortzeiten für Tor im Vergleich zu VPN und DNS-Resolver-Änderungsmethode postuliert, wird der Kruskal-Wallis-Test verwendet.

In Schritt 1 bei der Durchführung der Tests wird überprüft, ob die ausgewählten Webseiten tatsächlich einer DNS-Sperre unterliegen. Hierzu wird ermittelt, ob die über die ISP-DNS-Resolver erhaltenen IP-Adressen mit den über autoritative Nameserver ermittelten IPs übereinstimmen. Die autoritativen Nameserver sind dabei jene Server, die direkt von der Top-Level-Domain (TLD) verwaltet werden und die originalen Einträge der Domains besitzen. Im Gegensatz dazu sind die DNS-Resolver der ISPs rekursive Resolver, die ihre Daten von diesen autoritativen Quellen beziehen. ISPs können dabei Maßnahmen ergreifen, um bei gesperrten Domains keine oder andere IP-Adressen gegenüber der autoritativen Nameserver zu übermitteln. Es wird ein eigens entwickeltes Python-Skript eingesetzt, welches die Schritte zur Ermittlung der IP-Adressen durchführt und diese nach Durchführung der Tests der einzelnen Umgehungsmethoden vergleicht. Dabei werden Daten zu den Erfolgsraten und Antwortzeiten der Umgehungsmethoden gesammelt.

In Kapitel 5 werden die Ergebnisse der einzelnen Umgehungsmethoden vorgestellt und eine Hypothesenprüfung durchgeführt. In Kapitel 6 werden Schlussfolgerungen dargelegt, welche eine Beantwortung der Forschungsfrage und eine Hypothesenprüfung beinhaltet.

Folgend die Zusammenfassung der Ergebnisse der identifizierten und evaluierten Umgehungsmethoden:

Umgehungsmethode 1: IP-Adresse verwenden
Die theoretische Idee, DNS-Sperren durch direkte Eingabe der IP-Adresse zu umgehen, stößt in der Praxis auf Herausforderungen, insbesondere bei HTTPS-Anfragen aufgrund von SSL/TLS-Fehlern. Ein Python-Skript testet systematisch die Erreichbarkeit von Webseiten über ihre IP-Adressen und dokumentiert die Ergebnisse. Die Ergebnisse zeigen jedoch, dass diese Methode aufgrund technischer Barrieren und Zertifikatsproblemen nicht geeignet ist.

Umgehungsmethode 2: DNS-Resolver ändern
Die Änderung des im eigenen Netzwerk oder Betriebssystem konfigurierten DNS-Resolvers zu öffentlichen DNS-Resolvern wie Google DNS, Cloudflare DNS und OpenNIC wird getestet, um DNS-Sperren zu umgehen. Ein Python-Skript führt DNS-Abfragen über diese Resolver durch und vergleicht die Ergebnisse mit den autoritativen Nameserver Ergebnissen. Diese Methode erweist sich als effektiv, da öffentliche Resolver oft nicht den lokalen Zensurrichtlinien unterliegen. Google DNS (8.8.8.8) erreicht eine Erfolgsrate von 94,03 %, Cloudflare DNS (1.1.1.1) 93,75 % und OpenNIC (37.252.191.197) 89,20 %. Die Antwortzeiten variieren, wobei Google DNS (Median Antwortzeit: 0,12 Sekunden) die schnellsten Ergebnisse liefert.

Umgehungsmethode 3: VPN
Getestet wird die Nutzung des VPN-Dienstes Psiphon, der einen unzensierten DNS-Resolver verwendet. Ein Python-Skript überprüft die vom VPN-Resolver zurückgegebenen IP-Adressen. Auch diese Methode erweist sich mit einer Trefferquote von 93,75 % als effektiv. VPNs verschlüsseln den gesamten Datenverkehr und bieten zusätzlichen Schutz vor Überwachung und Zensur, auch wenn die Antwortzeiten aufgrund der Verschlüsselung und des Routings länger sind als bei der Umgehungsmethode 2.

Umgehungsmethode 4: Tor
Tor wird getestet, weil es nicht nur die IP-Adresse des Nutzers verbirgt, sondern auch DNS-Anfragen anonymisiert. Ein Python-Skript, das Tor verwendet, führt DNS-Abfragen über das Tor-Netzwerk durch. Tor zeigt eine Erfolgsrate von 89,77 % und erweist sich als robustes Mittel zur Umgehung von DNS-Sperren, trotz längerer Antwortzeiten aufgrund des mehrstufigen Routings zur Anonymisierung.

Methoden zur Überprüfung, ob eine DNS-Sperre vorliegt
Um die Umgehungsmethoden 2, 3 und 4 zu testen und zu analysieren, werden spezifische Funktionen entwickelt und eingesetzt:

- **DNS-Abfragefunktion:** Diese Funktion nimmt eine Domain und einen DNS-Server als Argumente und führt den Befehl `dig` aus, um die DNS-Abfrage durchzuführen. Die Funktion misst die Dauer der Abfrage und speichert die vom DNS-Resolver zurückgegebenen IP-Adressen. Die Funktion gibt die gesammelten IP-Adressen und die Antwortzeit zurück.

- **Vergleichsfunktion:** Diese Funktion vergleicht die IP-Adressen, die von einem DNS-Resolver zurückgegeben werden, mit den bekannten IP-Adressen, die von autoritativen Nameservern bereitgestellt werden. Sie bestimmt, ob eine DNS-Sperre effektiv umgangen wird, indem sie überprüft, ob es eine Überschneidung zwischen beiden IP-Adresssets gibt.

Die Auswertung der Daten zu den Umgehungsmethoden erfolgt durch eine Kombination aus deskriptiven Statistiken und visuellen Darstellungen, um die Effektivität der einzelnen Methoden zu bewerten und vergleichende Einblicke zu gewinnen. Die Erfolgsrate jeder Methode wird als Prozentsatz berechnet. Zur Analyse der Antwortzeiten werden Mittelwert, Median, Standardabweichung und Variationskoeffizient berechnet, um Haupttendenzen und Variabilität zu identifizieren.

Beantwortung der Forschungsfrage
Diese Arbeit kann somit die Forschungsfrage *Welche der identifizierten technischen Umgehungsmethoden von Netzsperren in Österreich können Netzsperren umgehen?* beantworten. Es zeigt sich, dass ein geänderter DNS-Resolver, die Nutzung von VPN und das Tor-Netzwerk effektive Methoden zur Umgehung von Netzsperren in Österreich sind. Die direkte Verwendung von IP-Adressen ist aufgrund technischer und sicherheitsrelevanter Probleme ungeeignet. Die Ergebnisse bieten wertvolle praktische Leitlinien für Nutzer*innen, Forscher*innen, politische Entscheidungsträger*innen und Entwickler*innen. Die entwickelten Python-Skripte und methodischen Ansätze können als Grundlage für zukünftige Studien dienen und die Forschung in diesem Bereich weiter vorantreiben. Die Erkenntnisse tragen zur informierten Gestaltung von Internetregulierungen bei und unterstützen die Entwicklung verbesserter Umgehungstechnologien.

Hypothesenprüfung
Die Hypothese H1, die einen negativen Zusammenhang zwischen der Erfolgsrate und der Antwortzeit postuliert, konnte nicht signifikant bestätigt werden. Die Hypothese H2, dass die Antwortzeiten von Tor signifikant höher sind als die von VPN und DNS-Resolver-Änderungsmethoden, konnte bestätigt werden.

Kritische Aspekte und Herausforderungen
Bei der Analyse wurden auch kritische Aspekte und mögliche Herausforderungen berücksichtigt:

- Caching von DNS-Anfragen: DNS-Resolver speichern Antworten auf frühere Anfragen, um die Antwortzeiten zu verbessern. Dieses Verhalten kann jedoch dazu führen, dass veraltete oder manipulierte Daten verwendet werden, was die Wirksamkeit der Umgehungsmethode beeinträchtigt.

- Geografische Unterschiede: DNS-Dienste können geografisch verteilte Server verwenden, die je nach Standort der Nutzer*innen unterschiedliche IP-Adressen zurückgeben können. Dies wird zwar durch eine erweiterte Prüfung in der Vergleichsfunktion berücksichtigt, kann aber dennoch zu Inkonsistenzen führen.

7.2. Ausblick

Die vorliegende Arbeit bietet eine fundierte Analyse der technischen Methoden zur Umgehung von Netzsperren in Österreich und stellt damit eine wertvolle Grundlage für zukünftige Forschungsarbeiten und praktische Anwendungen dar. Im folgenden Abschnitt werden mögliche Forschungsrichtungen für zukünftige Arbeiten aufgezeigt und ungelöste Herausforderungen dargestellt.

Die Ergebnisse dieser Arbeit eröffnen mehrere neue Forschungsrichtungen. Ein vielversprechender Ansatz wäre es, sich auf eine bestimmte Umgehungsmethode, wie zum Beispiel VPNs, zu konzentrieren und deren Wirksamkeit verschiedener VPN-Anbieter zu untersuchen. Dabei könnten verschiedene VPN-Anbieter und deren Leistungsfähigkeit in Bezug auf Geolokalisierung, DNS-Handling und Antwortzeiten verglichen werden.

Darüber hinaus könnte die Untersuchung auf andere DNS-Resolver ausgeweitet werden. Während in dieser Arbeit Cloudflare DNS, Google DNS und OpenNIC untersucht wurden, wäre es sinnvoll, weitere DNS-Resolver zu testen, um ein umfassenderes Bild ihrer Effizienz zu erhalten.

Eine weitere interessante Forschungsrichtung könnte die Entwicklung und Implementierung von verschlüsselten DNS-Technologien wie DNS über HTTPS (DoH) und DNS über TLS (DoT) sein. Diese Technologien könnten die Umgehung von DNS-Sperren erleichtern und gleichzeitig die Sicherheit und Privatsphäre der Nutzer*innen erhöhen.

Die in dieser Arbeit entwickelten Python-Skripte könnten zu einer eigenständigen Software weiterentwickelt werden. Diese Software könnte Forscher*innen weltweit zur Verfügung gestellt werden, um DNS-Sperren in verschiedenen lokalen und globalen Kontexten zu analysieren. Schließlich könnte die Zusammenarbeit mit internationalen Forschungseinrichtungen und zivilgesellschaftlichen Organisationen intensiviert werden, um globale Daten zu DNS-Sperren zu sammeln und auszuwerten. Durch diese Zusammenarbeit könnten umfassendere und vergleichbare Datensätze entstehen, die zu einem besseren Verständnis der globalen Internetzensur beitragen.

Ein weiteres Forschungsfeld könnte sich auf die Auswirkungen von Netzsperren auf das Nutzererlebnis konzentrieren. Insbesondere wäre es wichtig zu untersuchen, wie Netzsperren und ihre Umgehung die Geschwindigkeit, Stabilität und Sicherheit der Internetverbindung der Nutzer*innen beeinflussen.

Die Methode der direkten Verwendung von IP-Adressen hat sich als nicht geeignet erwiesen, insbesondere bei HTTPS-Anfragen. Zukünftige Untersuchungen könnten sich darauf konzentrieren, Lösungen für diese technischen Barrieren zu finden.

Zusammenfassend lässt sich sagen, dass diese Arbeit einen wichtigen Beitrag zur Erforschung der Umgehung von Netzsperren leistet und zahlreiche Möglichkeiten für zukünftige Untersuchungen eröffnet. Die Fortsetzung dieser Forschung kann sowohl das wissenschaftliche Verständnis als auch die praktische Anwendung der Umgehung von Netzsperren weiter verbessern.

Literaturverzeichnis

[AAH13] Aryan, Simurgh; Aryan, Homa; Halderman, J. Alex: Internet censorship in Iran: A first look. In: 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13). 2013.

[AC24a] ACOnet: ac.at-Domains, 2024, URL: https://www.aco.net/domain.html, besucht am: 25. 03. 2024.

[AC24b] ACOnet: Über ACOnet, 2024, URL: https://www.aco.net/organisation.html, besucht am: 18. 03. 2024.

[An08] Andreas Pfitzmann Stefan Kopsell, Thomas Kriegelstein: Sperrverfuegungen gegen Access-Provider–Technisches Gutachten. Dresden Technical University, 2008.

[An13] Anderson, Collin: Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran. CoRR abs/1306.4361, 2013, arXiv: 1306.4361, URL: http://arxiv.org/abs/1306.4361.

[AP15] Aceto, Giuseppe; Pescapé, Antonio: Internet censorship detection: A survey. Computer Networks 83, S. 381–421, 2015.

[BE22] BEREC: BEREC supports ISPs in implementing the EU sanctions to block RT and Sputnik, 2022, URL: https://www.berec.europa.eu/en/news-publications/news-and-newsletters/berec-supports-isps-in-implementing-the-eu-sanctions-to-block-rt-and-sputnik, besucht am: 03. 04. 2024.

[BFM05] Berners-Lee, Tim; Fielding, Roy T.; Masinter, Larry M: Uniform Resource Identifier (URI): Generic Syntax, RFC 3986, 2005, DOI: 10.17487/RFC3986, URL: https://www.rfc-editor.org/info/rfc3986.

[BK13] Betz, Joachim; Kübler, Hans-Dieter: Internet governance. Wer regiert wie das Internet, 2013.

[BM11] Bendrath, Ralf; Mueller, Milton: The end of the net as we know it? Deep packet inspection and internet governance. New Media & Society 13 (7), S. 1142–1160, 2011.

[BM24] BMDV: Internet Governance, 2024, URL: https://bmdv.bund.de/DE/Themen/Digitales/Internationale-Digitalpolitik/Internet-Governance/internet-governance.html, besucht am: 27. 03. 2024.

[Bo21] Bock, Kevin; Naval, Gabriel; Reese, Kyle; Levin, Dave: Even censors have a backup: Examining china's double https censorship middleboxes. In: Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet. S. 1–7, 2021.

[Br24] Breitsprecher, Victoria: Netzsperre oder DNS Sperre umgehen, 2024, URL: https://www.tarife.at/ratgeber/dns-sperre-netzsperre-umgehen, besucht am: 17. 04. 2024.

[Ch17] Christensson, Per: WHOIS, 2017, URL: https://techterms.com/definition/whois, besucht am: 05. 05. 2024.

[Cl24] Cloudflare: Was ist 1.1.1.1, 2024, URL: https://www.cloudflare.com/de-de/learning/dns/what-is-1.1.1.1/, besucht am: 05. 05. 2024.

[cl24a] cloudflare: Cloudflare, 2024, URL: https://www.cloudflare.com/, besucht am: 17. 04. 2024.

[cl24b] cloudflare: What is DNS?, 2024, URL: https://www.cloudflare.com/learning/dns/what-is-dns/, besucht am: 21. 04. 2024.

[Da19] Dahir, Abdi Latif: After a record of 16-month ban, this president has unblocked social media access. Quartz Africa, 2019.

[DH17] Deering, Dr. Steve E.; Hinden, Bob: Internet Protocol, Version 6 (IPv6) Specification, RFC 8200, 2017, DOI: 10.17487/RFC8200, URL: https://www.rfc-editor.org/info/rfc8200.

[DKK17] Dolunay, Ayhan; Kasap, Fevzi; Keçeci, Gökçe: Freedom of mass communication in the digital age in the case of the internet:"freedom house" and the USA example. Sustainability 9(10), S. 1739, 2017.

[Do04a] Dornseif, Maximilian: Government mandated blocking of foreign web content. arXiv preprint cs/0404005, 2004.

[Do04b] Dornseif, Maximillian: Government mandated blocking of foreign Web content. CoRR cs.CY/0404005, 2004, URL: http://arxiv.org/abs/cs/0404005.

[Do24] Domaintools: Whois Record for Kinox.to, 2024, URL: https://whois.domaintools.com/kinox.to, besucht am: 17. 04. 2024.

[DS20] De Gregorio, Giovanni; Stremlau, Nicole: Internet shutdowns and the limits of law. 2020.

[Es18] Esch, Johanna: Internationale Internet-Governance, de, 2018, URL: https://www.bpb.de/shop/zeitschriften/apuz/276561/internationale-internet-governance/, besucht am: 05. 04. 2024.

[Es21] Estl, Bertold: Das Internet in Österreich zwischen Freiheit, Regulierung und Kontrolle, Diss., Universität Wien, 2021, DOI: 10.13140/RG.2.2.19358.46406.

[EU15] EU: Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union. L 310/1, 2015.

[EU19] EU: Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 (Text von Bedeutung für den EWR.) de, Legislative Body: CONSIL, EP, 2019, URL: http://data.europa.eu/eli/reg/2019/1020/oj/deu, besucht am: 03. 04. 2024.

[EU22] EU: Verordnung (EU) 2022/350 des Rates vom 1. März 2022 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, de, Legislative Body: CONSIL, 2022, URL: http://data.europa.eu/eli/reg/2022/350/oj/deu, besucht am: 03. 04. 2024.

[Eu22] of European Regulators for Electronic Communications, Body: BEREC Guidelines on the Implementation of the Open Internet Regulation. BoR (22) 81, 2022.

[Fe21] Feldstein, Steven: The rise of digital repression: How technology is reshaping power, politics, and resistance. Oxford University Press, 2021.

[FNR22] Fielding, Roy T.; Nottingham, Mark; Reschke, Julian: HTTP Semantics, RFC 9110, 2022, DOI: 10.17487/RFC9110, URL: https://www.rfc-editor.org/info/rfc9110.

[Fo24] Foundation, The Apache Software: Apache-Dokumentation zu virtuellen Hosts, 2024, URL: https://httpd.apache.org/docs/2.4/de/vhosts/, besucht am: 16. 04. 2024.

[Ga24] Galan, Artem: Angriffe über HTTP und wie man sich davor schützt, 2024, URL: https://www.nine.ch/de/blog/angriffe-ueber-http-und-wie-man-sich-davor-schuetzt, besucht am: 30. 04. 2024.

[GD24] GDC: Global Digital Compact, 2024, URL: https://www.un.org/techenvoy/global-digital-compact, besucht am: 27. 03. 2024.

[Gm24] nic GmbH: Internetverwaltung, 2024, URL: https://www.nic.at/de/wissenswertes/internet-governance/uebersicht, besucht am: 27. 03. 2024.

[Go17] Gosain, Devashish; Agarwal, Anshika; Shekhawat, Sahil; Acharya, Hrishikesh B; Chakravarty, Sambuddho: Mending wall: On the implementation of censorship in India. In: International Conference on Security and Privacy in Communication Systems. Springer, S. 418–437, 2017.

[Go24] Google: Google Public DNS, 2024, URL: https://developers.google.com/speed/public-dns?hl=de, besucht am: 05. 05. 2024.

[Ho14] Horvath, Sabine: Aktueller Begriff - Internet Governance. Deutscher Bundestag - Nr. 11/14, 2014.

[Ho21] Hoang, Nguyen Phong; Niaki, Arian Akhavan; Dalek, Jakub; Knockel, Jeffrey; Lin, Pellaeon; Marczak, Bill; Crete-Nishihata, Masashi; Gill, Phillipa; Polychronakis, Michalis: How Great is the Great Firewall? Measuring China's {DNS} Censorship. In: 30th USENIX Security Symposium (USENIX Security 21). S. 3381–3398, 2021.

[Ho22] House, Freedom: Freedom On The Net 2022, 2022, URL: https://freedomhouse.org/explore-the-map?type=fotn&year=2023, besucht am: 13. 04. 2024.

[Ho23] House, Freedom: Freedom On The Net 2023, 2023, URL: https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf, besucht am: 03. 04. 2024.

[IC24] ICANN: ICANN, 2024, URL: https://www.icann.org/, besucht am: 27. 03. 2024.

[IE24] IETF: Introduction to the IETF, 2024, URL: https://www.ietf.org/about/introduction/, besucht am: 27. 03. 2024.

[Il24] Illsinger, Werner: Ein Land geht offline (25.3.1997), 2024, URL: https://digisociety.ngo/2017/03/25/ein-land-geht-offline-25-3-1997/, besucht am: 21. 04. 2024.

[IS17] ISPA: 20 Jahre Internet Service Providers Austria, 2017, URL: https://www.ispa.at/news-events/20-jahre-ispa/festschrift/, besucht am: 18. 03. 2024.

[IS23a] ISPA: ISPA News Dezember 2023, 2023.

[IS23b] ISPA: Netzsperren: Regulierungsbehörde bestätigt Unverhältnismäßigkeit und Rechtswidrigkeit, 2023, URL: https://www.ispa.at/presse/pressemitteilungen/pressemitteilungen-detailansicht/presseansicht/detail/2023-08-10/netzsperren-regulierungsbehoerde-bestaetigt-unverhaeltnismaessigkeit-und-rechtswidrigkeit/, besucht am: 09. 04. 2024.

[IS24a] ISOC: About the Internet Society, 2024, URL: https://www.internetsociety.org/about-internet-society/, besucht am: 27. 03. 2024.

[IS24b] ISPA: Frequently Asked Questions (FAQ) zu Netzsperren, 2024, URL: https://www.ispa.at/wissenspool/positionspapiere/ispa-position-faq-netzsperren/, besucht am: 05. 04. 2024.

[IS24c] ISPA: ISPA - Startseite, 2024, URL: https://www.ispa.at/startseite/, besucht am: 01. 04. 2024.

[IT24] ITU: About ITU, 2024, URL: https://www.itu.int/en/about/Pages/default.aspx, besucht am: 27. 03. 2024.

[Ji21] Jin, Lin; Hao, Shuai; Wang, Haining; Cotton, Chase: Understanding the Impact of Encrypted DNS on Internet Censorship. In: Proceedings of the Web Conference 2021. WWW '21: The Web Conference 2021. ACM, Ljubljana Slovenia, S. 484–495, 2021, ISBN: 978-1-4503-8312-7, DOI: 10.1145/3442381.3450084, URL: https://dl.acm.org/doi/10.1145/3442381.3450084, besucht am: 11. 02. 2024.

[Jo22] Johannes Guger, Michael Udulutsch: Collabroative Business. FernFH, 2022.

[Ka24a] Kamal, Adib: Die Internet Access-Technologien, 2024, URL: http://www.gpon.eu/breitband/access.html, besucht am: 25. 03. 2024.

[Ka24b] Karadeniz, Besim: netplanet.org - IP-Addressierung, 2024, URL: https://www.netplanet.org/adressierung/ip.shtml, besucht am: 01. 04. 2024.

[Kl05] Klensin, Dr. John C.: National and Local Characters for DNS Top Level Domain (TLD) Names, RFC 4185, 2005, DOI: 10.17487/RFC4185, URL: https://www.rfc-editor.org/info/rfc4185.

[Ko24] Kompendium, Elektronik: CPE - Customer Premises Equipment, 2024, URL: https://www.elektronik-kompendium.de/sites/kom/1204111.htm, besucht am: 16. 04. 2024.

[KR21] Knockel, Jeffrey; Ruan, Lotus: Measuring QQMail's automated email censorship in China. In: Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet. S. 8–15, 2021.

[Kw15] Kwon, Minseok: A tutorial on network latency and its measurements. Enabling real-time mobile cloud computing through emerging technologies, S. 272–293, 2015.

[La24] Lab, Citizen: citizenlab/testlists, 2024, URL: https://github.com/citizenlab/test-lists, besucht am: 27. 04. 2024.

[Lö23] Löbe, Dirk: HTTPS: Alles, was du über die verschlüsselte Verbindung wissen musst, 2023, URL: https://netzwerk-guides.de/https-grundlagen/, besucht am: 30. 04. 2024.

[Ma22] Magenta: Netzsperre: Was bedeutet "Diese Seite ist gesperrt"?, 2022, URL: https://blog.magenta.at/internet/sicherheit/netzsperre/, besucht am: 27. 04. 2024.

[Ma23] Master, Alexander: Modeling and Characterization of Internet Censorship Technologies, Diss., Purdue University, 2023, URL: https://hammer.purdue.edu/articles/thesis/Modeling_and_Characterization_of_Internet_Censorship_Technologies/23666784.

[Mc11] McNamee, Joe: The slide from self-regulation to corporate censorship. Brussels: EDRI, 2011.

[Me48] der Menschenrechte, Allgemeine Erklärung: Resolution der Generalversammlung der Vereinten Nationen. 1948.

[MG21] Master, Alexander; Garman, Christina: A Worldwide View of Nation-state Internet Censorship. 2021.

[Mi24] Minnich, Sebastian: VPN Test 2024, 2024, URL: https://www.heise.de/download/specials/Anonym-surfen-mit-VPN-Die-besten-VPN-Anbieter-im-Vergleich-3798036, besucht am: 16. 04. 2024.

[Mo20] Moon, Silver: How to Fetch Domain Whois Data with Sockets in Python, 2020, URL: https://www.binarytides.com/python-program-to-fetch-domain-whois-data-using-sockets/, besucht am: 03. 03. 2024.

[Mü20] Mühlenmeier, Lennart: Jordan does not block, it throttles internet access, 2020, URL: https://netzpolitik.org/2020/jordan-throttles-not-blocks-internet-access-shutdowns-keepiton/#netzpolitik-pw, besucht am: 13. 04. 2024.

[ne09] neogrid: OSI-Schichtenmodell — flickr.com, https://www.flickr.com/photos/neogrid/3518959740/, 2009, besucht am: 25. 03. 2024.

[ng24] nginx: nginx Server names, 2024, URL: https://nginx.org/en/docs/http/server_names.html, besucht am: 16. 04. 2024.

[on22] heise online: Leistungsschutzrecht: Netzsperre legt Teile des Internets in Österreich lahm, heise online, 2022, URL: https://www.heise.de/news/Leistungsschutzrecht-Netzsperre-legt-Teile-des-Internets-in-Oesterreich-lahm-7247466.html, besucht am: 13. 01. 2024.

[OO24] OONI: OONI Explorer, 2024, URL: https://explorer.ooni.org/de, besucht am: 28. 02. 2024.

[Op24] OpenNIC: OpenNIC Public Servers, 2024, URL: https://servers.opennic.org/edit.php?srv=ns1.at.dns.opennic.glue, besucht am: 05. 05. 2024.

[Or23] Ortiz Freuler, Juan: The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. Global Media and China 8 (1), S. 6–23, 2023.

[Ös22] Österreich, Republik: 55. Bundesgesetz: Änderung des Audiovisuelle Mediendienste-Gesetzes (NR: GP XXVII AB 1383 S. 149. BR: AB 10928 S. 939.) 2022, URL: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2022_I_55/BGBLA_2022_I_55.pdfsig, besucht am: 03. 04. 2024.

[Ös24a] Österreich, Republik: Urheberrechtsgesetz § 81, 2024, URL: https://ris.bka.gv.at/eli/bgbl/1936/111/P81/NOR40258199.

[Ös24b] Österreich, Republik: Verbraucherbehördenkooperationsgesetz, 2024, URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004891.

[Po81] Postel, Jon: Internet Protocol; RFC791, 1981.

[Pr22] Proschofsky, Andreas: Überzogene Netzsperre sorgt für Probleme im österreichischen Internet, DER STANDARD, 2022, URL: https://www.derstandard.at/story/2000138619757/ueberzogene-netzsperre-sorgt-fuer-probleme-im-oesterreichischen-internet, besucht am: 13. 01. 2024.

[Ps24] Psiphon: Psiphon, 2024, URL: https://psiphon.ca/, besucht am: 17. 03. 2024.

[Re22a] Reuter, Markus: Netzsperren klemmen in Österreich legale Webseiten ab, 2022, URL: https://netzpolitik.org/2022/overblocking-netzsperren-klemmen-in-oesterreich-legale-webseiten-ab/, besucht am: 17. 03. 2024.

[Re22b] Reuter, Markus: Overblocking: Netzsperren klemmen in Österreich legale Webseiten ab, netzpolitik.org, 2022, URL: https://netzpolitik.org/2022/overblocking-netzsperren-klemmen-in-oesterreich-legale-webseiten-ab/, besucht am: 13. 01. 2024.

[RF83a] RFC: Domain names: Concepts and facilities, RFC 882, 1983, DOI: 10.17487/RFC0882, URL: https://www.rfc-editor.org/info/rfc882.

[RF83b] RFC: Domain names: Implementation specification, RFC 883, 1983, DOI: 10.17487/RFC0883, URL: https://www.rfc-editor.org/info/rfc883.

[RF87a] RFC: Domain names - concepts and facilities, RFC 1034, 1987, DOI: 10.17487/RFC1034, URL: https://www.rfc-editor.org/info/rfc1034.

[RF87b] RFC: Domain names - implementation and specification, RFC 1035, 1987, DOI: 10.17487/RFC1035, URL: https://www.rfc-editor.org/info/rfc1035.

[RO19] Rastl, Peter; Oggolder, Christian: Die Geschichte des Internets als technische Infrastruktur. Österreichische Mediengeschichte: Band 2: Von Massenmedien zu sozialen Medien (1918 bis heute), S. 277–290, 2019.

[RT23a] RTR: Durchsetzung von EU-Sanktionen im Medienbereich: Verwaltungsstrafbestimmung § 64 Abs. 3a AMD-G (Update vom 11. Oktober 2023), 2023, URL: https://www.rtr.at/Paragraf_64_3a_AMD-G, besucht am: 03. 04. 2024.

[RT23b] RTR: Netzneutralitätsbericht 2023, 2023, URL: https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/netzneutralitaetsbericht/NNBericht2023.de.html, besucht am: 30. 03. 2024.

[RT23c] RTR: Regulierungsbehörde untersagt im Sinne der Netzneutralität überschießende IP-Sperren, 2023, URL: https://www.rtr.at/TKP/presse/pressemitteilungen/presseinformationen_2023/pinfo10082023tkp.de.html, besucht am: 06. 04. 2024.

[RT24a] RTR: Netzsperren, RTR, 2024, URL: https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_blockings.de.html, besucht am: 05. 03. 2024.

[RT24b] RTR: Netzsperren – Weitere Infos, RTR, 2024, URL: https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/blockings_legal.de.html, besucht am: 01. 04. 2024.

[RT24c] RTR: RTR - Netzneutralität, 2024, URL: https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/Netzneutralitaet.de.html, besucht am: 30. 03. 2024.

[RT24d] RTR: RTR Publikatonen, 2024, URL: https://www.rtr.at/TKP/aktuelles/publikationen/Uebersichtseite.de.html, besucht am: 25. 04. 2024.

[RT24e] RTR-GmbH: RTR Telekom Monitor 3. Quartal 2023 (14.03.2024), RTR, 2024, URL: https://exports.23degrees.io/fKAUjfPdh1kopsaL-report-rtr-telekom-monitor-q2-2023.pdf?v=1711017350083.

[RZP11] Roberts, Hal; Zuckerman, Ethan; Palfrey, John G: 2011 circumvention tool evaluation. Berkman Center Research Publication (2011-08), 2011.

[Sa22] Satariano, Adam: How Russia Took Over Ukraine's Internet in Occupied Territories, 2022, URL: https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-%20censorship.html, besucht am: 17. 03. 2024.

[Sc13] Schmidbauer, Franz: internet4jurists.at - Wie funktioniert das Internet, 2013, URL: http://www.internet4jurists.at/intern11.html, besucht am: 01. 04. 2024.

[Sc17] Schmitz, Peter: Was ist das Tor-Netzwerk?, 2017, URL: https://www.security-insider.de/was-ist-das-tor-netzwerk-a-586465/, besucht am: 16. 04. 2024.

[Sc23] Schreiber, Thomas: Technisches Gutachten für die Telekom-Control-Kommission im Verfahren R 33/22, Techn. Ber., Telekom-Control-Kommission, 2023.

[Sh21] Shepardson, David: Censorship circumvention tool helps 1.4 million Cubans get Internet access, 2021, URL: https://www.reuters.com/world/americas/censorship-circumvention-tool-helps-14-million-cubans-get-internet-access-2021-07-16/, besucht am: 17. 03. 2024.

[SNB16] Saputra, Ferry Astika; Nadhori, Isbat Uzzin; Barry, Balighani Fathul: Detecting and blocking onion router traffic using deep packet inspection. In: 2016 International Electronics Symposium (IES). S. 283–288, 2016, DOI: 10.1109/ELECSYM.2016.7861018.

[St21] Staudinger, Martin: Grundlagen wissenschaftlichen Schreibens. FernFH, 2021.

[st24] internet stiftung: nic.at: 1,5 Millionen .at-Domains, 2024, URL: https://www.internetstiftung.at/news/nic-at-15-millionen-at-domains/, besucht am: 18. 03. 2024.

[Th20] Thouvenin, Florent; Stiller, Burkhard; Hettich, Peter; Bocek, Thomas; Reutimann, Kento: Keine Netzsperren im Urheberrecht. Universität Zürich, RWI Bibliothek, 2020.

[TK23] TKK: R 23/22, 2023, URL: https://www.rtr.at/TKP/aktuelles/entscheidungen/entscheidungen/r23_22.de.html, besucht am: 09. 04. 2024.

[to17] tomas: Unesco-Bericht: Netzsperren nehmen zu und gefährden Meinungsfreiheit, netzpolitik.org, 2017, URL: https://netzpolitik.org/2017/unesco-bericht-netzsperren-nehmen-zu-und-gefaehrden-meinungsfreiheit/, besucht am: 13. 01. 2024.

[To22] Tor: Directly Connecting Users from Ukraine, 2022, URL: https://web.archive.org/web/20230105232136/https://web.ics.purdue.edu/~amaster/anticen%20sorship/Tor_usage_Ukraine_invasion.png, besucht am: 17. 03. 2024.

[To24] Tor: Tor Project, 2024, URL: https://www.torproject.org/, besucht am: 16. 04. 2024.

[Ts17] Tschohl, Christof: Studie zum Konzept einer zentralen „Clearingstelle“ zur inhaltlichen Beurteilung von Netzsperren im Zusammenhang mit Verletzungen des Urheberrechts. Research Institute AG & Co KG Zentrum für Digitale Menschenrechte, 2017.

[Un10] Univ.-Lektor Mag. Dr. Thomas Ledl: Quantitative Methoden der Wirtschaftsinformatik Teil 2: Analyse- und Strukturmodelle. 2010.

[Ve21] Ververis, Vasilis; Ermakova, Tatiana; Isaakidis, Marios; Basso, Simone; Fabian, Benjamin; Milan, Stefania: Understanding internet censorship in Europe: The case of Spain. In: Proceedings of the 13th ACM Web Science Conference 2021. S. 319–328, 2021.

[Ve23] Ververis, Vasilis; Lasota, Lucas; Ermakova, Tatiana; Fabian, Benjamin: Website blocking in the European Union: Network interference from the perspective of Open Internet. Policy & Internet, 2023.

[W324] W3: W3 - our mission, 2024, URL: https://www.w3.org/mission/, besucht am: 27. 03. 2024.

[Wa14] Wander, Matthäus; Boelmann, Christopher; Schwittmann, Lorenz; Weis, Torben: Measurement of globally visible dns injection. IEEE Access 2, S. 526–536, 2014.

[WBC21] Weinberg, Zachary; Barradas, Diogo; Christin, Nicolas: Chinese wall or Swiss cheese? Keyword filtering in the Great Firewall of China. In: Proceedings of the Web Conference 2021. S. 472–483, 2021.

[WK24] WKO: EU-weites Verbreitungsverbot für russische TV-Sender und Plattformen, 2024, URL: https://www.wko.at/oe/information-consulting/telekommunikations-rundfunkunternehmungen/eu-weites-verbreitungsverbot-fuer-rt-und-sputnik, besucht am: 27. 04. 2024.

[WS24] WSIS: Definition Internet Governance by WSIS, 2024, URL: https://www.nic.at/de/wissenswertes/internet-governance/uebersicht, besucht am: 27. 03. 2024.

[Xu21] Xue, Diwen; Ramesh, Reethika; S, Valdik S; Evdokimov, Leonid; Viktorov, Andrey; Jain, Arham; Wustrow, Eric; Basso, Simone; Ensafi, Roya: Throttling Twitter: an emerging censorship technique in Russia. In: Proceedings of the 21st ACM Internet Measurement Conference. IMC '21, Association for Computing Machinery, Virtual Event, S. 435–443, 2021, ISBN: 9781450391290, DOI: 10.1145/3487552.3487858, URL: https://doi.org/10.1145/3487552.3487858.

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Anhang

Der Anhang dieser Masterarbeit enthält alle erforderlichen und nicht im Literaturverzeichnis referenzierten Dokumente, die für die Nachvollziehbarkeit des empirischen Teils wichtig sind, einschließlich der Python-Skripte, welche für die Umgehungsmethoden entwickelt wurden.

Rohdaten, wie die Ausgaben der Python-Skripte und die Open-Data-Eingaben (im CSV-Format) sowie die R-Skripte für die statistische Analyse, befinden sich in den zusätzlich abgegebenen Dateien. Diese zusätzlichen Dateien sind in den Formaten CSV und Text verfügbar und gewährleisten die vollständige Transparenz und Reproduzierbarkeit der durchgeführten Untersuchungen. Im folgenden wird auf diese zusätzlich abgegebenen Dateien referenziert.

A. Anhang: Liste der Zielwebseiten

Die Liste der Zielwebseiten sind in den zusätzlich abgegebenen Dateien enthalten:

- A1: `Anhang_A_A1_netzsperrenOpenData.csv`
- Drei: `Anhang_A_Drei_netzsperrenOpenData.csv`
- Magenta: `Anhang_A_Magenta_netzsperrenOpenData.csv`

B. Anhang: Python-Skript Ermittlung gesperrter Domains

Listing B.1: Python-Skript Ermittlung gesperrter Domains.

```
#!/usr/bin/env python3
import socket, sys
import subprocess
import datetime
import csv

def perform_whois(server, query):  # Definition einer Funktion perform_whois für WHOIS-Abfrage
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  # Erstellung eines Socket-Objekts für TCP-Verbindung
    s.connect((server, 43))  # Verbindung zum WHOIS-Server auf Port 43 herstellen

    query_bytes = query.encode('utf-8')  # Kodierung der Abfrage in Bytes
    s.send(query_bytes + b'\r\n')  # Senden der Abfrage an den WHOIS-Server mit Zeilenumbruch

    msg = ''  # Initialisierung einer leeren Nachricht
    while len(msg) < 10000:  # Schleife für den Empfang von Datenchunks bis 10.000 Zeichen
        chunk = s.recv(1024)  # Empfangen eines Datenchunks mit maximal 1024 Bytes
        if not chunk:  # Überprüfen, ob keine Datenchunks mehr empfangen wurden
            break
        msg += chunk.decode('utf-8')  # Dekodierung und Hinzufügen des empfangenen Datenchunks zur Nachricht

```

```
21      return msg  # Rückgabe der vollständigen WHOIS-
    Antwortnachricht
22
23  def get_whois_data(domain):  # Definition einer Funktion
    get_whois_data für den Abruf von WHOIS-Daten
24      domain = domain.replace('http://', '')  # Entfernen des Prä
    fixes 'http://' aus der Domain
25      domain = domain.replace('www.', '')  # Entfernen des Präfixes
    'www.' aus der Domain
26
27      ext = domain[-3:]  # Extrahieren der TLD (Top-Level-Domain)
    der Domain
28      if ext == 'com' or ext == 'org' or ext == 'net':  # Überprüfen
    , ob die TLD eine der gängigen ist
29          whois = 'whois.internic.net'  # Verwendung des WHOIS-
    Servers 'whois.internic.net'
30          msg = perform_whois(whois, domain)  # Ausführen der WHOIS-
    Abfrage an den WHOIS-Server
31          lines = msg.splitlines()  # Aufteilen der WHOIS-Antwort in
     Zeilen
32          for line in lines:  # Durchlaufen jeder Zeile der WHOIS-
    Antwort
33              if ':' in line:  # Überprüfen, ob die Zeile ein
    Trennzeichen ':' enthält
34                  words = line.split(':')  # Aufteilen der Zeile in
    Wörter anhand des Trennzeichens
35                  if 'Whois' in words[0] and 'whois.' in words[1]:
    # Überprüfen, ob ein spezifischer WHOIS-Server gefunden wurde
36                      whois = words[1].strip()  # Aktualisierung des
     WHOIS-Servers
37                      break  # Beenden der Schleife nach Fund des
    WHOIS-Servers
38      else:  # Wenn die TLD nicht eine der gängigen ist
39          ext = domain.split('.')[-1]  # Extrahieren der TLD aus der
     Domain
40          whois = 'whois.iana.org'  # Verwendung des allgemeinen
    WHOIS-Servers 'whois.iana.org'
41          msg = perform_whois(whois, ext)  # Ausführen der WHOIS-
    Abfrage an den WHOIS-Server
42          lines = msg.splitlines()  # Aufteilen der WHOIS-Antwort in
     Zeilen
43          for line in lines:  # Durchlaufen jeder Zeile der WHOIS-
    Antwort
```

```
44              if ':' in line:  # Überprüfen, ob die Zeile ein
    Trennzeichen ':' enthält
45                  words = line.split(':')  # Aufteilen der Zeile in
    Wörter anhand des Trennzeichens
46                  if 'whois.' in words[1] and 'Whois Server (port
    43)' in words[0]:  # Überprüfen, ob ein spezifischer WHOIS-
    Server gefunden wurde
47                      whois = words[1].strip()  # Aktualisierung des
     WHOIS-Servers
48                      break  # Beenden der Schleife nach Fund des
    WHOIS-Servers
49
50      msg = perform_whois(whois, domain)  # Ausführen der WHOIS-
    Abfrage an den ermittelten WHOIS-Server für die Domain
51      return msg  # Rückgabe der WHOIS-Antwort
52
53  def get_whois_nameservers(whois_response):  # Definition einer
    Funktion get_nameservers zum Extrahieren von Nameservern aus
    der WHOIS-Antwort
54      nameservers = []  # Initialisierung einer leeren Liste für
    Nameserver
55      lines = whois_response.splitlines()  # Aufteilen der WHOIS-
    Antwort in Zeilen
56      for line in lines:  # Durchlaufen jeder Zeile der WHOIS-
    Antwort
57          if line.strip().startswith("nserver:"):  # Überprüfen, ob
    die Zeile mit "nserver:" beginnt
58              parts = line.split()  # Aufteilen der Zeile in Teile
59              if len(parts) >= 2:  # Überprüfen, ob genügend Teile
    vorhanden sind
60                  nameservers.append(parts[1])  # Hinzufügen des
    zweiten Teils (Nameserver) zur Liste
61      return nameservers  # Rückgabe der Liste der Nameserver
62
63
64  # Definiert eine Funktion zur Durchführung von NSLOOKUP-Anfragen
65  def perform_nslookup(nameserver, domain):
66      try:
67          # Startet einen NSLOOKUP-Prozess für den gegebenen Domain-
    Namen am spezifizierten Nameserver
68          result = subprocess.run(['nslookup', '-type=NS', domain,
    nameserver], capture_output=True, text=True)
69          # Gibt das Ergebnis der NSLOOKUP-Anfrage zurück
70          return result.stdout
```

```
71      except Exception as e:
72          # Gibt eine Fehlermeldung aus, wenn die NSLOOKUP-Anfrage
    fehlschlägt
73          print(f"Fehler bei der nslookup-Abfrage für {domain} an
    den Nameserver {nameserver}: {e}")
74          return ''
75
76  # Definiert eine Funktion zum Abrufen der autoritativen Nameserver
     aus der WHOIS-Antwort
77  def get_authoritative_nameservers(nameservers, domain):
78      authoritative_nameservers = set()  # Erstellt ein Set, um
    doppelte Nameserver zu vermeiden
79      for ns in nameservers:
80          # Ruft perform_nslookup auf, um die Nameserver für die
    gegebene Domain abzufragen
81          output = perform_nslookup(ns, domain)
82          if output:
83              lines = output.split('\n')  # Teilt die Ausgabe in
    Zeilen
84              for line in lines:
85                  if "nameserver =" in line.lower():
86                      parts = line.split('=')  # Teilt die Zeile bei
     "="
87                      if len(parts) >= 2:
88                          auth_ns = parts[1].strip()  # Entfernt ü
    berflüssige Leerzeichen
89                          authoritative_nameservers.add(auth_ns)  #
    Fügt den Nameserver zum Set hinzu
90      return list(authoritative_nameservers)  # Konvertiert das Set
    in eine Liste und gibt es zurück
91
92  # Definiert eine Funktion zum Abrufen der IP-Adressen der
    autoritativen Nameserver
93  def get_domain_ip(authoritative_nameservers, domain):
94      domain_ips = set()  # Verwendet ein Set, um Duplikate bei den
    IP-Adressen zu vermeiden
95      found_ips = False
96      for auth_ns in authoritative_nameservers:
97          # Führt den 'dig' Befehl aus, um IP-Adressen vom
    autoritativen Nameserver zu erfragen
98          output = subprocess.run(['dig', '+short', '@' + auth_ns,
    domain], capture_output=True, text=True)
99          if output.returncode == 0 and output.stdout.strip():
```

```
100             ip_addresses = output.stdout.strip().split('\n')  # Teilt die Ausgabe in IP-Adressen
101             domain_ips.update(ip_addresses)  # Fügt die gefundenen IP-Adressen zum Set hinzu
102             found_ips = True
103         elif output.returncode == 0 and not output.stdout.strip():
104             # Gibt eine Meldung aus, wenn keine IP-Adressen gefunden wurden
105             print(f"Keine IP-Adressen gefunden für {domain} bei Nameserver {auth_ns}")
106     if not found_ips:
107         domain_ips.add("Keine IP-Adressen gefunden")  # Fügt eine Meldung hinzu, falls keine IPs gefunden wurden
108     return list(domain_ips)  # Konvertiert das Set zurück in eine Liste und gibt sie zurück
109 
110 
111 # Definiert eine Funktion zum Abrufen der IP-Adressen der Domain über den System-DNS-Resolver
112 def get_ips_from_system_resolver(domain):
113     system_ips = set()  # Initialisiert ein Set, um doppelte IP-Adressen zu vermeiden
114     try:
115         # Führt den 'dig' Befehl aus, ohne einen spezifischen Nameserver anzugeben, nutzt also den Standard-DNS des Systems
116         output = subprocess.run(['dig', '+short', domain], capture_output=True, text=True)
117         if output.returncode == 0 and output.stdout.strip():
118             # Wenn der Befehl erfolgreich war und die Ausgabe nicht leer ist, werden die IP-Adressen extrahiert
119             ip_addresses = output.stdout.strip().split('\n')
120             system_ips.update(ip_addresses)  # Fügt die gefundenen IP-Adressen zum Set hinzu
121         elif output.returncode == 0 and not output.stdout.strip():
122             # Wenn keine IP-Adressen gefunden wurden, wird eine Nachricht ausgegeben
123             print(f"Keine IP-Adressen gefunden für {domain} mit dem System-DNS-Resolver")
124     except Exception as e:
125         # Bei einem Fehler während der Ausführung wird eine Fehlermeldung ausgegeben
126         print(f"Fehler beim Abrufen der IP-Adressen für {domain} über den System-DNS-Resolver: {e}")
127 
```

```
128     if not system_ips:
129         # Wenn keine IP-Adressen gefunden wurden, fügt eine
    Meldung dem Set hinzu
130         system_ips.add("Keine IP-Adressen gefunden")
131 
132     return list(system_ips)  # Konvertiert das Set in eine Liste
    und gibt sie zurück
133 
134 # Definiert eine Funktion zur Überprüfung einer DNS-Sperre
135 def check_dns_block(auth_ips, isp_ips):
136     # Überprüft, ob beide IP-Listen leer sind oder den Eintrag "
    Keine IP-Adressen gefunden" enthalten
137     if (not auth_ips or all(ip == "Keine IP-Adressen gefunden" for
     ip in auth_ips)) and \
138        (not isp_ips or all(ip == "Keine IP-Adressen gefunden" for
    ip in isp_ips)):
139         return "Keine IP-Adressen gefunden."
140     # Vergleicht die IP-Listen auf Überschneidungen
141     overlap = set(auth_ips) & set(isp_ips)
142     return "Nein" if overlap else "Ja"  # Gibt "Nein" zurück, wenn
     Überschneidungen existieren, sonst "Ja"
143 
144 # Definiert eine Funktion zum Lesen von Domainnamen aus einer CSV-
    Datei
145 def read_domains_from_csv(csv_file_path):
146     domains = []  # Initialisiert eine leere Liste für Domains
147     with open(csv_file_path, newline='', encoding='ISO-8859-1') as
     csvfile:
148         reader = csv.DictReader(csvfile, delimiter=';')
149         for row in reader:
150             domains.append(row['Website'])  # Fügt jede Domain aus
     der Spalte 'Website' zur Liste hinzu
151     return domains  # Gibt die Liste der Domains zurück
152 
153 # Definiert eine Funktion zum Schreiben der Ergebnisse in eine CSV
    -Datei
154 def write_to_csv(writer, timestamp, domain, whois_ns, auth_ns,
    auth_ns_ips, isp_ips, dns_block):
155     # Bereitet die IP-Strings für die Ausgabe vor
156     auth_ns_ips_string = ', '.join(auth_ns_ips)
157     isp_ips_string = ', '.join(isp_ips)
158     # Schreibt eine Zeile in die CSV-Datei
159     writer.writerow([timestamp, domain, ', '.join(whois_ns), ', '.
    join(auth_ns), auth_ns_ips_string, isp_ips_string, dns_block])
```

```
160
161 # Definiert die Hauptfunktion des Skripts
162 def main():
163     # Überprüft, ob ein Argument (Pfad zur Eingabe-CSV) übergeben
    wurde; falls nicht, wird eine Anleitung ausgegeben und das
    Skript beendet
164     if len(sys.argv) < 2:
165         print("Verwendung: python script.py <input_csv>")
166         sys.exit(1)
167
168     # Speichert den Pfad zur Eingabe-CSV-Datei, der als erstes
    Argument übergeben wurde
169     input_csv_path = sys.argv[1]
170     # Legt den Pfad für die Ausgabe-CSV-Datei fest
171     output_csv_path = "output.csv"
172     # Liest die Domains aus der Eingabe-CSV-Datei
173     domains = read_domains_from_csv(input_csv_path)
174
175     # Öffnet die Ausgabe-CSV-Datei zum Schreiben und sorgt dafür,
    dass sie nach dem Block automatisch geschlossen wird
176     with open(output_csv_path, 'w', newline='') as file:
177         # Erstellt einen CSV-Writer, der Semikolon als
    Trennzeichen verwendet
178         writer = csv.writer(file, delimiter=';')
179         # Schreibt die Kopfzeile der Ausgabe-CSV-Datei
180         writer.writerow(['Timestamp', 'Domain', 'Whois-Nameserver'
    , 'Authorative-Nameserver', 'Auth.-Nameserver IP-Adressen', '
    ISP-Nameserver IP-Adressen', 'DNS-Sperre'])
181
182         # Durchläuft jede Domain in der Liste
183         for domain_name in domains:
184             try:
185                 # Ruft WHOIS-Informationen für die Domain ab
186                 whois_response = get_whois_data(domain_name)
187                 # Extrahiert WHOIS-Nameserver aus der WHOIS-
    Antwort
188                 whois_nameservers = get_whois_nameservers(
    whois_response)
189                 # Ermittelt die autoritativen Nameserver aus den
    WHOIS-Nameservern
190                 authoritative_nameservers =
    get_authoritative_nameservers(whois_nameservers, domain_name)
191                 # Ruft die IP-Adressen der autoritativen
    Nameserver ab
```

```
192                 domain_ips_auth = get_domain_ip(
    authoritative_nameservers, domain_name)
193                 # Ruft die IP-Adressen über den System-DNS-
    Resolver ab
194                 domain_ips_system = get_ips_from_system_resolver(
    domain_name)
195                 # Überprüft, ob eine DNS-Sperre vorliegt,
    basierend auf den IP-Adressen der autoritativen und System-
    Nameserver
196                 dns_block_status = check_dns_block(domain_ips_auth
    , domain_ips_system)
197
198                 # Erstellt einen Zeitstempel für den aktuellen
    Zeitpunkt
199                 timestamp = datetime.datetime.now().strftime("%Y-%
    m-%d %H:%M:%S")
200                 # Schreibt die gesammelten Informationen in die
    Ausgabe-CSV-Datei
201                 write_to_csv(writer, timestamp, domain_name,
    whois_nameservers, authoritative_nameservers, domain_ips_auth,
    domain_ips_system, dns_block_status)
202
203                 # Gibt eine Bestätigung der erfolgreichen
    Verarbeitung der Domain aus
204                 print("Daten von "+domain_name+" erfolgreich in '
    output.csv' geschrieben.")
205                 print("DNS-Sperre:", dns_block_status)
206
207                 # Druckt zusätzliche Informationen zu den
    Nameservern und IP-Adressen
208                 print_info(domain_name, authoritative_nameservers,
     domain_ips_auth, domain_ips_system)
209             except Exception as e:
210                 # Fängt alle Ausnahmen während der Verarbeitung
    einer Domain ab und gibt eine Fehlermeldung aus
211                 print(f"Ein Fehler ist aufgetreten bei {
    domain_name}: {e}")
212
213
214
215 def print_info(domain_name, authoritative_nameservers,
    domain_ips_auth, domain_ips_system):
216     # Überprüft, ob autoritative Nameserver für die gegebene
    Domain gefunden wurden
```

```
217     if authoritative_nameservers:
218         # Gibt die gefundenen autoritativen Nameserver aus
219         print("Authoritative Nameservers:",
    authoritative_nameservers)
220     else:
221         # Gibt eine Nachricht aus, wenn keine autoritativen
    Nameserver gefunden wurden
222         print("Authoritative Nameservers konnten nicht gefunden
    werden.")
223
224     # Überprüft, ob IP-Adressen für die autoritativen Nameserver
    gefunden wurden
225     if domain_ips_auth:
226         # Gibt die gefundenen IP-Adressen der autoritativen
    Nameserver aus
227         print("Autharitive-Resolver IPs:", domain_ips_auth)
228     else:
229         # Gibt eine Nachricht aus, wenn keine IP-Adressen von den
    autoritativen Nameservern gefunden wurden
230         print("Keine IPs vom Autharitive-Resolver gefunden.")
231
232     # Überprüft, ob IP-Adressen vom System-DNS-Resolver gefunden
    wurden
233     if domain_ips_system:
234         # Gibt die gefundenen IP-Adressen des System-DNS-Resolvers
     aus
235         print("System DNS Resolver IPs:", domain_ips_system)
236     else:
237         # Gibt eine Nachricht aus, wenn keine IP-Adressen vom
    System-DNS-Resolver gefunden wurden
238         print("Keine IPs vom System DNS-Resolver gefunden.")
239
240 if __name__ == '__main__':
241     # Startet das Hauptprogramm
242     main()
```

C. Anhang: Aufrechte DNS-Sperren

Folgend die Anhänge der aufrechten DNS-Sperren der einzelnen ISPs, welche in eine .csv Datei für die weitere Verarbeitung mit R zusammengefasst wurden.

C.1. Anhang: Aufrechte DNS-Sperren. ISP: A1

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_C_output1_Schritt1_AufrechteSperren.csv` zu finden.

C.2. Anhang: Aufrechte DNS-Sperren. ISP: Drei

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_C_output1_Schritt1_AufrechteSperren.csv` zu finden.

C.3. Anhang: Aufrechte DNS-Sperren. ISP: Magenta

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_C_output1_Schritt1_AufrechteSperren.csv` zu finden.

D. Anhang: Python-Skript Umgehungsmethode 1: IP-Adresse verwenden

Listing D.1: Python-Skript für Umgehungsmethode 1: IP-Adresse verwenden.

```python
#!/usr/bin/env python3
import csv  # Zum Lesen und Schreiben von CSV-Dateien
import requests  # Zum Durchführen von HTTP-Anfragen
import argparse  # Zum Parsen von Argumenten in der Befehlszeile
import logging  # Zum Logging von Informationen
from datetime import datetime  # Zum Generieren von Zeitstempeln
from requests.exceptions import RequestException, SSLError  # Zum Fangen spezifischer Requests-Ausnahmen

# Konfiguriert das Logging-System, um Informationen in eine Datei namens 'access_log.txt' zu schreiben
logging.basicConfig(level=logging.INFO, filename='access_log.txt', filemode='a', format='%(asctime)s - %(levelname)s - %(message)s')

# Funktion zum Testen der Erreichbarkeit einer Domain über deren IP-Adresse
def test_access_via_ip(domain, ip_addresses):
    results_list = []  # Liste zum Speichern der Ergebnisse jeder getesteten IP
    for ip_address in ip_addresses.split(','):  # Zerlegt die IP-Adressen-String und iteriert über jede IP-Adresse
        ip_address = ip_address.strip()  # Entfernt überflüssige Leerzeichen
        results = {
            'Timestamp': datetime.now().strftime('%Y-%m-%d %H:%M:%S'),  # Setzt den aktuellen Zeitstempel
            'Domain': domain,  # Die Domain, die getestet wird
```

```
20              'IP': ip_address,  # Die IP-Adresse, die getestet wird
21              'Erreichbar über HTTP?': 'Nein',  # Initialisiert den
    HTTP-Erreichbarkeitsstatus als 'Nein'
22              'HTTP Statuscode': '',  # Leeres Feld für den HTTP-
    Statuscode
23              'Erreichbar über HTTPS?': 'Nein',  # Initialisiert den
     HTTPS-Erreichbarkeitsstatus als 'Nein'
24              'HTTPS Statuscode': ''  # Leeres Feld für den HTTPS-
    Statuscode
25          }
26          # Dictionary zur Abbildung von Protokollen zu ihren
    Ergebnisschlüsseln im results-Dictionary
27          protocols = {'http': ('Erreichbar über HTTP?', 'HTTP
    Statuscode'), 'https': ('Erreichbar über HTTPS?', 'HTTPS
    Statuscode')}
28          for protocol in protocols:  # Testet sowohl HTTP als auch
    HTTPS
29              url = f"{protocol}://{ip_address}"  # Bildet die URL
30              try:
31                  # Führt den GET-Request aus mit einem spezifischen
     Host-Header
32                  response = requests.get(url, headers={'Host':
    domain}, timeout=10, verify=True)
33                  status_code = response.status_code  # Speichert
    den Statuscode der Antwort
34                  results[protocols[protocol][1]] = f"{status_code}
    {response.reason}"  # Speichert Statuscode und Grund
35                  if status_code == 200:
36                      results[protocols[protocol][0]] = 'Ja'  #
    Setzt den Erreichbarkeitsstatus auf 'Ja', wenn 200 OK
37                  else:
38                      results[protocols[protocol][0]] = 'Nein'
39              except SSLError:
40                  results[protocols[protocol][1]] = "SSL/TLS Error"
     # Speichert einen SSL-Fehler
41                  logging.warning(f"SSL/TLS error encountered while
    accessing {url}")  # Loggt eine Warnung bei SSL-Fehlern
42              except RequestException as e:
43                  error_message = " ".join(str(e).split()[:2])  #
    Reduziert die Fehlermeldung auf die ersten zwei Wörter
44                  results[protocols[protocol][1]] = f"Error: {
    error_message}"  # Speichert die Fehlermeldung
45                  logging.error(f"Request failed for {url}: {
    error_message}")  # Loggt einen Fehler bei Request-Fehlern
```

```
46
47          results_list.append(results)  # Fügt die Ergebnisse der
    Liste hinzu
48      return results_list  # Gibt die Liste der Ergebnisse zurück
49
50  def process_csv(input_file, output_file='output-final.csv'):
51      # Öffnet die Eingabe-CSV-Datei zum Lesen und eine Ausgabe-CSV-
    Datei zum Schreiben.
52      with open(input_file, mode='r', newline='', encoding='utf-8')
    as infile, \
53           open(output_file, mode='w', newline='', encoding='utf-8')
     as outfile:
54          reader = csv.DictReader(infile, delimiter=';')  # Erstellt
     einen CSV-Reader, der Zeilen als Dictionaries liest.
55          fieldnames = ['Timestamp', 'Domain', 'IP', 'Erreichbar ü
    ber HTTP?', 'HTTP Statuscode', 'Erreichbar über HTTPS?', 'HTTPS
     Statuscode']  # Definiert die Spaltennamen für die Ausgabe-CSV
    .
56          writer = csv.DictWriter(outfile, fieldnames=fieldnames,
    delimiter=';')  # Erstellt einen CSV-Writer mit den
    spezifizierten Spaltennamen.
57          writer.writeheader()  # Schreibt die Kopfzeile in die
    Ausgabe-CSV-Datei.
58
59          # Iteriert über jede Zeile in der Eingabe-CSV-Datei.
60          for row in reader:
61              # Überprüft, ob die DNS-Sperre 'Ja' ist und ob IP-
    Adressen gefunden wurden.
62              if row['DNS-Sperre'] == 'Ja' and row['Auth.-Nameserver
     IP-Adressen'] != 'Keine IP-Adressen gefunden':
63                  access_results = test_access_via_ip(row['Domain'],
     row['Auth.-Nameserver IP-Adressen'])  # Ruft die Funktion auf,
     die die Erreichbarkeit über die IP testet.
64                  for result in access_results:  # Iteriert über die
     Ergebnisliste jeder getesteten IP.
65                      print(result)
66                      writer.writerow(result)  # Schreibt jedes
    Ergebnis als Zeile in die Ausgabe-CSV-Datei.
67
68  if __name__ == '__main__':
69      parser = argparse.ArgumentParser(description='Überprüfen Sie
    die Erreichbarkeit von Domains über IP-Adresse mithilfe einer
    angegebenen CSV-Datei.')  # Erstellt einen Argument-Parser.
```

```
70      parser.add_argument('input_file', type=str, help='Die Eingabe-
        CSV-Datei mit Domain-Informationen.')  # Fügt ein Argument für
        den Eingabe-Dateipfad hinzu.
71
72      args = parser.parse_args()  # Liest die Argumente aus der
        Kommandozeile.
73      process_csv(args.input_file)  # Ruft die Funktion auf, um die
        CSV-Datei zu verarbeiten.
```

E. Anhang: Ausgabe Python-Skript Umgehungsmethode 1

Folgend die Anhänge der Ausgaben der Python-Skripte für Umgehungsmethode 1 der einzelnen ISPs, welche in eine .csv Datei für die weitere Verarbeitung mit R zusammengefasst wurden.

E.1. Anhang: Ausgabe Umgehungsmethode 1: Verwendung der IP-Adresse. ISP: A1 Domains

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_E_output_Methode1_IP-Access.csv` zu finden.

E.2. Anhang: Ausgabe Umgehungsmethode 1: Verwendung der IP-Adresse. ISP: Drei Domains

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_E_output_Methode1_IP-Access.csv` zu finden.

E.3. Anhang: Ausgabe Umgehungsmethode 1: Verwendung der IP-Adresse. ISP: Magenta Domains

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_E_output_Methode1_IP-Access.csv` zu finden.

F. Anhang: Python-Skript Umgehungsmethode 2: DNS-Resolver ändern

Listing F.1: Python-Skript für Umgehungsmethode 2: DNS-Resolver ändern.

```python
#!/usr/bin/env python3
import subprocess  # Importiert das subprocess-Modul, um externe Befehle auszuführen.
import csv  # Importiert das csv-Modul für das Lesen und Schreiben von CSV-Dateien.
import argparse  # Importiert das argparse-Modul zur Verarbeitung von Kommandozeilenargumenten.
import time  # Importiert das time-Modul für Zeitfunktionen.
from datetime import datetime  # Importiert datetime für das Formatieren und Arbeiten mit Datums- und Zeitstempeln.

#Führt eine DNS-Abfrage für die angegebene Domain über den spezifizierten DNS-Server aus.
def query_dns(domain, dns_server):
    start_time = time.time()  # Startzeit der Messung
    try:
        # Führt den 'dig'-Befehl aus und fängt die Ausgabe auf.
        output = subprocess.run(['dig', '+short', '@' + dns_server, domain], capture_output=True, text=True)
        duration = time.time() - start_time  # Berechnet die Dauer der Anfrage
        # Überprüft, ob der Prozess erfolgreich war und gibt die Antwort als Liste zurück.
        if output.returncode == 0 and output.stdout.strip():
            return output.stdout.strip().split('\n'), duration
    except Exception as e:
        # Gibt eine Fehlermeldung aus, wenn ein Fehler auftritt.
```

```
20          print(f"Fehler bei DNS-Anfrage für {domain} über {
    dns_server}: {e}")
21      # Gibt eine leere Liste zurück, wenn keine Daten gefunden
    wurden oder ein Fehler auftrat.
22      return [], time.time() - start_time
23
24 #Vergleicht zwei Listen von IP-Adressen und gibt zurück, ob eine
    DNS-Sperre umgangen wurde.
25 def compare_dns_results(known_ips, new_ips):
26      known_set = set(known_ips)  # Konvertiert die bekannten IPs in
     ein Set
27      new_set = set(new_ips)  # Konvertiert die neuen IPs in ein Set
28      # Überprüft, ob es eine Überschneidung zwischen beiden Sets
    gibt und gibt 'Ja' oder 'Nein' zurück.
29      return "Ja" if known_set.intersection(new_set) else "Nein"
30
31 def read_known_ips_from_csv(csv_file):
32      """ Liest bekannte IPs aus einer CSV-Datei, wenn DNS-Sperre '
    Ja' ist. """
33      domain_ips = {}  # Ein Dictionary, das Domains auf ihre IP-
    Adressen abbildet
34      with open(csv_file, mode='r', encoding='utf-8') as file:
35          reader = csv.DictReader(file, delimiter=';')
36          # Durchläuft jede Zeile in der CSV-Datei
37          for row in reader:
38              # Überprüft, ob die DNS-Sperre 'Ja' ist und ob IP-
    Adressen vorhanden sind
39              if row['DNS-Sperre'].strip().lower() == 'ja' and row['
    Auth.-Nameserver IP-Adressen'] != 'Keine IP-Adressen gefunden':
40                  domain = row['Domain']
41                  ips = row['Auth.-Nameserver IP-Adressen'].split(',
     ')
42                  # Fügt die Domain und ihre IPs dem Dictionary
    hinzu
43                  domain_ips[domain] = ips
44      # Gibt das Dictionary zurück
45      return domain_ips
46
47 def main(csv_file):
48      domain_ips = read_known_ips_from_csv(csv_file)  # Liest
    bekannte IPs aus einer CSV-Datei basierend auf der DNS-Sperre.
49      output_csv = "output-dns.csv"  # Definiert den Namen der
    Ausgabe-CSV-Datei.
50
```

```
51      with open(output_csv, 'w', newline='') as file:  # Öffnet eine neue CSV-Datei zum Schreiben.
52          writer = csv.writer(file, delimiter=';')  # Erstellt einen CSV-Writer mit dem gewünschten Trennzeichen.
53          # Schreibt die Kopfzeile in die CSV-Datei mit den Spaltenüberschriften.
54          writer.writerow(['Timestamp', 'Domain', 'Authorative Nameserver IPs', 'Google IPs', 'Google Antwortzeit', 'Google DNS-Sperre umgangen?',
55                           'Cloudflare IPs', 'Cloudflare Antwortzeit', 'Cloudflare DNS-Sperre umgangen?', 'OpenNIC IPs', 'OpenNIC Antwortzeit', 'OpenNIC DNS-Sperre umgangen?'])
56
57          for domain, known_ips in domain_ips.items():  # Iteriert durch die Domains und ihre zugeordneten IPs.
58              timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')  # Generiert einen Zeitstempel für den aktuellen Moment.
59              # Führt DNS-Abfragen über unterschiedliche DNS-Resolver durch.
60              google_ips, google_time = query_dns(domain, '8.8.8.8')
61              cloudflare_ips, cloudflare_time = query_dns(domain, '1.1.1.1')
62              opennic_ips, opennic_time = query_dns(domain, '37.252.191.197')
63
64              # Vergleicht die bekannten IPs mit den von den DNS-Resolvern zurückgegebenen IPs.
65              google_dns_blocked = compare_dns_results(known_ips, google_ips)
66              cloudflare_dns_blocked = compare_dns_results(known_ips, cloudflare_ips)
67              opennic_dns_blocked = compare_dns_results(known_ips, opennic_ips)
68
69              # Schreibt die Ergebnisse für jede Domain in die CSV-Datei.
70              writer.writerow([timestamp, domain, ', '.join(known_ips), ', '.join(google_ips), f"{google_time:.3f}s", google_dns_blocked,
71                               ', '.join(cloudflare_ips), f"{cloudflare_time:.3f}s", cloudflare_dns_blocked,
72                               ', '.join(opennic_ips), f"{opennic_time:.3f}s", opennic_dns_blocked])
73
```

```
74 if __name__ == "__main__":
75     parser = argparse.ArgumentParser(description="DNS-Resolver
       Comparison Tool with CSV input")  # Erstellt ein Parser-Objekt
       für die Befehlszeilenargumente.
76     parser.add_argument("csv_file", type=str, help="Path to the
       CSV file containing domain and known IP addresses.")  #
       Definiert ein erforderliches Argument für den Pfad zur CSV-
       Datei.
77     args = parser.parse_args()  # Parst die Argumente.
78     main(args.csv_file)  # Ruft die Hauptfunktion mit dem Pfad zur
       CSV-Datei als Argument auf.
```

G. Anhang: Ausgabe Python-Skript Umgehungsmethode 2

Folgend die Anhänge der Ausgaben der Python-Skripte für Umgehungsmethode 2 der einzelnen ISPs, welche in eine .csv Datei für die weitere Verarbeitung mit R zusammengefasst wurden.

G.1. Anhang: Ausgabe Umgehungsmethode 2: DNS-Resolver verwenden. ISP: A1

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_G_output_Methode2_dns-resolver.csv` zu finden.

G.2. Anhang: Ausgabe Umgehungsmethode 2: DNS-Resolver verwenden. ISP: Drei

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_G_output_Methode2_dns-resolver.csv` zu finden.

G.3. Anhang: Ausgabe Umgehungsmethode 2: DNS-Resolver verwenden. ISP: Magenta

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_G_output_Methode2_dns-resolver.csv` zu finden.

H. Anhang: Python-Skript Umgehungsmethode 3: VPN

Listing H.1: Python-Skript für Umgehungsmethode 3: VPN.

```python
#!/usr/bin/env python3
import subprocess
import csv
import argparse
import time
from datetime import datetime

#Führt eine DNS-Abfrage für die angegebene Domain über den Netzwerk-DNS-Resolver (potenziell über eine VPN-Verbindung) aus.
def query_dns(domain):
    start_time = time.time()  # Startzeit der Messung
    try:
        # Führt den 'dig'-Befehl aus, ohne einen spezifischen DNS-Server zu spezifizieren. ACHTUNG: VPN Verbindung vor Ausführung herstellen um unter VPN-Verbindungen zu testen.
        output = subprocess.run(['dig', '+short', domain], capture_output=True, text=True)
        duration = time.time() - start_time  # Berechnet die Dauer der Anfrage
        # Überprüft, ob der Prozess erfolgreich war und gibt die Antwort als Liste zurück.
        if output.returncode == 0 and output.stdout.strip():
            return output.stdout.strip().split('\n'), duration
    except Exception as e:
        # Gibt eine Fehlermeldung aus, wenn ein Fehler auftritt.
        print(f"Fehler bei DNS-Anfrage für {domain} über den Netzwerk-DNS-Resolver: {e}")
    return [], time.time() - start_time

```

```
23 def compare_dns_results(known_ips, network_ips):
24     """ Vergleicht zwei Listen von IP-Adressen und gibt zurück, ob
       eine DNS-Sperre umgangen wurde. """
25     known_set = set(known_ips)
26     network_set = set(network_ips)
27     return "Ja" if known_set.intersection(network_set) else "Nein"
28
29 def read_known_ips_from_csv(csv_file):
30     """ Liest bekannte IPs aus einer CSV-Datei, wenn DNS-Sperre '
      Ja' ist. """
31     domain_ips = {}
32     with open(csv_file, mode='r', encoding='utf-8') as file:
33         reader = csv.DictReader(file, delimiter=';')
34         for row in reader:
35             if row['DNS-Sperre'].strip().lower() == 'ja' and row['
      Auth.-Nameserver IP-Adressen'] != 'Keine IP-Adressen gefunden':
36                 domain = row['Domain']
37                 ips = row['Auth.-Nameserver IP-Adressen'].split(',
       ')
38                 domain_ips[domain] = ips
39     return domain_ips
40
41 def main(csv_file):
42     domain_ips = read_known_ips_from_csv(csv_file)
43     output_csv = "output-vpn.csv"
44     with open(output_csv, 'w', newline='') as file:
45         writer = csv.writer(file, delimiter=';')
46         writer.writerow(['Timestamp', 'Domain', 'Aufgelöste IP-
      Adresse von Authorative Nameserver',
47                          'Aufgelöste IP-Adresse bei aktiver VPN-
      Verbindung', 'Antwortzeit VPN-Verbindung Resolver', 'DNS-Sperre
       umgangen mit VPN?'])
48         for domain, known_ips in domain_ips.items():
49             timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S
      ')
50             network_ips, network_time = query_dns(domain)
51             network_dns_blocked = compare_dns_results(known_ips,
      network_ips)
52             writer.writerow([timestamp, domain, ', '.join(
      known_ips),
53                              ', '.join(network_ips), f"{
      network_time:.3f}s", network_dns_blocked])
54
55 if __name__ == "__main__":
```

```
56     parser = argparse.ArgumentParser(description="DNS-Resolver
       Comparison Tool with CSV input")
57     parser.add_argument("csv_file", type=str, help="Path to the
       CSV file containing domain and known IP addresses.")
58     args = parser.parse_args()
59     main(args.csv_file)
```

I. Anhang: Ausgabe Python-Skript Umgehungsmethode 3

Folgend die Anhänge der Ausgaben der Python-Skripte für Umgehungsmethode 3 der einzelnen ISPs, welche in eine .csv Datei für die weitere Verarbeitung mit R zusammengefasst wurden.

I.1. Anhang: Ausgabe Umgehungsmethode 3: VPN. ISP: A1

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_I_output_Methode3_vpn.csv` zu finden.

I.2. Anhang: Ausgabe Umgehungsmethode 3: VPN. ISP: Drei

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_I_output_Methode3_vpn.csv` zu finden.

I.3. Anhang: Ausgabe Umgehungsmethode 3: VPN. ISP: Magenta

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_I_output_Methode3_vpn.csv` zu finden.

J. Anhang: Python-Skript Umgehungsmethode 4: Tor

Listing J.1: Python-Skript für Umgehungsmethode 4: Tor.

```python
#!/usr/bin/env python3
import subprocess
import csv
import argparse
import time
from datetime import datetime

#Verwendet tor-resolve, um eine DNS-Abfrage für die angegebene Domain über Tor auszuführen.
def tor_resolve(domain):
    start_time = time.time()  # Startzeit für die Zeiterfassung der Funktion
    try:
        # Führt tor-resolve Befehl aus
        output = subprocess.run(['tor-resolve', domain], capture_output=True, text=True)
        duration = time.time() - start_time  # Berechnet die Dauer der Anfrage
        # Überprüft, ob der Prozess erfolgreich war
        if output.returncode == 0:
            return [output.stdout.strip()], duration
        else:
            raise Exception(output.stderr.strip())
    except Exception as e:
        print(f"Fehler bei der DNS-Anfrage für {domain} über Tor: {e}")
        return [], time.time() - start_time

def read_known_ips_from_csv(csv_file):
```

```
25      """ Liest bekannte IPs aus einer CSV-Datei, wenn DNS-Sperre '
    Ja' ist. """
26      domain_ips = {}
27      with open(csv_file, mode='r', encoding='utf-8') as file:
28          reader = csv.DictReader(file, delimiter=';')
29          for row in reader:
30              if row['DNS-Sperre'].strip().lower() == 'ja' and row['
    Auth.-Nameserver IP-Adressen'] != 'Keine IP-Adressen gefunden':
31                  domain = row['Domain']
32                  ips = row['Auth.-Nameserver IP-Adressen'].split(',
     ')
33                  domain_ips[domain] = ips
34      return domain_ips
35
36  def compare_dns_results(known_ips, tor_ips):
37      known_set = set(known_ips)
38      tor_set = set(tor_ips)
39      if known_set.intersection(tor_set):
40          return "Ja"
41      elif any(ip.rsplit('.', 1)[0] == tor_ip.rsplit('.', 1)[0] for
    ip in known_ips for tor_ip in tor_ips):
42          return "Ja-Geolokalisiert"
43      else:
44          return "Nein"
45
46  def main(csv_file):
47      domain_ips = read_known_ips_from_csv(csv_file)  # Liest
    bekannte IPs aus CSV-Datei
48      output_csv = "output-tor.csv"
49      with open(output_csv, 'w', newline='') as file:
50          writer = csv.writer(file, delimiter=';')
51          writer.writerow(['Timestamp', 'Domain', 'Authorative
    Nameserver IPs',
52                           'Aufgelöste IP-Adresse bei aktiver Tor-
    Verbindung', 'Antwortzeit Tor-Verbindung Resolver', 'DNS-Sperre
     umgangen mit Tor?'])
53          for domain, known_ips in domain_ips.items():
54              timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S
    ')
55              tor_ips, tor_time = tor_resolve(domain)
56              tor_dns_blocked = compare_dns_results(known_ips,
    tor_ips)
57              writer.writerow([timestamp, domain, ', '.join(
    known_ips),
```

```
58                                ', '.join(tor_ips), f"{tor_time:.3f}s
    ", tor_dns_blocked])
59
60 if __name__ == "__main__":
61     parser = argparse.ArgumentParser(description="DNS-Resolver
    Comparison Tool using Tor")
62     parser.add_argument("csv_file", type=str, help="Path to the
    CSV file containing domain and known IP addresses.")
63     args = parser.parse_args()
64     main(args.csv_file)
```

K. Anhang: Ausgabe Python-Skript Umgehungsmethode 4

Folgend die Anhänge der Ausgaben der Python-Skripte für Umgehungsmethode 4 der einzelnen ISPs, welche in eine .csv Datei für die weitere Verarbeitung mit R zusammengefasst wurden.

K.1. Anhang: Ausgabe Umgehungsmethode 4: Tor. ISP: A1

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_K_output_Methode4_tor.csv` zu finden.

K.2. Anhang: Ausgabe Umgehungsmethode 4: Tor. ISP: Drei

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_K_output_Methode4_tor.csv` zu finden.

K.3. Anhang: Ausgabe Umgehungsmethode 4: Tor. ISP: Magenta

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_K_output_Methode4_tor.csv` zu finden.

L. Anhang: R-Skript Umgehungsmethode 1: IP-Adresse verwenden

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_L_R_Methode1_IP-Access.R` zu finden.

M. Anhang: R-Skript Umgehungsmethode 2: DNS-Resolver ändern

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_M_R_Methode2_dns-resolver.R` zu finden.

N. Anhang: R-Skript Umgehungsmethode 3: VPN

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_N_R_Methode3_VPN.R` zu finden.

O. Anhang: R-Skript Umgehungsmethode 4: Tor

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_O_R_Methode4_Tor.R` zu finden.

P. Anhang: R-Skript Hypothesen

Der Anhang ist in der zusätzlich abgegebenen Datei `Anhang_P_R_Hypothesen.R` zu finden.