Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Auslandsverbindungen und CDN-Kompetenz (ZwIBACK)

Zweite Internet Backbone-Studie – Projekt 415 Los 1

Zweite Internet Backbone-Studie:

Auslandskabelverbindungen und CDN-Kompetenz (ZwIBACK)

Projekt 415 Los 1

Infrastruktur, Ausfallszenarien und Konsolidierung

im Auftrag des BSI

STUDIENERGEBNISSE

Abschlussbericht

21. Februar 2022

Konsortialführer
Leitwert GmbH

Donaustraße 17
85049 Ingolstadt

Tel.: +49 841 93 76 84 93
E-Mail: contact@leitwert.net

Kontakt zum BSI
providersicherheit@bsi.bund.de

Dr. Johann Schlamp
schlamp@leitwert.net

Prof. Dr. Thomas C. Schmidt
schmidt@link-lab.net

Prof. Dr. Matthias Wählisch
mw@link-lab.net

Inhaltsverzeichnis

Kapitel 1
Einführung und Motivation

Das Internet befindet sich im Wandel. Seit der "Internet-Revolution" der späten 90er Jahre hat es sich zu einer (geschäfts-)kritischen Infrastruktur entwickelt, ohne die große Teile der heutigen (Wirtschafts-)prozesse zusammenbrächen. Andere kritische Infrastrukturen wie das Telefonsystem oder die elektrischen Energieversorgungsnetze können ohne ein funktionierendes Internet nicht mehr betrieben werden. Das zuverlässige Funktionieren des Internets ist zu einer gesamtgesellschaftlichen Grundvoraussetzung geworden, und der regionale Zugang zu einer leistungsfähigen Internet-Infrastruktur ist inzwischen strukturprägend. Weiträumige oder wiederholte Internet-Ausfälle müssen als Gefährdung für die Grundversorgung in unserem Land angesehen werden. Versorgungsdefizite – etwa in ländlichen, schwach besiedelten Regionen – wirken strukturell benachteiligend sowohl auf die wirtschaftliche Entwicklung als auch auf die Bildung der Bevölkerung.

Das Internet operiert global und mit ihm sind globale Unternehmen herangewachsen, die wirtschaftlich Spitzenpositionen einnehmen und gleichzeitig die Internet-gestützte Informationsgesellschaft nachdrücklich prägen. Google, Amazon, Facebook und Apple hatten 2018 gemeinsam einen Börsenwert, der größer als das Bruttosozialprodukt von Frankreich war. Die Google Suchmaschine hat heute einen weltweiten Marktanteil von 92,5% und das "Googlen" ist aus dem Alltag der meisten Internet-Nutzer nicht mehr wegzudenken. Dieses überproportionale Wachstum einiger Akteure hat insbesondere in der vergangenen Dekade einen Konsolidierungstrend manifestiert, welcher die ursprüngliche Diversifizierung im Internet nach dem Fall der Telekommunikationsmonopole umgedreht hat.

1.1 Entwicklung der Internet-Anwendungen

Der Erfinder des World Wide Web, Tim Berners Lee, erweckte zu Beginn des neuen Jahrtausends die Initiative Web 2.0 zum Leben und mit ihr die Entwicklung interaktiver Technologien, welche das Web für Inhalte der Endanwender öffnete. Statt bilateral zu kommunizieren und Inhalte zu konsumieren, begannen mehr und mehr Nutzer auf neu entstehenden Plattformen eigene Daten hochzuladen und neue Formen der Gruppenkommunikationsprozesse auszuprobieren: Ausgewählte soziale Netze gewannen sehr schnell an Beliebtheit und die Internet-Nutzer orientierten sich mit wachsender Intensität auf immer weniger Plattformen. Dieser Trend leitete eine Zentralisierung im World Wide Web ein und es wuchsen Systeme von neuartiger Dimension heran: Großsysteme, wie sie heute

nurmehr wenige, finanzstarke Unternehmen betreiben können.

In den letzten Jahren hat sich das Internet in seinem Gebrauch weiter geändert. Das oft exponentielle Wachstum der Internet-Anwendungen hat es in einen (volumens-)kritischen Marktplatz verwandelt, dessen direkte und vor allem indirekte, oft auf Werbung beruhende Geschäftschancen viele Bereiche der realen Wirtschaft merklich übertreffen. Die Internet-Infrastruktur bildet hierbei zunächst die zugrundeliegende Plattform, welche Diensteanbieter mit ihren Konsumenten verbindet. Diese verknüpfende Plattform wird nun teilweise zur indirekten Informationsgewinnung genutzt. Endgeräte (Browser, Sensoren) werden als Sonden mit Datenaggregatoren und –analysten verknüpft, deren Geschäftsmodell nicht in Kundenbeziehungen über das Internet, sondern in der Datenerhebung aus dem Internet bestehen.

Das Nutzungsverhalten der Endkunden hat sich dabei in den letzten Jahren ebenfalls signifikant verändert. Während einerseits Infotainment-Angebote insbesondere in den Bereichen Audio und Video "on Demand" (wie Spotify, Netflix, Amazon Prime u.a.) den Internet-Verkehr volumenseitig dominieren, was wiederum Infrastruktur-Anpassungen nach sich zieht, erleben auch klassische Standard-Netzdienste eine Transformation weg von langjährig etablierten, offenen Kommunikationsstandards hin zu proprietären, anbietergebundenen Anwendungen. Tabelle 1.1 illustriert diesen Trend durch eine exemplarische Gegenüberstellung populärer Dienste.

Internet-Dienst		
Offene Version	**Proprietäre Version**	**Anwendungskontext**
Email	Whatsapp	Nachrichtenaustausch auch in Gruppen
WWW	Facebook	Veröffentlichung persönlicher Informationen
Usenet	Reddit	Thematische Diskussionsforen
FTP	Dropbox	Austausch von Dateien
IRC	Slack	Online Chat

Tabelle 1.1: Gängige offene Internet-Dienste und deren Ersetzung durch geschlossene, proprietäre Anwendungs-Provider.

Parallel zu diesen Nutzungsveränderungen wachsen die Kommunikationsbedarfe exponentiell — getrieben sowohl durch die Datenvolumina der Dienste, als auch durch die explodierende Zahl der Endgeräte[1]. Die Bereitstellung sowie der Betrieb der benötigten Infrastruktur wird dementsprechend technisch wie wirtschaftlich immer anspruchsvoller. Zum Verständnis der Entwicklungen, welche die Infrastruktur treiben, ist die Aufteilung in zwei Bereiche hilfreich: (*i*) den Internet-Core bestehend aus einer Höchstleistungs-Netz- und Serverinfrastruktur sowie (*ii*) den Internet-Edge mit seinen kabel- oder funkbasierten Zugängen zu Endgeräten und Endkunden.

[1]Gartner'17 erwartet Milliarden neuer IoT-Knoten p.a., ABI [1] prognostiziert ein IoT Datenvolumen von ZettaBytes für die nahe Zukunft.

1.2 Technische Infrastrukturentwicklung

Die Entwicklung der Internet-Infrastruktur ist in den letzen Jahren geprägt von dem Spannungsverhältnis zwischen Edge und Core, d.h. zwischen den Akteuren, die Kontrolle über die jeweiligen Teile der Infrastruktur innehaben bzw. erlangen wollen. Die Entwicklung des Internet-Cores wurde lange Zeit getrieben vom Wachstum der Internet Exchange Points (IXPs) einerseits, die einen direkten, regionalen Datenaustausch zu Lasten der Tier-1 Transit Provider ermöglichen [2]. Andererseits trieben die Betreiber der Andwenungs-Großsysteme, die sogenannten "Over-the-Top" Service Provider (OTTs), den Ausbau eigener Infrastruktur und die Vernetzung ihrer Rechenzentren selbsttätig voran. Insbesondere die globalen Content Distribution Networks (CDNs) sowie große Software-Hersteller verfügen heute über globale Verteilinfrastrukturen und werden deshalb auch "Hyper-Giants" genannt. Beide Entwicklungstrends haben kürzere Datenübergänge und eine Abflachung der Routing-Hierarchien zur Folge, wogegen die Transit-Provider in den letzten Jahren eine Gegenbewegung zu etablieren versuchen.

Viele große ISPs versuchen, sich dem Druck der IXPs und OTTs entgegenzustemmen, indem sie ihre Stellung bei Endkunden als "Eyballs" stärken und damit ihre Marktmacht auf Basis ihrer Kundenzugänge festigen. Diese Endkunden sind meist nur durch einen ISP erreichbar. Die notwendige Kundenbindung wird dabei oft primär durch günstige Preise bei der Netzanbindung erreicht, welche die Kernnetzkosten kaum refinanzieren können.[2] Durch ein (quasi) Zugangsmonopol gestärkt, begegnen die Carrier den IXPs und Hyper-Giants mit Gegenmodellen zum offenen Peering: Einerseits bestehen viele ISPs gegenüber den OTTs auf direktem, privaten Peering, andererseits lassen sie sich im Rahmen von "Paid Peering" den exklusiven Kundenzugang bezahlen. Der Grundgedanke der großen ISPs ist dabei, den Content-Providern sowohl die technische Qualität, als auch die Skalierbarkeit im zugehörigen Datenvolumen für die Kundenzugänge in Rechnung zu stellen.

Alle relevanten Teilhaber an der Internet-Infrastruktur versuchen gegenwärtig, ihre Marktstellung zu festigen und auszuweiten:

- Große IXPs, indem sie ihre Präsenz und Infrastruktur teilweise transkontinental ausdehnen und so (*i*) regionale Provider als Kunden erschliessen sowie (*ii*) zum Tranistdienstleister werden;
- OTTs, indem sie auch ihre eigene Netz-Infrastruktur global ausbauen, eigene Kabel verlegen lassen (s. MAREA und Google Fiber) und darüber hinaus sich an Kabelprovidern wirtschaftlich beteiligen. Zudem zielen OTTs aufgrund ihrer Marktmacht verstärkt auf eine Reduktion bezahlter Transitverbindungen ab und nehmen kleinere Internet Service Provider durch die Forderung nach netzlokalen Caches in die Pflicht, was diese letztlich für das anfallende Transitvolumen finanziell aufkommen lässt;
- OTTs, indem sie Basisdienste konsolidieren und an ihre Infrastruktur binden bzw. die Einflussmöglichkeiten von Zugangsprovidern beschränken – z.B. durch neue Dienste wie DNS over HTTP (DoH), Certificate Transparency (CT) oder verschleierten Datentransport (z.B. mit Quic);

[2]Nach einem ruinösen Wettbewerb in der ersten Dekade des neuen Jahrtausends hat es bisher keinen deutlichen Trend zur Preissteigerung bei Internet-Zugängen gegeben.

- Netzwerkprovider, indem sie versuchen, ihren Einfluss auf die "letzten Meilen" auszuweiten und durch Zukäufe von Eyeballs, Gewinnung von Funkfrequenzen, etc. einen möglichst umfangreichen Kundenzugang exklusiv durch ihre regionale Infrastruktur zu erschliessen und damit sich selbst und die Infrastruktur im Markt abzusichern.

Eine wachsene Bedeutung ist hierbei den Funknetz-Infrastrukturen einzuräumen. Mehr und mehr Internet-Zugängssitzungen werden kabellos und ausserhalb von lokalen WLANs abgehalten — dies betrifft den allgegenwärtigen Kommunikationsverbund der Mobiltelephone genauso wie das aufkommende Internet der Dinge. Die sich gegenwärtig entwickelnde 5G Infrastruktur spielt dabei folgende multidimensionale Rolle in Leistung und Funktion.

Zunächst werden Breitband-Funkzugänge stark an Leistungsfähigkeit gewinnen. Gleichzeitig sollen aber Netzwerk-Teilbereiche für ultra-geringe Latenzen einerseits und sehr viele, kommunikationsschwache Endgeräte andererseits bereitgestellt werden. Private "vertical Networks", das Ausrollen anbieterspezifischer Protokolle und Dienste in der Fläche, wie es in der aufkommenden 5G Infrastruktur ebenfalls vorgesehen ist, öffnet in diesem Kontext die bisher im Internet unbekannte Gelegenheiten, eine mindestens regional kontrollierte, geschlossene Infrastruktur für abgeschottete Kommunikation zwischen Maschinen, d.h. Sensoren, Aktoren und Datenzentren, zu errichten. Der prominenteste Anwendungsfall hierfür ist die Automobilindustrie mit der benötigten Kommunikation zum autonomen Fahren.

Vertikale 5G-Teilnetze können absehbar zu einer Vergrößerung der Kundenbasis im Netzzugang führen, sobald große Industrieunternehmen wie z.B. die OEMs am Automarkt flächig Funknetzlösungen für ihre Flotten bei ausgewählten Providern einkaufen. Bereits durch ihre Netzkapazitäten wird die nahe Entwicklung der 5G Infrastruktur das Marktgefüge im Internet-Ökosystem beeinflussen und interessante Fragestellungen über die zukünftigen Entwicklung aufwerfen.

1.3 Resilienz der Internet-Infrastruktur

Die stetig steigende Marktbedeutung und die wachsend wertschöpfende Rolle der Internet-Infrastruktur erhöhen gleichzeitig Wirkungsmacht und Attraktivität von Angriffen auf ihre Verfügbarkeit: (Distributed) Denial-of-Service ((D)DoS) wird mit der zunehmenden Zahl und Bedeutung der Service-Nutzer lukrativer. Die Effektivität und technische Wirksamkeit von DDoS Angriffen verändert sich hierbei einerseits mit dem Wandel der Internet-Infrastruktur, andererseits mit der Robustheit und Missbräuchlichkeit weitverbreiteter Protokolle und Dienste und auch mit der Entwicklung des Ökosystems der Endgeräte, die die Infrastruktur nutzen.

Aus Infrastruktursicht, ohne Berücksichtigung von Zahl und Art der Endgeräte, wird folgende Dynamik erkennbar: Wachsen die Infrastrukturkapazitäten von Netzen, Servern und Diensten gleichförmig, bleibt der Status Quo aus Bedrohung und Bedrohungsabwehr in einem Gleichgewicht der Kräfte erhalten. Die gegenwärtigen Konsolidierungsentwicklungen weisen jedoch in eine andere Richtung. Während die Netzbandbreiten sowohl im Kernnetz als auch im Netzzugang sich stetig vermehren, diversifizieren sich Systeme

und Dienste im Internet zunehmend. Große Infrastrukturprovider entwickeln immer leistungsfähigere Datenzentren, welche durch zentralisierte, elastische Cloud-Infrastruktur den DDoS-Angriffen gewachsen bleiben und diese ggfs. auf der Datenebene herausfiltern können. Die heterogene Server-Infrastruktur in der Fläche dagegen, insbesondere aber auch der zunehmend intelligente Edge des Internets[3] können dieses Wachstum nicht leisten. Hieraus entstehen Abhängigkeiten von wenigen großen Akteuren, die alleine diesen Kapazitätswettbewerb aufnehmen können, ohne ihn freilich zuverlässig zu gewinnen (s. Cloudflare 2013). Abhilfe können hier intelligente Infrastrukturmaßnahmen wie ein feingranulares Blackholing etwa an IXPs oder großen Transit-Peerings bringen, aber auch die zunehmende Härtung der Internet-Protokolle und Dienste gegen Missbrauch.

Der Blick auf die Dynamik der Engeräte, hier insbesondere das heranwachsende IoT, gibt Anlaß zur Sorge. Eine schnell wachsende Vielzahl von ressourcen-schwachen – und oft schwach gesicherten – Endgeräten betreibt eine kleine Auswahl von Protokollen und Diensten der Maschinenkommunikation: MQTT-SN und CoAP verbreiten sich rasch als Service-Protokolle, die mittels UDP Transport per se für Reflektions- und Amplifikationsangriffe geeignet sind. Amplifikationen durch Milliarden von IoT Endgeräten können hierbei schnell zu einer massiven Gefahr für die Internet Kernnetzinfrastruktur heranwachsen. Diese Herausforderungen der Zukunft sind in der Studie zu betrachten.

1.4 Grundmodelle der Internet-Ökonomie im Wandel

Die vorgenannten Kräfte des Wandels führen auch dazu, dass das traditionelle Modell der Internet-Ökonomie [3] und ein darauf basierende Verständnis der Beziehungen zwischen den Internet-Akteuren an Bedeutung verlieren. “All IP”-Lösungen in Kombination mit Konsolidierungsbestrebungen bei den unterschiedlichen Interessensgruppen verändern Geschäftsgebaren. Eine kleine Gruppe sehr großer Akteure verfolgt so mit wachsendem Erfolg die Strategie, ihr Geschäftsfeld auf viele Schichten und grundlegende Infrastrukturkomponenten des Internets auszuweiten und damit die tradierte Rollenverteilung zu verlassen.

Durch diese und andere Veränderungen der Verhältnisse folgen Peering-Relationen und Inter-Provider-Übereinkünfte zunehmend anderen Regeln. Diese Verhaltensänderungen bewirken Veränderungen in der Kooperationsstruktur, Protokollanpassungen und topologische Verschiebungen. Funktions- und Resilienz-Veränderungen ergeben sich daraus genauso wie gesellschaftliche Implikationen in dem weitgespannten Bereich von Sicherheit und Katastrophenschutz bis zur Grundversorgung mit Informationen und ihrer gesellschaftlichen Rezeption und Reflektion.

[3]Eine zunehmende Anzahl von (mobilen) Anwendungen bedarf eines schnellen Zugriffs auf Daten und Berechnungen, weshalb die Zugangsinfrastruktur im Internet künftig Speicher- und Rechenkapazitäten bereitstellen soll.

1.5 Die Struktur dieser Studie

In der vorliegenden Studie wollen wir die Kernaspakte dieser aktuellen Internet-Entwicklungen thematisisieren und an Fallbeispielen hinterfragen. Unser Ziel ist es, die vielschichtige Bedeutung des Internets aus technischer, wirtschaftlicher und gesellschaftlicher Perspektive in vielen Details zu betrachten und hierdurch ein umfassendes Verständnis zu befördern.

Wir sammeln und analysieren zunächst signifikante Internet-Störungen der vergangenen Jahre in Kapitel 2 und klassifizieren diese sowohl nach ihren Ursachen als auch ihren Auswirkungen. Fünf der mehr als 100 betrachteten Vorfälle werden zudem mithilfe zusätzlicher Messungen und detaillierter Analysen gründlich forensisch durchleuchtet.

In Kapitel 3 diskutieren wir die Verwundbarkeit der gegenwärtigen Infrastruktur an fiktiven Ausfallszenarien unterschiedlicher Infrastrukturkomponenten. Wir analysieren detailliert (*i*) den Totalausfall eines wichtigen Überseekabels, (*ii*) den Ausfall aller Transitverbindungen durch ein Land, (*iii*) einen DDoS-Angriff auf einen populären DNS-Dienstleister und (*iv*) den Ausfall des sehr großen Internet-IXPs DE-CIX in Frankfurt. Hierbei fließen in unsere fiktiven Analysen die real beobachteten Fehlerfälle aus Kapitel 2 mit ein.

Dediziert werden internationale Kabelverbindungen in Kapitel 4 betrachtet und ihre Bedeutung im Transit untersucht. Ein besonderer Schwerpunkt liegt hierbei auf einer Bewertung einer verbesserten Widerstandsfähigkeit gegenüber Ausfällen. Diese Analysen wurden auf Basis der realen Vorfälle und zusätzlicher empirischer Messungen durchgeführt.

Hiernach konzentrieren wir uns in Kapitel 5 auf die aktuellen Veränderungen der Internet-Infrastruktur und beleuchten die technischen Aspekte. Der durch die Konsolidierung induzierte Wandel und seine Auswirkungen werden an Fallbeispielen diskutiert und auch durch erweiterte Messungen belegt.

Kapitel 6 diskutiert die wirtschaftlichen und gesellschaftlichen Entwicklungen sowohl der Internet-Infrastruktur, als auch der Dienste und Anwendungen und illustriert damit verbundenene Zusammenhänge. Unsere Beobachtungen ergeben ein facettenreiches, aber teilweise auch alarmierendes Lagebild, welches eine hohe Abhängigkeit des Internet-Ökosystems von wenigen Akteuren sichtbar werden lässt.

Schließlich geben wir in Kapitel 7 einen Ausblick auf künftig zu erwartende Entwicklungen in der kritischen Infrastruktur des gegenwärtigen Internets, indem wir thesenartig unsere aus den Analysen gewonnenen Erwartungen zuspitzen. Kapitel 8 fasst diese Studie zusammen.

Kapitel 2
Weitreichende Internet-Störungen

2.1 Vorfallskatalog

Um die Robustheit der Internet-Infrastruktur gegenüber Ausfällen und Angriffen zu beurteilen, ist es zweckmäßig, reale Internet-Vorfälle zu sammeln und in einem Vorfallskatalog zu bündeln. Durch eine strukturierte und methodische Aufarbeitung lassen sich hernach fundierte Aussagen über Ursachen, Auswirkungen und Gegenmaßnahmen sowie hinsichtlich aktueller Trends und Entwicklungen treffen. Basierend auf diesen Erkenntnissen können sowohl der Schutzbedarf insbesondere für die deutsche Internet-Infrastruktur abgeleitet als auch besonders relevante Fälle für eine detaillierte technische Analyse identifiziert werden.

2.1.1 Methodisches Vorgehen

Im Folgenden wird das methodische Vorgehen erläutert, mithilfe dessen der Vorfallskatalog erstellt und ausgewertet wurde. Dies umfasst sowohl eine allgemeine Beschreibung von Analyseansätzen mit der dazu nötigen Online- und Literaturrecherche, Kategorisierung und Bewertung von identifizierten Vorfällen, als auch die den Analysen zugrundeliegende Methodik. Anschließend werden die verwendeten Kategorien und Bewertungskriterien im Detail vorgestellt. Zuletzt wird die Vorgehensweise bei der Erarbeitung von fallübergreifenden Statistiken erläutert.

Allgemeiner Analyseansatz

Relevante Internet-Vorfälle wurden über Online- und Literaturrecherchen identifiziert. Um eine möglichst diverse Auswahl von Internet-Vorfällen zu garantieren, ist es hierbei wichtig, verschiedene Arten von Medien zu betrachten. Ein erster Überblick lässt sich mit Hilfe von Suchmaschinen sowie News- und Tech-Portalen verschaffen. Diese Kanäle sind besonders geeignet, um schwerwiegende Fälle mit weitreichenden Konsequenzen für Endnutzer zu identifizieren, da derartige Vorfälle in der Regel große mediale Aufmerksamkeit erzeugen. Durch die breite Zielgruppe der Nachrichtenportale beschränkt sich die Berichterstattung allerdings hauptsächlich auf den Ausfall selbst, geht jedoch nicht weiter auf technische Details und Abläufe ein. Demgegenüber stehen private Blogs sowie Firmen mit Fokus auf Sicherheitsfragen, die vermehrt Internet-Vorfälle im Nach-

hinein aufbereiten, um genaue Ursachen, getroffene Gegenmaßnahmen oder langfristige Konsequenzen zu beleuchten. Über diese Informationsquellen lassen sich auch Störungen finden, die keine globalen Auswirkungen nach sich zogen oder sehr schnell behoben werden konnten, aber dennoch aus technischer Sicht von Interesse sind. Nicht zuletzt eignen sich aber auch Mailinglisten, Ausfallbenachrichtigungen und Post-Mortem-Analysen von betroffenen Netzbetreibern und Dienstanbietern selbst. Mit deren Hilfe lassen sich Einblicke in exakte Zeitabläufe, sowie zu tieferliegenden Ursachen, Gegenmaßnahmen und Konsequenzen, gewinnen.

Im Anschluss werden die gesammelten Fälle kategorisiert. So lassen sich gleich geartete Vorfälle nach verschiedenen Gesichtspunkten wie der Schwere der Auswirkungen oder den dafür nötigen Vorbedingungen, d.h. der technischen Komplexität von Vorfällen, bewerten und allgemeine Aussagen bezüglich unterschiedlicher Bedrohungsszenarien treffen. Zur Bewertung werden dabei verschiedene Aspekte eines Vorfalls analysiert und nach deren Schwere klassifiziert, worüber anschließend eine statistische Auswertung durchgeführt wird. Um diese Auswertungen möglichst strukturiert und vergleichbar zu gestalten, werden bei allen Vorfällen stets die gleichen Bewertungsmetriken verwendet. Dadurch lassen sich sowohl einzelne Fälle untereinander priorisieren, als auch allgemeine Aussagen über verschiedene Fallkategorien treffen und miteinander vergleichen.

Basierend auf diesen Bewertungen werden im Anschluss besonders lehreiche Einzelfälle ausgewählt und in größerem Detail ausgearbeitet. Über weitere Recherchen werden unter anderem genaue Zeitpunkte, Beteiligte und Ursachen aufgezeigt. Die Auswahl dieser Einzelfälle wird jeweils begründet und dient als Grundlage für die in Abschnitt 2.2 folgenden qualitativen Detailanalysen. Schließlich werden die Ergebnisse der Bewertung zusammengefasst und daraus ein Überblick über die Gefahrenlage der heutigen Internet-Landschaft sowie über mögliche zukünftige Entwicklungen gegeben. Dies umfasst die statistische Aufarbeitung von Gefahrenquellen, Schäden und Mitigationstechniken, sowie daraus abgeleitet den Schutzbedarf der deutschen Internet-Infrastruktur.

Kategorisierung von Vorfällen

Die Kategorisierung des Vorfallskatalogs basiert auf den Gesichtspunkten Ursache, betroffene Dienstklasse und betroffene Parteien. Die Vorfallsursache wird als Hauptkategorie gewählt, da sich hieraus eine unmittelbare Vergleichbarkeit der Fälle innerhalb der jeweiligen Kategorie ergibt und sich somit allgemeine Aussagen über deren Gefährdungspotential ableiten lassen. Die Definition der einzelnen Ursachenkategorien resultiert dabei direkt aus den identifizierten Fällen und ist so gewählt, dass möglichst alle Ausfallszenarien abgedeckt werden und eine hinreichend große Anzahl von Fällen je Kategorie vertreten ist, um belastbare Aussagen treffen zu können. Folgende zehn Kategorien wurden nach diesem Vorgehen erarbeitet und für eine bessere Übersichtlichkeit in die drei Gruppen Ausfälle, Umleitungen und Angriffe eingeteilt.

Ausfälle Die erste Gruppe von Ursachen beschreibt allgemeine Ausfälle eines Systems, Netzwerkes oder Dienstes. Für diese Fälle kommen als Auslöser weder Änderungen oder Störungen im Internet-Backbone noch gezielte Angriffe oder Manipulationen in Frage. Entsprechende Ausfälle werden in folgende drei Kategorien eingeteilt.

- *Technischer Defekt* Hardware-Ausfälle ohne direkten äußeren Einfluss, aber auch Naturkatastrophen oder Versagen von für den Betrieb nötigen Versorgungssystemen.
- *Menschlicher Fehler* Ausfälle aller Art, die durch fahrlässige menschliche Einwirkung verursacht werden, jedoch nicht mutwillig sind, z.B. fehlerhafte Konfigurationen von Software oder irrtümliches Abschalten von Hardware.
- *Software-Fehler* Fehlerhaftes Verhalten von laufenden Systemen, die durch Software-Probleme im System selbst verursacht werden, z.B. abgelaufene Zertifikate oder unerwartetes Verhalten bei Teilausfällen der genutzten Infrastruktur.

Umleitungen Eine zweite Gruppe von Vorfallsursachen stellen Verkehrsumleitungen dar. Hierunter fallen überwiegend Vorfälle in Bezug auf eine Störung des Internet-Backbones, woraus sich weitreichende Routing-Änderungen und damit Beeinträchtigungen oder Ausfälle bei davon abhängigen Systemen, Netzwerken oder Diensten ergeben.

- *Kabelbeschädigung* Teilabtrennung von Netzwerken oder Überlastung von alternativen Routen, die durch Beschädigung oder Wegfall von wichtigen Kabelverbindungen verursacht werden, z.B. durch Bauarbeiten oder Sabotage.
- *Peering Dispute* Verminderte Dienstqualität oder Abbruch individueller Peering-Verbindungen zwischen großen Providern aufgrund von Streitigkeiten, z.B. durch einseitige Verletzung von Peering-Verträgen oder aufgrund Druck durch Dritte.
- *Route Leak* Verkehrsumleitung durch fehlerhafte, nicht mutwillige Annoncierung von Netzbereichen im Interdomain-Routing, z.B. aufgrund von fehlenden Filterregeln oder falsch konfigurierten Route-Optimizern.

Angriffe Zur letzten Ursachengruppe zählen mutwillig verursachte Störungen sowie gezielte Angriffe auf einzelne Systeme, Netzwerke oder Dienste. Neben expliziten technischen Ausfällen ist bspw. auch das Abtragen von sensiblen Daten Teil dieser Gruppe.

- *BGP-Hijacking* Mutwillige und gezielte Umleitung von Verkehren durch Manipulation von Routing-Nachrichten des Border Gateway Protokolls (BGP), bspw. zur Störung von Diensten oder zum Abhören von Kommunikationsverbindungen.
- *Denial-of-Service* Überlastung oder Totalausfall eines Systems, Netzwerkes oder Dienstes durch künstlich erzeugte Anfragen in großen Mengen, z.B. mit Hilfe von Bot-Netzen oder durch Ausnutzen von Implementierungsfehlern.
- *Hacking-Angriff* Gezielte Angriffe auf einzelne Systeme mit dem Ziel eines illegitimen Datenzugriffs oder einer Störung des laufenden Betriebs, z.B. durch Schwachstellen in Software-Komponenten oder mittels Social-Engineering.
- *Staatliche Aktion* Zumeist Ressourcen-intensive Operationen staatlicher Akteure gegen andere Länder und Dienste im In- und Ausland, bspw. zur Zensur oder Überwachung der Kommunikation von Bürgern.

Betroffene Dienstklassen Neben den beschriebenen Ursachen lassen sich Vorfälle auch nach der jeweils betroffenen Dienstklasse einteilen. Eine Dienstklasse bezeichnet dabei den Anwendungsbereich eines betroffenen Systems, Netzwerkes oder Dienstes. Folgende Dienstklassen werden zur Kategorisierung verwendet:

- *Backbone* Komponenten des Internet-Backbones, die für den Betrieb des Internets essentiell sind, z.B. Seekabel, aber auch Verbindungen zwischen großen Providern.
- *ISP* Netzwerke einzelner Internet Service Provider (ISP), deren Ausfall nur Konsequenzen für direkte Kunden nach sich zieht, bspw. Mobilfunknetze oder DSL.

- *Content* Alle Arten von Diensten mit explizitem Fokus auf Inhalte für Endanwender, darunter Video-Streaming, soziale Netzwerke oder andere populäre Webseiten.
- *Enterprise* Firmen-interne oder externe Dienste Dritter für den Geschäftskundenbereich, wie Verwaltungs-, Abrechnungs- oder Steuerungssysteme.
- *DNS* Dienste, die unmittelbar zur Aufrechterhaltung des Domain Name Systems (DNS) beitragen, bspw. Root-Server oder öffentliche DNS-Resolver.
- *Cloud* Technische Plattformen zur Bereitstellung von Diensten über alle Anwendungsbereiche hinweg, z.B. Server-Hosting oder Cloud Computing.
- *Anwender* Dienste mit direktem Bezug zu Endanwendern, bspw. Online-Banking und Crypto-Währungen, aber auch vernetzte Endgeräte.

Betroffene Parteien Ausfälle bei zentralen Internet-Diensten gehen in Abhängigkeit der jeweiligen Dienstklasse meist mit großflächigen Beeinträchtigungen einher. Unabhängig davon werden bei der Auswertung der Internet-Vorfälle auch die unmittelbar betroffenen Parteien mit angegeben. Beispiele hierfür sind die Betreiber von Internet-Diensten, physische Einrichtungen wie Rechenzentren oder Seekabel, oder auch geographische Regionen bei groß angelegten Angriffen oder Naturkatastrophen.

Bewertungs- und Analysekriterien

Die quantitative Analyse des Vorfallskatalogs wird anhand von sechs verschiedenen Bewertungs- und Analysekriterien durchgeführt, um relevante Aspekte der Vorfälle individuell zu beleuchten. Diese Kriterien werden auf jeden erfassten Fall angewandt und liefern jeweils ein Maß für die Schwere bzw. Qualität der betrachteten Aspekte. Für die Durchführung einer Risikobewertung wird zwischen hergangs- und datenspezifischen Kriterien unterschieden. Zu erstgenannten Kriterien zählen Dauer, Reichweite und Auswirkungen des jeweiligen Vorfalls. Aus diesen Hauptmerkmalen lässt sich das Schadenspotential jeder Vorfallskategorie durch eine statistische Auswertung der Einzelvorfälle ableiten, dementsprechend erfolgt für diese Kriterien im weiteren Verlauf auch eine farbliche Kodierung. Zur besseren Einordnung der Vorfälle wird zudem deren Komplexität untersucht und der – davon oft unabhängigen – Eintrittserwartung je Vorfallskategorie gegenübergestellt. Datenspezifische Kriterien beschreiben die verfügbare Informationslage zum jeweiligen Fall, darunter die generelle Datenlage im Hinblick auf tiefergehende Erkenntnisgewinne sowie die über Post-Mortem-Analysen kommunizierten Maßnahmen. In diesen Kriterien spiegeln sich demnach auch der Umfang der Berichterstattung und die Transparenz der Betroffenen wieder, und damit ebenso, in welchem Maß qualitative Aussagen über einzelne Vorfälle möglich sind. Da die Kriterien Komplexität, Post-Mortem und Datenlage wenig zu einer Risikobewertung beitragen können, werden sie farblich nicht weiter hervorgehoben. Im Folgenden wird die Bedeutung aller erarbeiteten Kriterien näher erläutert und der jeweilige Bewertungsmaßstab festgelegt.

Dauer Mit der Dauer eines Vorfalls wird stets der unmittelbare Zeitraum der Störung angegeben. Die Dauer möglicher Auswirkungen und Konsequenzen fließt nicht in dieses Bewertungskriterium mit ein und wird unabhängig davon betrachtet. Dadurch kann sowohl zwischen kurzen Störungen mit längerfristigen Beeinträchtigungen, wie bspw. Route Leaks, als auch lang anhaltenden Ausfällen mit kurzfristigen Mitigationsmöglichkeiten, bspw. Verkehrsumleitung bei Ausfällen von Seekabeln, differenziert werden.

1 *Vorfallsdauer im Minutenbereich*
2 *Vorfallsdauer von wenigen Stunden*
3 *Vorfallsdauer von Tagen oder Wochen*

Reichweite Die Anzahl der beeinträchtigten Systeme, Netzwerke oder Dienste wird durch das Kriterium Reichweite abgebildet. Dabei fließt auch die Größe der jeweils betroffenen Nutzerbasis mit in die Bewertung ein, um bspw. Ausfälle einzelner, aber stark frequentierter Dienste in geeigneter Weise abbilden zu können.

1 *Nur einzelne Dienste, Anbieter oder Netzwerke mit geringeren Nutzerzahlen*
2 *Populäre Plattform mit zahlreichen Nutzern oder unabhängigen Kunden*
3 *Vielzahl unabhängiger Dienste, Anbieter oder Netzwerke*

Auswirkungen Mit der Auswirkung eines Vorfalls werden alle kurz- und längerfristigen Folgen für Verursacher, Betroffene und weitere Beteiligte bewertet. Neben der Schwere der Auswirkungen fließen auch anhaltende Konsequenzen über den Zeitpunkt der Behebung oder Mitigation eines Vorfalls hinaus in die Beurteilung mit ein.

1 *Kurzfristig oder geringfügig verminderte Dienstqualität, zuverlässige Backup-Lösung*
2 *Signifikante Qualitätseinbußen, begrenzte Dienstausfälle, immaterieller Schaden*
3 *Anhaltender Totalausfall, hoher finanzieller Schaden, juristische Konsequenzen*

Komplexität Ein weiteres Kriterium zur Einordnung von Vorfällen wird unter dem Begriff Komplexität zusammengefasst. Hiermit werden die technischen oder physikalischen Eigenschaften eines Ausfalles oder Angriffes und die dazu nötigen Vorbedingungen berücksichtigt. Da die Komplexität eines Vorfalls nicht zwangsläufig auch Aussagen über dessen Gefährdungspotential zulässt, wird keine farbliche Risikobewertung vorgenommen.

1 *Spontanes Ereignis, breite Zielgruppen, große Angriffsoberflächen*
2 *Kaskadeneffekt, technisches Expertenwissen oder kriminelle Energie nötig*
3 *Mehrere Angriffsvektoren, hoher Ressourcenbedarf, Insiderwissen, Naturkatastrophen*

Post-Mortem Dieses Kriterium beschreibt die Datenqualität hinsichtlich der von den beteiligten Parteien als Reaktion auf den jeweiligen Vorfall ergriffenen Maßnahmen. Die Maßnahmen selbst werden dabei aufgrund der zumeist spärlichen Informationslage nicht bewertet, stattdessen wird für die Auswahl späterer Detailanalysen eine Bewertung der Nachvollziehbarkeit entsprechender Maßnahmen anhand von veröffentlichten Informationen abgegeben. Da die Informationslage nicht in die Risikobewertung einfließt, wird dieses Kriterium farblich nicht hervorgehoben.

1 *Keinerlei Informationen zu den getroffenen Maßnahmen verfügbar*
2 *Bekannter Einsatz eines Standardprodukts, öffentliche Stellungnahme vorhanden*
3 *Detailliertes Post-Mortem, lehrreiche Mitigationsansätze, orthogonale Maßnahmen*

Datenlage Zuletzt wird anhand der jeweiligen Charakteristik eines Vorfalls und den zur Verfügung stehenden Datenquellen beurteilt, inwieweit eine detaillierte Rekonstruktion des Vorfallsherganges im Rahmen einer Detailanalyse möglich erscheint. Dieses Kriterium fließt nicht in die farblich veranschaulichte Risikobewertung ein.

1 *Keine verwertbaren Daten vorhanden, betroffene Parteien unbekannt*
2 *Technische Informationen verfügbar, jedoch nicht unabhängig nachprüfbar*
3 *Betroffene Internet-Ressourcen bekannt, öffentliche oder eigene Daten vorhanden*

Fallübergreifende Risikobewertung

Basierend auf der vorangehend beschriebenen Kategorisierung und Bewertung des Vorfallskatalogs werden fallübergreifende Analysen durchgeführt. Diese basieren in erster Linie auf statistischen Erhebungen innerhalb einzelner Fallkategorien. Dadurch können Häufungen von Ursachen, Auswirkungen und betroffener Dienstklassen identifiziert werden. Weiterhin ist auch eine Korrelation von Auslösern, Folgen und betroffener Parteien möglich, woraus sich Aussagen über das Gefahrenpotential verschiedener Szenarien ergeben. Schließlich können über eine Analyse im zeitlichen Verlauf Trends und zukünftige Entwicklungen abgeleitet und die Eintrittserwartung vergleichbarer Fälle bestimmt werden. Unter Einbezug von aktuellen sowie zukünftig möglichen Schutz- und Gegenmaßnahmen wird der Handlungsbedarf für die deutsche Internet-Landschaft diskutiert.

Interaktive Darstellung

Alle im Zuge der Erstellung des Vorfallskatalogs erarbeiteten Informationen und Ergebnisse können neben der Aufarbeitung in diesem Dokument auch über die interaktive Web-Anwendung zum Projekt abgerufen werden:

`https://zwiback.leitwert.net`

Auf entsprechenden Detailseiten werden alle identifzierten Vorfälle sortier- und priorisierbar aufgelistet. Insbesondere können mit diesem Werkzeug auch Bewertungskriterien individuell gewichtet und Rangfolgen der Vorfälle generiert werden. Darüber hinaus sind auch interaktive Korrelationsanalysen über die Schwere und Qualität von Internet-Vorfällen sowie historische Vergleiche von Vorfallshäufigkeiten nach Kategorien möglich.

2.1.2 Identifizierte Internet-Vorfälle

Im Folgenden werden alle identifizierten Vorfälle kategorisiert und bewertet. Innerhalb jeder Kategorien werden zudem Ursachen, betroffene Parteien und Gegenmaßnahmen untersucht und deren Risiko im Vergleich zum Gesamtkatalog statistisch bewertet. Darüber hinaus werden zu jeder Kategorie besonders lehreiche Vorfälle vorgestellt.

Praktische Herausforderungen Bei der Recherche und Bewertung der Internet-Vorfälle traten verschiedentlich größere Herausforderungen auf. Die Qualität von Informationsquellen ist häufig unzureichend, da belastbare Aussagen und technische Details fehlen oder Mutmaßungen angestellt werden. Zudem beinhalten mehrere zu einem Vorfall recherchierte Quellen oft widersprüchliche Informationen, die sich vor allem bei älteren Fällen aufgrund verwaister Referenzen nicht immer auflösen lassen. Weiterhin bezieht sich die Berichterstattung häufig nur auf Ausfälle selbst, Konsequenzen und Mitigation werden im Nachgang dagegen selten beleuchtet. Aus der großen Anzahl betrachteter Vorfälle ergeben sich ebenfalls Herausforderungen in Bezug auf eine gleichmäßige Fallzahl je Kategorie und der Auswahl möglichst diverser Ursachen und Hergänge. Aufgrund des schwankenden Detailgrads bei den Vorfallsberichten ist auch eine konsistente Bewertung über alle Vorfälle hinweg schwierig. Zudem lässt sich nicht jeder Vorfall zweifelsfrei einer einzelnen Kategorie zuordnen, da oft mehrere Gründe, Auswirkungen und Betroffene vorliegen.

Automatisierbare Lösungsansätze Um die vorangehenden Herausforderungen weitestgehend zu bewältigen, wurde bei der Verarbeitung und Aufbereitung der Vorfälle auf teilautomatisierte Prozesse zurückgegriffen. So wurden die identifizierten Vorfälle nach manueller Kategorisierung und Bewertung in ein einheitliches Datenformat überführt und der Informationsgehalt von Quellen für später Analysen archiviert. Dadurch können die Vorfälle mit Hilfe eines Web-Clients sortiert und durchsucht sowie statistische Merkmale einzelner Kategorien visualisiert werden. Dieser Ansatz könnte in Zukunft zu einem nutzergestützten Online-Dienst zur Vorfallskatalogisierung ausgebaut werden.

2.1.2.1 Technischer Defekt

Der Vorfallskatalog umfasst 12 Vorfälle, die im weiteren Sinne einen technischen Defekt als Ursache haben und im Zeitraum zwischen 2015 und 2019 aufgetreten sind. Dabei zeigt sich, dass bei technischen Defekten mit besonders starken Auswirkungen zu rechnen ist und diese sich nur im Vorfeld durch geeignete Maßnahmen abwenden lassen. Empfohlene Detailanalysen sind ein großflächiger Stromausfall in Südamerika [I2] sowie ein Stromausfall in einem Frankfurter Rechenzentrum [I5].

Kategorie: **Technischer Defekt**

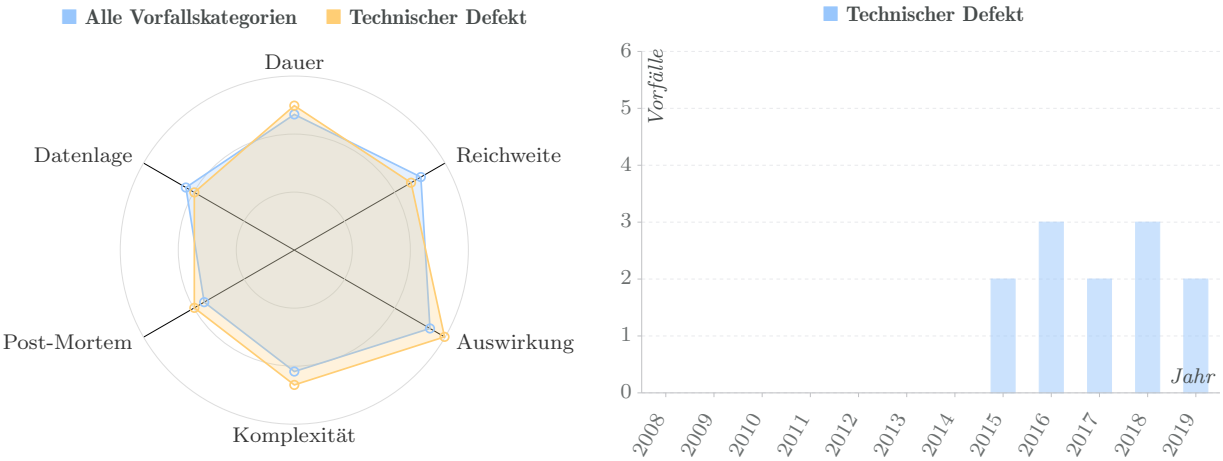
Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-11-13	ISP	Vodafone	Störung im Netz von Vodafone führt zu Internet-Ausfällen bei 13,000 Kunden [I1]	3	2	3	2	1	3
2019-06-16	Backbone	Südamerika	Großflächiger Stromausfall in Argentinien und Uruguay mit weiten Internet-Störungen [I2]	2	3	3	3	3	3
2018-11-24	ISP	Korea Telecom	Brand in Kabelschacht führt zu städteweitem Telekommunikationsausfall in Süd Korea [I3]	3	3	3	2	2	3
2018-09-04	Cloud	Microsoft	Blitzeinschlag in Rechenzentrum führt zu Ausfall von Azure-Diensten im Süden der USA [I4]	3	2	3	2	3	1
2018-04-09	Backbone	Interxion	Stromausfall in Frankfurter Rechenzentrum führt zu starken Störungen am DE-CIX [I5]	2	3	3	3	2	3
2017-09-29	Cloud	Microsoft	Azure-Dienste durch fälschlicherweise ausgelöstes Löschsystem in Nordeuropa offline [I6]	3	2	3	2	2	1
2017-05-27	Enterprise	British Airways	Defekte Notstromversorgung führt nach Wartungsfehler zu weltweiten Flugausfällen [I7]	3	2	3	3	3	1
2016-06-04	Cloud	Amazon	Stromausfall und defekte USV führen zu Ausfällen der AWS Services in Australien [I8]	2	2	3	3	2	2
2015-12-28	ISP	Vodafone UK	Ausfall eines Rechenzentrums nach Überschwemmung stört Internetanschlüsse [I9]	3	2	3	3	1	1
2016-01-28	Content	GitHub.com	Kurze Stromunterbrechung in Rechenzentrum führt zu mehrstündigem Ausfall [I10]	2	2	3	1	3	2
2016-01-14	Enterprise	JetBlue	Stromausfall in Verizon-Rechenzentrum führt zu landesweitem Ausfall von Flügen [I11]	2	2	3	2	1	1
2015-11-16	Backbone	Delta Telecom	Internet-Anbindung von Aserbaidschan nach Feuer auf Landkabel zu 94% eingeschränkt [I12]	2	3	3	2	1	3

Ursachen Als häufigste Ursache für technische Vorfälle stechen Störungen in der Stromversorgung heraus [I2, I5, I7, I8, I10, I11]. Diese umfassen dabei entweder einen kompletten Ausfall inklusive der Notstromversorgung oder auch eine Störung der unterbrechungsfreien Stromversorgung mit anschließenden Problemen beim Neustart der betroffenen Systeme. Weitere Ursachen sind Überschwemmung [I9], Blitzeinschlag [I4] und Brände [I3, I12], die durch besonders langanhaltende und starke Störungen auffallen. Ausfälle durch Defekte an Hardware [I1] und sonstiger Ausrüstung [I6] treten hingegen selten auf, da erstere durch redundante Systeme und Komponenten aufgefangen werden können und letztere vermutlich selten zu einem berichtenswerten Ausfall führen.

Betroffene Von technischen Defekten sind häufig nur einzelne Systeme oder Netzwerke betroffen, weshalb daraus überwiegend Ausfälle von spezifischen Diensten wie Cloud [I4, I6, I8], Enterprise [I7, I11] und Content [I10] resultieren. Da sich aber durchaus auch größere Ausfälle in Rechenzentren und damit in der Infrastruktur von Providern und Internet-Knoten verzeichnen lassen, sind auch ISPs [I1, I3, I9] sowie der Internet-Backbone selbst immer wieder von Ausfällen betroffen [I2, I5, I12].

Gegenmaßnahmen Unmittelbare Mitigationsmöglichkeiten während und nach technischen Defekten beschränken sich auf schnelle Schadensbeseitigung und Bereitstellung von alternativen Diensten. Meist führen einzelne Vorfälle aber zu besseren Präventivmaßnahmen in der Zukunft. So werden bspw. kürzere Wartungsintervalle und Testprozeduren an Notstromaggregaten und unterbrechungsfreier Stromversorgung [I5] sowie das Schließen von Lücken in der Branderkennung oder der Ausbau von Löschsystemen [I3] angeführt.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.1).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.1: (Technischer Defekt) **Statistische Auswertung**

- *Hohe Dauer*, da defekte Hardware und Infrastruktur in der Regel aufwendig überholt oder erneuert werden müssen, bis ein ungestörter Betrieb wieder möglich ist.
- *Mittlere Reichweite*, da technische Defekte in den meisten Fällen nur bei einzelnen Systemen oder Einrichtungen auftreten und demnach stets nur wenige Dienste oder beschränkte Kundenkreise der betroffenen Anbieter beinträchtigt werden.
- *Hohe Auswirkung*, da regelmäßig Totalausfälle der betroffenen Dienste zu verzeich-

nen sind. Zudem entstehen z.T. erhebliche finanzielle Schäden an den betroffenen Komponenten und durch aufgedeckte Mängel oft auch langfristige Folgekosten.
- *Komplexität* hoch, da Auslöser meist nicht vorhersehbar sind und Ursachen weder einem Muster noch einem steuerbaren Einfluss unterliegen. Des Weiteren müssen im Falle eines Ausfalls häufig mehrere Schutzmaßnamen gleichzeitig versagen.
- *Post-Mortem* überdurchschnittlich, da betroffene Kunden wie auch die Öffentlichkeit oft durch regelmäßige und detaillierte Berichterstattung informiert werden.
- *Datenlage* unterdurchschnittlich, da Hardware-Ausfälle selten mit Messdaten belegbar sind und oft einen schwer zu bestimmenden Kreis an Betroffenen aufweisen.

Risikobewertung Das Schadenspotential technischer Defekte ist im Allgemeinen als hoch zu bewerten. Mit längerer Beeinträchtigung von einzelnen Diensten oder Netzen ist zu rechnen, auch finanzielle Folgekosten sind generell zu erwarten.

Schadenspotential	**Hoch**
Eintrittserwartung	**Hoch**

Kategorie: **Technischer Defekt**

Die Eintrittserwartung technischer Defekte wird als hoch eingeschätzt, da sich Naturereignisse und Ausfälle weder vorhersagen noch zuverlässig verhindern lassen. Präventivmaßnahmen beschränken sich auf materiellen Schutz gegen äußere Einflüsse, regelmäßige Überprüfung sowie Vorhaltung von Redundanz, führen also zu dauerhaft höheren Kosten.

Fallbeispiel: Großflächiger Stromausfall in Südamerika [I2] Durch eine beschädigte Hochspannungsleitung kommt es 2019 zu flächendeckenden Stromausfällen in Südamerika. Die Datenlage ist durch weltweite Berichterstattung und landesweiten Beeinträchtigungen überdurchschnittlich, auch sind Hergang und Größenordnung des Vorfalls bemerkenswert. So führte ein einzelner isolierter Fehler letztlich zu Netzausfällen in mehreren Ländern. Des Weiteren lässt der Fall eine Analyse von beliebigen Beobachtungspunkten aus zu, wodurch weltweite Konsequenzen untersucht werden können.

Fallbeispiel: Stromausfall in einem Frankfurter Rechenzentrum [I5] In einem Frankfurter Rechenzentrum des Anbieters Interxion kommt es durch einen überhitzten Transformator und versagende Notstromversorgung zu einem langanhaltenden Stromausfall. Der Vorfall zeigt eindrucksvoll, wie ein Totalausfall trotz umfangreicher Präventivmaßnahmen entstehen kann und lässt sich aufgrund der detaillierten Datenlage und Ursachenforschung seitens des Anbieters sehr gut nachvollziehen. Der Fall ist insbesondere auch deshalb von Bedeutung, weil mit dem Internet Exchange Point DE-CIX und der Deutschen Telekom zwei integrale Bestandteile der deutschen Internet-Infrastruktur direkt vom Ausfall betroffen sind.

2.1.2.2 Menschlicher Fehler

Der Vorfallskatalog umfasst 11 Vorfälle, die durch versehentliches menschliches Fehlverhalten verursacht wurden und im Zeitraum zwischen 2014 und 2019 aufgetreten sind. Fehler dieser Art lassen sich nur schwer durch Präventivmaßnahmen vermeiden, da diese sehr individuell ausfallen und keinen vorhersehbaren Einflüssen unterliegen. Gleichzeitig sind die Auswirkungen oft sehr weitreichend, da bspw. Konfigurations- und Code-Fehler auch Backup-Systeme betreffen können. Empfohlene Detailanalysen sind eine Fehlkonfiguration der Cloudflare Firewall [I13] sowie eines Routers beim Tier1-ISP Telia [I19].

Kategorie: **Menschlicher Fehler**

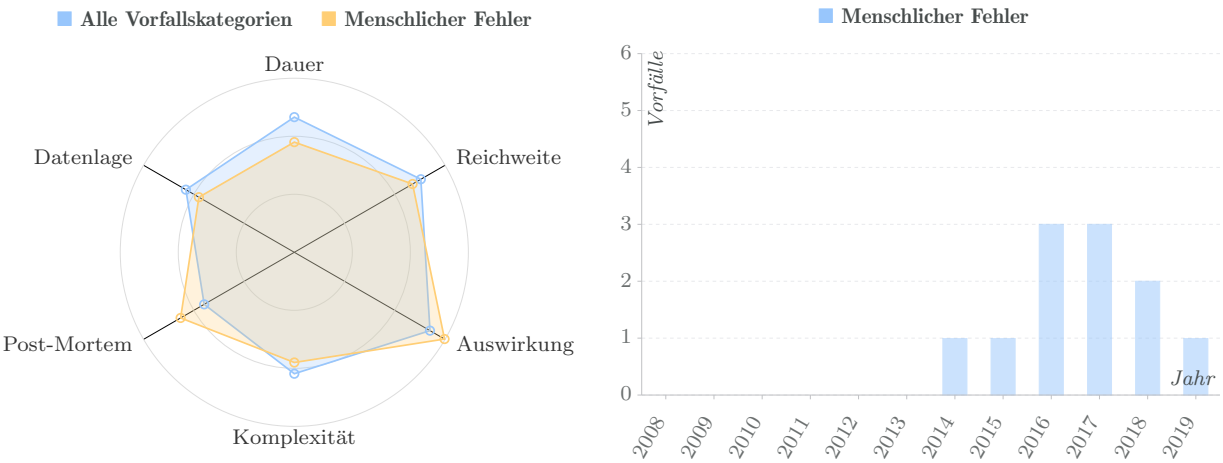
Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-07-02	Content	Cloudflare	Fehlerhafte Firewall-Regel auf Proxy führt zu weltweitem Ausfall aller CDN-Dienste [I13]	1	3	3	2	3	3
2018-12-09	Anwender	Quadriga CX	Crypto-Wallets im Wert von $190 Millionen nach Tod des Firmengründers unzugänglich [I14]	3	1	3	1	3	2
2018-05-31	DNS	Cloudflare	Fehlkonfigurierter DDoS-Schutz blockiert Zugang zu eigenem DNS-Server 1.1.1.1 [I15]	1	2	3	2	3	3
2017-08-29	Cloud	Google	Fehlerhafte VM-Netzwerkkonfiguration führt zu Ausfällen in Compute Engine Instanzen [I16]	3	2	3	2	3	3
2017-05-02	Backbone	Telia	Konfigurationsfehler führt zu Transatlantik-Ausfall und weltweiten Cloud-Störungen [I17]	1	3	3	2	1	2
2017-02-28	Cloud	Amazon	Tippfehler führt zu Backend-Neustart und S3/AWS-Ausfall an der US-Ostküste [I18]	2	2	3	2	3	1
2016-06-20	Backbone	Telia	Router-Fehlkonfiguration führt zu Routing von europäischem Verkehr über Hong Kong [I19]	2	3	3	2	1	1
2016-04-16	Cloud	123-reg	Fehlerhaftes Cleanup-Script löscht zahlreiche Kunden-Webseiten auf VPS-Instanzen [I20]	3	2	3	2	1	1
2016-02-09	ISP	Telstra	Wartungsfehler führt zu landesweitem Ausfall aller Kommunikationsdienste [I21]	2	3	3	3	1	1
2015-05-13	Backbone	AMS-IX	Fehlkommunikation bei Wartungsarbeiten führt zu Ausfall von 500 Peering-Sessions [I22]	1	3	3	2	3	3
2014-05-27	Cloud	Joyent	Versehentlicher Neustart aller VMs führt zu Überlast in Netboot-Infrastruktur [I23]	2	2	3	1	3	1

Ursachen Bei den Ausfallursachen dominieren Bedienfehler im Zuge von Wartungsarbeiten [I18, I20, I21, I22, I23] und Konfigurationsänderungen [I13, I15, I16, I17, I19] für einzelne Dienste und Systeme. In einem Fall führte der Verlust eines Crypto-Wallet-Passworts zu hohem finanziellen Schaden [I14] ohne technische Auswirkungen.

Betroffene Zu den betroffenen Dienstklassen zählen vorrangig Cloud [I16, I18, I20, I23], Content [I13] und DNS [I15], wobei hier neben der Störung des Betriebs auch ein Datenverlust als mögliche Auswirkung in Betracht gezogen werden muss. Neben Diensten mit Fokus auf Endanwender wirken sich menschliche Fehler häufig auch direkt auf den Internet-Backbone [I17, I19, I22] oder Internet Service Provider [I21] aus.

Gegenmaßnahmen Abgesehen von selteneren Datenverlusten [I14, I20] entstehen durch fehlgeschlagene Wartungsarbeiten oder Konfigurationsfehler keine dauerhaften Schäden. Gestörte Systeme müssen jedoch fallabhängig wieder in ihren Ursprungszustand zurück versetzt werden, was bei größeren Infrastrukturen zumeist einen funktionstüchtigen Backup-Mechanismus voraussetzt. Geeignete Gegenmaßnahmen lassen sich dabei schwer im Vorfeld implementieren, da bspw. Wartungsarbeiten oft tief im System und damit vorbei an Schutzmechanismen durchgeführt werden. Bei Konfigurationsänderungen hingegen ist Prävention mit Einschränkungen möglich, indem Änderungen erst in einem isolierten System getestet oder Aktualisierungen schrittweise ausgerollt werden [I13]. Auch ein Vier-Augen-Prinzip kann die Ausfallsicherheit potentiell erhöhen.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.2).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.2: (Menschlicher Fehler) **Statistische Auswertung**

- *Mittlere Dauer*, da die Ausfallgründe meist unmittelbar vom Verursacher als eigener Fehler erkannt und somit häufig auch schnell behoben werden können.
- *Mittlere Reichweite*, da meist nur isolierte Dienste oder Netzbereiche von Fehlern betroffen sind und diese nicht zu systemübergreifenden Ausfällen führen. Demgegenüber stehen Fehler bei Netz- und Infrastrukturbetreibern mit großen Kundenkreisen.
- *Hohe Auswirkung*, da betroffene Systeme oft vollständig ausfallen bzw. Netzbereiche überhaupt nicht oder nur mehr mit großen Einschränkungen erreichbar sind.
- *Komplexität* mittel, da generell mit menschlichem Versagen zu rechnen ist und sich keine allgemeingültigen Schutzmechanismen implementieren lassen. Gleichzeitig ist der Kreis potentieller Verursacher meist auf wenige Techniker begrenzt.
- *Post-Mortem* überdurchschnittlich, da viele Vorfälle aufgrund der tendentiell großen Auswirkungen durch eigene Analysen der Betroffenen detailliert aufbereitet werden.
- *Datenlage* unterdurchschnittlich, da Informationen über betroffene Kunden und Netzbereiche selten ohne Anonymisierung oder Abstraktion veröffentlicht werden.

Risikobewertung Das Schadenspotential menschlicher Fehler ist im Allgemeinen als mittel zu bewerten. Auch wenn die Auswirkungen auf betroffene Dienste in allen betrachteten Fällen hoch einzustufen war, so überwiegen dennoch eine zumeist mittlere Dauer und Reichweite. Einzelfallabhängig variiert die Bewertung der beiden Kriterien in dieser Vorfallskategorie allerdings besonders stark.

Schadenspotential	**Mittel**
Eintrittserwartung	**Mittel**

Kategorie: **Menschlicher Fehler**

Die Eintrittserwartung von menschlichen Fehler wird als mittel eingeschätzt, da sich ein zuverlässiger Schutz aufgrund der Bandbreite möglichen Versagens kaum bewerkstelligen lässt. Gleichzeitig ist insbesondere bei populären Diensten oder kritischen Infrastrukturen in der Regel nur ein eng begrenzter Personenkreis mit ausreichend Befugnissen für schwerwiegende Systemeingriffe ausgestattet.

Fallbeispiel: Fehlkonfiguration einer Cloudflare Firewall [I13] Eine fehlerhafte Firewall-Konfiguration führt zu massiven weltweiten Ausfällen im Cloudflare-CDN. Dieser Fall ist allein aufgrund der großflächigen Auswirkungen auf zahlreiche populäre Web-Dienste bemerkenswert, aber auch weil hier die enorme Marktmacht von Cloudflare in negativer Weise hervorsticht. Zudem bietet die sehr detaillierte Aufarbeitung des Vorfalls durch den Betreiber lehrreiche Einblicke, wie selbst umfangreiche Test- und Präventivmechanismen keinen umfassenden Schutz gegen jegliche Art von Fehlern bieten können, und wie sensibel komplexe Infrastrukturen auch auf kleine Fehler reagieren können.

Fallbeispiel: Fehlkonfiguration eines Telia Routers [I19] Der internationale Tier1-ISP Telia leitet nach Verbreitung einer fehlerhaften Router-Konfiguration innereuropäischen Verkehr über Hong Kong um. Trotz lückenhafter Berichterstattung zeigt dieser Vorfall eindringlich, wie stark der Internet-Backbone von menschlichem Fehlverhalten beeinträchtigt werden kann. Vor allem Telias nachlässiger Umgang im Hinblick auf Schutzmaßnahmen für kritische Infrastrukturen wurde öffentlich kritisiert.

2.1.2.3 Software-Fehler

Der Vorfallskatalog umfasst 15 Vorfälle, die durch Fehler in der bei Netz- und Dienstbetreibern eingesetzten Software verursacht wurden und im Zeitraum zwischen 2014 und 2019 aufgetreten sind. Bei der Auswertung zeigt sich, dass sich Vorfälle dieser Art nicht auf Endanwender und Dienste beschränken, sondern auch viele kritische Komponenten des Internet-Backbones direkt betroffen sind. Dies ist vor allem im Hinblick auf die unvorhersehbare Natur von Software-Ausfällen in immer komplexer werdenden Systeme problematisch. Empfohlene Detailanalysen sind der weltweite Dienstausfall einer Cloud-Lösung durch eine abgelaufene Software-Lizenz [I31] sowie der fälschliche Produktiveinsatz eines revokierten Schulungszertifikats [I33].

Kategorie: **Software-Fehler**

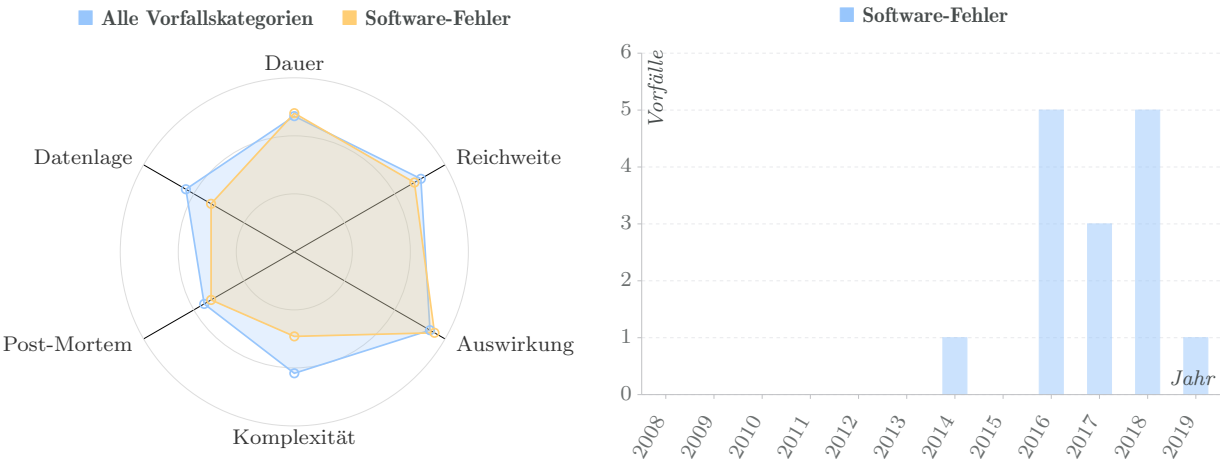
Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-05-13	ISP	China Telecom	Router-Störungen führen zu Verbindungsausfällen zwischen Asien und Nordamerika [I24]	2	2	2	3	1	2
2018-12-06	ISP	Ericsson UK	Abgelaufenes Software-Zertifikat führt zu landesweitem Ausfall des Mobilfunknetzes [I25]	3	3	3	1	2	2
2018-10-04	Anwender	Ecobee	Ausfall eines internen Web-Dienstes führt zu Unnutzbarkeit aller Smart-Home-Produkte [I26]	2	2	3	1	1	1
2018-03-18	Content	Fortnite	BGP Route Flapping bei italienischem Hoster führt zu regionalem Dienstausfall [I27]	1	1	3	1	2	3
2018-06-15	DNS	MYNIC	Abgelaufenes DNSSEC-Zertifikat führt zu Totalausfall der .my Top-Level-Domain [I28]	3	3	3	1	3	1
2018-03-13	Content	Google	Störung bei DoubleClick-Werbung führt zu eingeschränkter Nutzbarkeit von Webseiten [I29]	2	3	2	1	1	2
2017-07-25	Enterprise	Adobe Marketo	Fehler in automatisierter Domain-Erneuerung führt zu Domain-Parking und Dienstausfall [I30]	3	1	3	1	2	2
2017-06-29	Cloud	Rackspace	Abgelaufene Software-Lizenz einer Cloud-Lösung führt zu weltweitem Dienstausfall [I31]	2	2	3	1	1	1
2017-01-10	DNS	GoDaddy	Fehlerhafter Domain-Validierungsprozess führt zur Revokierung von 6,100 Zertifikaten [I32]	3	2	3	2	2	1
2016-10-13	Content	GlobalSign	Produktiveinsatz eines revokierten Schulungszertifikats führt zu HTTPS-Fehlern [I33]	3	3	3	2	3	1
2016-10-28	DNS	NIC.IO	Fehlerhafte Name Server liefern NXDOMAIN für alle Zonen der .io Top-Level-Domain [I34]	3	3	3	2	1	1
2016-08-15	Anwender	Tesla	Datennetzwerk der Fahrzeugflotte nach 3G-Ausfall bei AT&T landesweit offline [I35]	3	2	2	3	1	1
2016-07-03	ISP	Seacom	Seekabelverbindung für australischen ISP Syrex nach Router-Upgrade unterbrochen [I36]	2	3	3	1	1	1
2016-06-28	Backbone	AMS-IX	Ausfall von BGP Sessions beider Route Server durch nicht unterstützte BGP-Nachricht [I37]	2	3	3	1	3	3
2014-08-12	Backbone	Cisco	Router-Ausfälle nach Überschreiten des 512K-Limits in der globalen Routing-Tabelle [I38]	2	3	3	1	1	3

Ursachen Der häufigste Grund für Ausfälle durch Software-Fehler ist naturgemäß eine fehlerhafte Programmierung der jeweils eingesetzten Software [I24, I27, I32, I34, I36, I37, I38]. Beispiele hierfür sind inkorrekte Software-Updates sowie anormales Verhalten nach unerwarteten äußeren Einflüssen wie nicht unterstützte Nachrichten oder das Überschreiten von Ressourcengrenzen. Darüber hinaus führt oft auch ein Wegfall benötigter Web-Dienste zur eingeschränkten Nutzbarkeit von Anwendungen [I26, I29, I30, I35], bspw. bei Fahrzeugnavigation oder vernetzten IoT-Geräten. Dies umfasst bezeichnenderweise auch Komponenten, die zum eigentlichen Betrieb des jeweiligen Dienstes nicht vonnöten sind, wie Software-Störungen durch Fehler beim Einbinden von externen Werbeinhalten. Durch die immer stärkere Verbreitung von Ende-zu-Ende-Verschlüsselung und Software-as-a-Service kommt es auch entsprechend häufiger zu Ausfällen durch fehlerhafte oder abgelaufene Zertifikate [I25, I28, I33] und Software-Lizenzen [I31].

Betroffene Störungen durch Software-Fehler betreffen alle Bereiche Internet-basierter Dienste und umfassen demnach alle analysierten Dienstklassen. Dies schließt insbesondere auch kritische Infrastrukturen wie DNS [I28, I32, I34], Backbone [I37, I38] und ISPs [I24, I25, I36] mit ein. Neben den immer komplexer werdenden Diensten im Bereich Content [I27, I29, I33], Enterprise [I30] und Cloud [I31] sind auch Endanwender selbst von Software-Fehlern betroffen [I26, I35].

Gegenmaßnahmen Durch die äußerst vielfältigen Arten von Software-Fehler gibt es keine allgemeingültigen Mechanismen zur Prävention, insbesondere können Eigen- und Fremdentwicklungen durch umfassende Software-Tests kaum erschöpfend abgedeckt werden. In der Regel muss vorfallsabhängig mit individuellen Maßnahmen auf unerwartete Probleme reagiert werden. Dies schließt immer wieder auch eine kurzfristig nötige Zusammenarbeit mit Fremdherstellern [I31, I32] und damit versteckte Abhängigkeiten ein. Präventiv niedrig konfigurierte Caching-Zeiten können längere Störungen abmildern.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.3).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.3: (Software-Fehler) **Statistische Auswertung**

- *Mittlere Dauer*, da keine dauerhaften Schäden zu erwarten sind und Hotfix-Updates sich in der Regel schnell auf den betroffenen Systemen verteilen lassen. Zertifikatsfehler können aber auch längere Wartezeiten zur Neuausstellung nach sich ziehen.
- *Mittlere Reichweite*, da ein Großteil aller Fehler isoliert in einzelnen Diensten auftritt. Nur im Falle kritischer Infrastruktur erhöht sich die Reichweite entsprechend.
- *Hohe Auswirkung*, da Software-Probleme häufig zu einem Totalausfall führen und im Falle von Zertifikats- oder DNS-Fehlern aufgrund von Caching-Mechanismen in der Internet-Infrastruktur auch nach Behebung der Probleme andauern können.
- *Komplexität* niedrig, da stets mit mannigfaltigen Unzulänglichkeiten in jedweder eigenentwickelten oder zugekauften Software-Lösung gerechnet werden muss.
- *Post-Mortem* unterdurchschnittlich, da Fehler in der von Anbietern eingesetzten Software meist nur indirekt durch spätere Software-Patches bekannt werden.
- *Datenlage* unterdurchschnittlich, da die von Software-Fehlern betroffenen Nutzerkreise und Netzbereiche von außen meist nicht ersichtlich sind.

Risikobewertung Das Schadenspotential von Software-Fehlern ist im Allgemeinen als mittel zu bewerten. Vielfach lassen sich Störungen in angemessener Zeit beheben. Auch die Reichweite beschränkt sich zumeist nur auf einzelne Dienste, wodurch die generell hohen Auswirkungen einzelner Fehler nicht zu weitreichenden Konsequenzen führen. Software-Probleme in der Internet-Infrastruktur bergen allerdings größeres Schadenspotential.

Schadenspotential	**Mittel**
Eintrittserwartung	**Hoch**

Kategorie: **Software-Fehler**

Die Eintrittserwartung von Software-Fehlern wird als hoch eingeschätzt. Die Ursachen möglicher Probleme sind aufgrund der komplexen Natur von Software und der zunehmenden Abhängigkeit von Drittanbietern besonders vielfältig. Sowohl äußere Einflüsse als auch selbst verschuldete Fehler können jederzeit zu unerwarteten Störungen führen.

Fallbeispiel: Abgelaufene Software-Lizenz einer Cloud-Lösung [I31] Der vorliegende Ausfall eines Cloud-Balancers ist zwar unterdurchschnittlich dokumentiert und zog aufgrund der Einschränkung auf einen einzelnen Dienst keine größeren Auswirkungen nach sich. Dennoch ist der Fall von Interesse, da ein mehrfach redundantes System durch eine abgelaufene Software-Lizenz zum Erliegen gebracht wurde. Dies zeigt, dass neben der eingesetzten Software und Hardware auch Lizenzen und damit wirtschaftliche Belange einen Single-Point-of-Failure darstellen können. Zusätzlich wird deutlich, wie stark Abhängigkeiten zu Drittanbietern auch im Enterprise-Bereich ausgeprägt sein können, was die eigene Reaktionsgeschwindigkeit von Anbietern deutlich einschränken kann.

Fallbeispiel: Produktiveinsatz eines revokierten Schulungszertifikats [I33] Dieser Vorfall wurde durch den betroffenen Betreiber besonders ausführlich dokumentiert, insbesondere auch dessen aktuelle und zukünftige Gegenmaßnahmen. Dabei wurde gezeigt, wie ein zu Schulungszwecken durchgeführter Vorgang langanhaltende, weltweite Ausfälle nach sich ziehen kann. Wie auch im vorherigen Fall lag die Fehlerquelle in der Software eines Drittanbieters. Zusätzlich verdeutlicht der Hergang aber auch, wie lange negative Auswirkungen durch Einsatz von Caching-Mechanismen anhalten können, selbst wenn das zugrundeliegende Problem schnell identifiziert und behoben wird.

2.1.2.4 Kabelbeschädigung

Der Vorfallskatalog umfasst 9 Vorfälle, die durch Störungen an Land- und Seekabeln verursacht wurden und im Zeitraum zwischen 2011 und 2018 aufgetreten sind. Es zeigt sich, dass internationale Kabelverbindungen durch eine Vielzahl von Faktoren gefährdet sind und trotz ihrer zentralen Rolle für das Internet nicht vollständig vor diesen Gefahren geschützt werden können. Zudem wird auch die starke Kabelabhängigkeit von Entwicklungsländern und abgelegenen Regionen deutlich, die bei Ausfällen vom Internet getrennt werden können. Empfohlene Detailanalysen sind massive Internet-Ausfälle in Afrika durch Kabelbeschädigung [I40] und der Totalausfall der libanesischen Internet-Anbindung [I45].

Kategorie: **Kabelbeschädigung**

Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2018-06-29	ISP	Comcast	Kabelbrüche bei Level3 und Zayo führen zu landesweitem Telekommunikationsausfall [I39]	2	3	3	3	2	3
2018-03-30	Backbone	ACE	Kabelbeschädigung führt zu massiven Internet-Ausfällen in zehn afrikanischen Ländern [I40]	3	3	3	1	2	3
2016-05-17	Backbone	SMW-4	Paketverlust in Südamerika durch SEA-ME-WE4-Störung zwischen Europa und Asien [I41]	2	3	2	1	2	2
2016-02-05	ISP	PPC-1	Kabelbeschädigung zwischen Sydney und Guam führt zu Ausweich-Routen hoher Latenz [I42]	3	3	2	1	2	1
2016-01-21	Backbone	Seacom	Kabelbeschädigung bei Bauarbeiten in Ägypten führt zu Internet-Ausfällen in ganz Afrika [I43]	2	3	3	2	2	1
2013-03-27	Backbone	SMW-4	SEA-ME-WE4-Sabotage trennt Ägypten und Pakistan von westlichem Internet [I44]	3	3	3	3	2	2
2012-07-04	Backbone	I-ME-WE	Totalausfall der libanesischen Internet-Anbindung durch Kabelbeschädigung [I45]	3	3	3	1	2	2
2012-06-06	Backbone	SMW-4	Singapore Telecom in Südostasien durch SEA-ME-WE4-Beschädigung nicht erreichbar [I46]	3	3	2	1	1	2
2011-03-28	Backbone	Armenien	Ältere Frau beschädigt georgisches Landkabel und trennt Armenien vom Internet [I47]	2	3	3	1	1	1

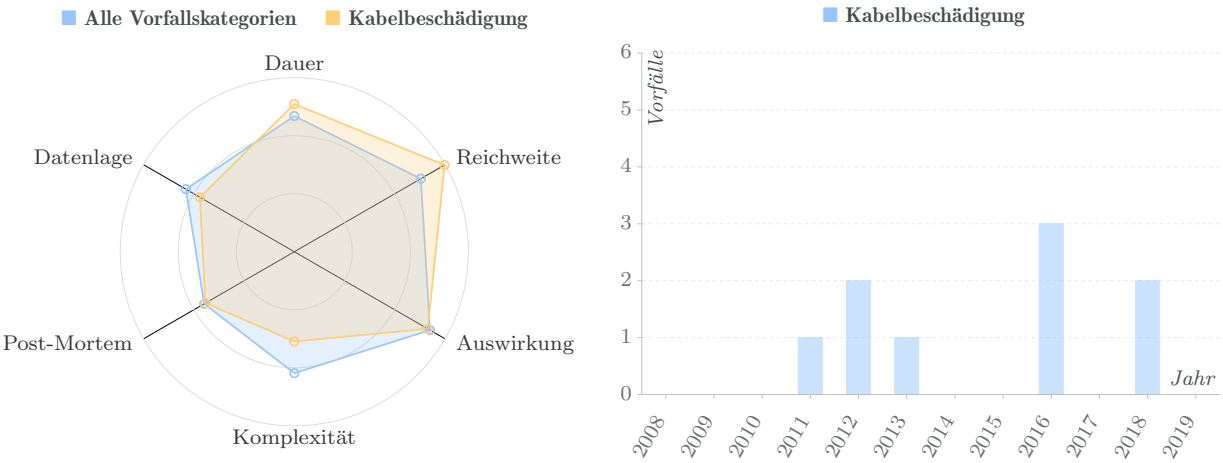
Ursachen Als häufigste Ursache für Ausfälle und Störungen treten physische Beschädigungen auf [I39, I40, I42, I43, I44, I46, I47]. Neben Umwelteinflüssen sind Kabelverbindungen auch durch alltägliche Vorgänge wie Bauarbeiten und Fischerei gefährdet, wobei genaue Ursachen oft nicht vom Betreiber kommuniziert werden. Bemerkenswert ist auch ein Fall aus Armenien, bei dem ein Landkabel von einer älteren Frau angegraben und das Land dadurch fast vollständig vom Internet getrennt wurde [I47]. Störungen im Nahen Osten resultierten aus geplanten Wartungsarbeiten [I45], die dem Betreiber und dessen Kunden jedoch nicht kommuniziert wurden. Ein weiterer Vorfall wurde vom Betreiber nicht näher erläutert [I41], obwohl damit mehrstündige weltweite Internet-Störungen verbunden waren. Bei einem Ausfall in Ägypten wurde ein Seekabel durch mehrere Personen beschädigt [I44], was laut Stellungnahme der ägyptischen Regierung auf Sabotage zurückzuführen ist. Dabei handelt es sich um die einzige Kabelbeschädigung im Vorfallskatalog, die von offizieller Seite als gezielter Angriff eingestuft wurde.

Betroffene Durch die hohen Investitions- und Betriebskosten werden Kabelverbindungen in der Regel für eine Vielzahl von Diensten verwendet. Dies zeigt sich auch dadurch, dass über alle Vorfälle hinweg nur die Dienstklassen Backbone [I40, I41, I43, I44, I45, I46, I47] und ISP [I39, I42] betroffen sind. Während Ausfälle zu einem großen Teil durch alternative Routen ausgeglichen werden können, sind vor allem entlegene Gebiete und Entwicklungsregionen stark von Kabelbeschädigungen betroffen und können in diesen Fällen meist nur eine rudimentäre Notversorgung via Satellitenverbindung herstellen.

Gegenmaßnahmen Eine Absicherung gegen Beschädigung oder Sabotage ist durch den schwer zugänglichen und langgestreckten Verlauf von See- und Landkabel in der Regel schwer zu realisieren. Als präventive Maßnahmen können aber seismisch aktive Gebiete vermieden oder die besonders gefährdeten Küstenabschnitte besser gesichert werden. Letz-

teres ist durch eine Überwachung von Fischerei und Bauarbeiten sowie durch redundant ausgebaute Anlandungsstellen möglich. Eine Störung im Libanon [I45] hätte durch bessere Kommunikation im Vorfeld weitgehend vermieden werden können. Ausreichend redundante Kapazitäten, die den Totalausfall eines Kabel auffangen können, werden aufgrund der hohen Investitions- und Betriebskosten nicht oder nur für wirtschaftlich lukrative Verbindungen umgesetzt. Für stark frequentierte Verbindungsstrecken, bspw. zwischen den USA und Europa, herrscht allerdings ein Wettbewerb unabhängiger Kabelbetreiber vor, auch drängen zunehmend Content-Anbieter in diesen Markt. Hochentwickelte Länder sind dadurch insgesamt weniger stark von einzelnen Kabelausfällen betroffen.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.4).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.4: (Kabelbeschädigung) **Statistische Auswertung**

- *Hohe Dauer*, da Beschädigungen an Seekabeln generell mehrwöchige Reparaturzeiten nach sich ziehen und bei großen Meerestiefen Spezialausrüstung benötigt wird. Auch für Störungen von Landkabeln ist aufgrund deren großer Länge von hunderten Kilometern und mehr grundsätzlich nicht mit kurzfristigen Reparaturen zu rechnen.
- *Hohe Reichweite*, da See- und auch Landkabel essentiell für die Kommunikation ganzer Länder und Kontinente sein können. Ausfälle betreffen häufig den gesamten Internet-Verkehr und sind nicht auf einzelne Dienste oder Netzbereiche beschränkt.
- *Hohe Auswirkung*, da zwar fast alle Regionen redundant über mehrere Kabelverbindungen angeschlossen sind, ein Ausfall aber zu großflächigen Kapazitätsengpässen und in weniger entwickelten Regionen auch zu Totalausfällen führen kann.
- *Komplexität* niedrig, da keine flächendeckende Überwachung von Kabelverbindungen umsetzbar ist. Es bestehen zahlreiche alltägliche Gefahrenquellen wie Bauarbeiten und Umwelteinflüsse, auch gezielte Sabotage ist jederzeit möglich.
- *Post-Mortem* durchschnittlich, da nur selten genaue Informationen über Maßnahmen veröffentlicht werden, in den Medien aber regelmäßig darüber berichtet wird.
- *Datenlage* unterdurchschnittlich, da durch redundante Anbindungen oft keine genauen Aussagen über die tatsächlich betroffenen Ressourcen möglich sind. Zudem lassen sich Schicht-2-Probleme generell nur indirekt datengestützt beobachten.

Risikobewertung Das Schadenspotential von Kabelbeschädigungen ist im Allgemeinen als hoch zu bewerten. Sowohl Dauer, Reichweite als auch Auswirkung von Vorfällen sind in dieser Kategorie allesamt hoch, Gegenbeispiele mit niedrigerer Einstufung sind kaum zu verzeichnen. Dies gilt allerdings nur in eingeschränktem Maße für Hochtechnologie-Standorte wie Deutschland, da hier die Auswirkung von Kabelausfällen aufgrund großer Redundanzen und starker Vernetzung abgemildert werden (siehe auch Abschnitt 4.1).

Schadenspotential	**Hoch**
Eintrittserwartung	**Hoch**

Kategorie: **Kabelbeschädigung**

Die Eintrittserwartung von Kabelbeschädigungen wird als hoch eingeschätzt, da sich alltägliche Pannen und seismische Naturereignisse weder vorhersagen noch verhindern lassen. Ein zuverlässiger materieller Schutz der anfälligen See- und Landkabel ist bestenfalls an exponierten Stellen möglich, in keinem Fall aber streckenübergreifend denkbar.

Fallbeispiel: Massive Internet-Ausfälle in Afrika [I40] Ein beschädigtes Seekabel führt in zehn afrikanischen Ländern zu Ausfällen. Da die Schäden durch einen Fischkutter verursacht wurden, zeigt dieser Vorfall eindringlich die Verwundbarkeit kritischer Infrastruktur gegenüber alltäglichen Vorgängen. Des Weiteren wird auch die fragile Anbindung von Entwicklungsländern an die globale Internet-Landschaft offenbar, da mehrere Länder während des Ausfalls nicht auf ausreichend Redundanzen zurückgreifen konnten.

Fallbeispiel: Totalausfall der libanesischen Internet-Anbindung [I45] Dieser Vorfall ist besonders interessant, da der Ausfall nicht auf eine Kabelbeschädigung, sondern auf geplante Wartungsarbeiten zurückzuführen ist. So wurde die Anbindung erst durch die Wartung selbst beeinträchtigt und anschließend durch Erweiterungsarbeiten am Kabel für mehrere Tage vollständig unterbrochen. Dies ist bemerkenswert, da der Betreiber den Kabelausbau dessen Kunden nicht kommunizierte, wodurch im Vorfeld auch keine ausreichenden Alternativkapazitäten aufgebaut werden konnten. Darüber hinaus zeigt sich auch hier die Abhängigkeit eines Landes von einer einzelnen Kabelverbindung.

2.1.2.5 Peering Dispute

Der Vorfallskatalog umfasst 9 Vorfälle, die durch ausgesetzte oder dauerhaft aufgekündigte Peering-Verbindungen zwischen großen Internet Service Providern verursacht wurden und im Zeitraum zwischen 2008 und 2015 aufgetreten sind. Die Ursachen derartiger Ausfälle sind selten technischer Natur, vielmehr liegen meist wirtschaftliche Differenzen zugrunde. Aus diesen oft langanhaltenden Auseinandersetzungen wird klar, dass hier vor allem eine bessere Rechtssprechung bzw. Regulierung nötig ist, um Betroffene vor einer Verschlechterung der Dienstqualität in Zukunft effektiver zu schützen. Empfohlene Detailanalysen sind Netflix-Störungen durch einen Provider-Streit zwischen Verizon und Level3 [I49] sowie ein Machtkampf zwischen den Tier1-ISPs Sprint und Cogent [I55].

Kategorie: **Peering Dispute**

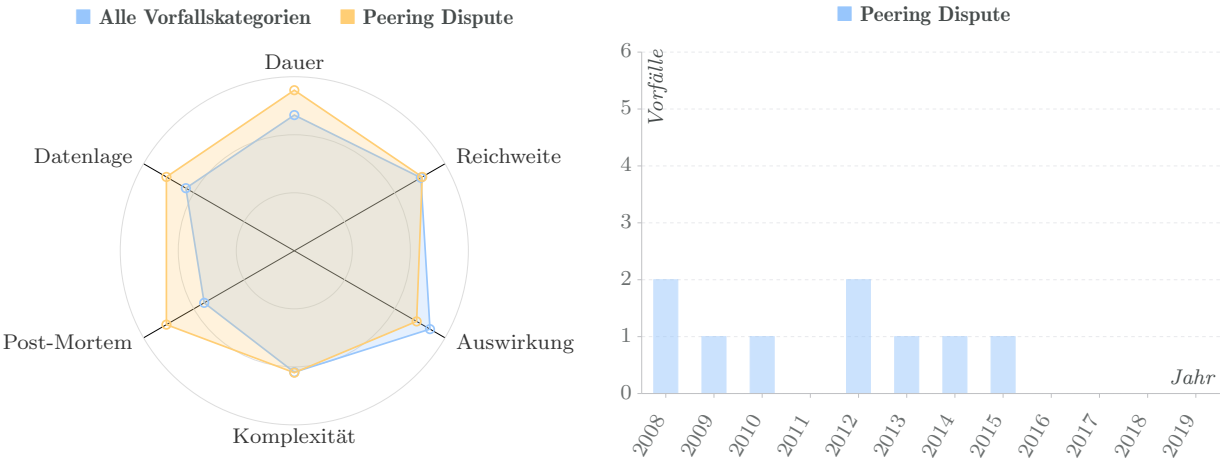
Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2015-12-08	Backbone	DTAG	Cogent verklagt Deutsche Telekom wegen Nicht-einhaltung von Peering-Verträgen [I48]	3	3	2	2	3	2
2014-06-22	Content	Netflix	Verizon nimmt Paketverlust bei Netflix über Level3-Peering in Kauf [I49]	3	2	2	1	3	3
2013-06-19	Content	Netflix	Verizon nimmt Paketverlust bei Netflix über Cogent-Peering in Kauf [I50]	3	2	2	1	2	2
2012-11-22	Content	YouTube	France Telecom blockiert YouTube regulierungs-konform im Peering-Streit mit Cogent [I51]	3	2	2	3	3	3
2012-02-23	ISP	Telstra	Upstream-ISPs beenden BGP-Sessions aufgrund eines vorangehenden Route Leaks [I52]	1	3	3	3	3	3
2010-11-29	Content	Netflix	Comcast fordert Paid-Peering mit Level3 auf-grund einseitigem Netflix-Verkehr [I53]	3	2	2	2	2	2
2009-10-12	Backbone	Hurricane	Peering-Streit zwischen Hurricane Electric und Cogent führt zu Teilung des IPv6-Internets [I54]	3	3	3	3	3	2
2008-10-30	Backbone	Cogent	Sprint beendet Peering mit Cogent als Reaktion auf eskalierenden Peering-Streit [I55]	3	3	3	2	3	3
2008-03-13	Backbone	Telia	Cogent beendet Peering mit Telia wegen Nicht-einhaltung von Peering-Vereinbarungen [I56]	3	3	3	2	1	3

Ursachen Auseinandersetzungen zwischen großen Providern basieren in der Regel auf einem ungleichen Verkehrsverhältnis, in dem einer der beiden Peering-Partner unverhältnismäßig mehr Daten sendet, als er entgegennimmt, und damit auch ungleich mehr von einer – meist kostenneutralen – Peering-Verbindung profitiert. In der Konsequenz drängen benachteiligte Provider häufig auf einseitige Paid-Peering-Verträge, um die wirtschaftlichen Nachteile des erhöhten Verkehrsaufkommens auszugleichen. Nicht selten liegt die Ursache eines unausgewogenen Traffic Ratios dabei in einzelnen Streaming-Diensten [I49, I50, I51] begründet, deren Verkehr im Netz des betroffenen Providers billigend einem erheblichen Paketverlust ausgesetzt oder in Einzelfällen auch vollständig blockiert wird. Dementsprechend führen Peering-Auseinandersetzungen in der Regel auch zu unmittelbaren Qualitätseinbußen bei Endanwendern. Die daraus resultierenden Beschwerden der Content-Anbieter selbst sowie deren große Nutzerbasis werden von Peering-Partnern oft bewusst als Druckmittel eingesetzt, um die eigenen Vorstellungen bzgl. des jeweiligen Peering-Übereinkommens durchzusetzen. Oftmals werden im Zuge von Auseinandersetzungen jedoch nicht nur einzelne Dienste oder Router überlastet, sondern Peering-Verbindungen auch einseitig und meist spontan aufgekündigt [I54, I55, I56]. Parallel zu unmittelbaren technischen Maßnahmen werden in der Regel auch rechtliche Schritte eingeleitet. So wurde die Deutsche Telekom von Cogent verklagt, da laut deren Aussage ein vertraglich festgeschriebener Kapazitätsausbau verweigert wurde [I48]. Schlussendlich können Peering-Ausfälle aber auch aufgrund technischen Versagens oder Fehlverhaltens erfolgen. In einem Vorfall wurde eine Peering-Verbindung als Reaktion auf mangelhafte Routenfilter [I52] des Partners beendet, um dem steigenden Risiko eines Route Leaks über diesen Provider zu begegnen.

Betroffene Wird eine Peering-Verbindung zwischen großen Providern beendet, zieht dies neben einer potentiellen Verschlechterung der Dienstqualität der jeweiligen Kunden, meist im Content-Bereich [I49, I50, I51] auch Konsequenzen im Internet-Backbone [I48, I54, I55, I56] nach sich. Da weggefallene Peering-Verbindungen durch alternative Routen kompensiert werden müssen, ist mit kurzzeitigen Unterkapazitäten und damit sporadischen Beeinträchtigungen im gesamten Internet-Routing zu rechnen. Darüber hinaus kann ein Depeering-Ereignis für einzelne *single-homed* Netzwerke, d.h. für Netzwerke mit nur einem Provider für Internet-Konnektivität, auch zu einer Teilabtrennung vom Internet [I54] führen. Entsprechende Dienste und Kunden auf beiden Seiten der Peering-Verbindung, meist direkte Enterprise-Kunden [I55] der in den Vorfall verwickelten Peering-Partner, können sich dadurch gegenseitig nicht mehr erreichen. Analog dazu kann auch die Internet-Konnektivität einzelner ISPs [I52] in Mitleidenschaft gezogen werden.

Gegenmaßnahmen Konkrete technische Gegenmaßnahmen können von allen Netzbetreibern selbst getroffen werden, indem sie sich *multi-homed*, d.h. über mehrere Provider, mit dem Internet verbinden. Dadurch kann im Falle von Peering-Abbrüchen unmittelbar auf alternative Routen ausgewichen werden. Für Endkunden bietet sich diese Möglichkeit jedoch nicht, sie sind den Peering-Machtkämpfen in der Regel hilflos ausgeliefert. Um ungleiche Verkehrsverhältnisse und damit Differenzen im Vorfeld zu vermeiden, sollten Peering-Verträge öffentlich ausgehandelt und überwacht werden. Auch sollten Content-Anbieter neben verstärktem Einsatz von lokalen Caching-Servern mehr in die Pflicht zum Paid-Peering [I53] genommen werden, da diese Anbieter zumeist für das gesteigerte Verkehrsaufkommen verantwortlich zeichnen und am höchsten davon profitieren. Gleichzeitig sollte eine mutwillige Router-Überlastung als Mittel zur Degradierung [I49, I50] oder Blockierung [I51] von Internet-Verkehr über Netzneutralitätsgesetze unterbunden werden.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.5).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.5: (Peering Dispute) **Statistische Auswertung**

- *Hohe Dauer*, da die Ursachen selten technischer Natur, sondern meist in wirtschaftlichen oder juristischen Auseinandersetzungen begründet sind. Rechtsstreite und öffentlich ausgetragene Machtkämpfe können sich über Monate hinziehen.

- *Hohe Reichweite*, da eine breite Kundenbasis der Peering-Partner und zumeist auch unabhängige Content-Dienste mit ebenso hohen Nutzerzahlen betroffen sind.
- *Mittlere Auswirkung*, da neben juristischen Konsequenzen für Peering-Partner nur mit verminderter Dienstqualität, jedoch nicht mit Totalausfällen zu rechnen ist.
- *Komplexität* mittel, da der Markt zwar großes Potential für wirtschaftliche Konflikte bietet, diese aber selten eskalieren und nur einen kleinen Kreis von ISPs betreffen.
- *Post-Mortem* überdurchschnittlich, da Peering-Differenzen meist mit Stellungnahmen der betroffenen Parteien sowie richterlichen Entscheidungen einhergehen und sich Maßnahmen für eine Vielzahl an Endkunden unmittelbar bemerkbar machen.
- *Datenlage* überdurchschnittlich, da Peering-Verbindungen sowie der Kundenstamm von Peering-Partnern in der globalen Routing-Tabelle sichtbar sind und neben Beobachtungen zudem auch Simulationen duchgeführt werden können.

Risikobewertung Das Schadenspotential von Peering Disputes ist im Allgemeinen als hoch zu bewerten. Auch wenn keine Totalausfälle zu erwarten sind, so ergeben sich insbesondere aus der hohen Dauer und Reichweite der Vorfälle, der integralen Rolle großer Transit-ISPs sowie potentiell spontanen Verkehrsumleitungen im Multi-100 GBit/s Bereich unkalkulierbare Risiken für die weltweite Internet-Infrastruktur.

Schadenspotential	**Hoch**
Eintrittserwartung	**Gering**

Kategorie: **Peering Dispute**

Die Eintrittserwartung von Peering Disputes wird als gering eingeschätzt. Bedeutsame Vorfälle treten häufigstenfalls 1-2 mal pro Jahr, nicht aber in den letzten fünf Jahren auf. Mit der Zunahme anbietereigener CDNs und netzlokaler Caches sowie einer steten Neuausrichtung von Transit-Geschäftsmodellen auf den Content-Markt sinkt das Konfliktrisiko. Letztlich liegen Selbstschutzmaßnahmen für neutrale Netzbetreiber auf der Hand.

Fallbeispiel: Netflix-Störungen durch einen Provider-Streit [I49] Verizon nimmt Paketverlust bei Netflix über eine Peering-Verbindung im Streit mit Level3 billigend in Kauf. Dieser Vorfall ist vor allem deshalb von Interesse, weil er in vollem Umfang öffentlich ausgetragen wurde und dadurch tiefe Einblicke in die Hintergründe und Motivationen der jeweiligen Akteure erlaubt. Zudem trug der Vorfall zu einem Strategiewechsel bei Netflix hin zu einem eigenen Content Delivery Network und verstärktem Einsatz von lokalen Caching-Servern bei. Zuletzt verdeutlicht der Fall auch die Notwendigkeit einer starken Gesetzgebung zur Netzneutralität inkl. Mechanismen zu deren Überwachung und Durchsetzung, um Internet-Machtkämpfe auf Kosten von Endkunden zu unterbinden.

Fallbeispiel: Depeering zwischen Sprint und Cogent [I55] Sprint beendet eine Peering-Verbindung mit Cogent als Reaktion auf eskalierende Differenzen. Der Fall ist ein Musterbeispiel für Peering-Probleme, bei denen ungleiche Verkehrsverhältnisse zur einseitigen Aufkündigung einer Verbindung führen. Selbst nach deren vollständiger Wiederherstellung ist auf beiden Seiten ein dauerhafter Kundenverlust zu verzeichnen. Der Vorfall verdeutlicht die erheblichen Auswirkungen auf single-homed Netzwerke und Endkunden, und zeigt unmittelbare Folgen für Internet Service Provider auf.

2.1.2.6 Route Leak

Der Vorfallskatalog umfasst 13 Vorfälle, die durch BGP Route Leaks verursacht wurden und im Zeitraum zwischen 2012 und 2019 aufgetreten sind. Die große Anzahl und Regelmäßigkeit dieser Vorfälle zeigt, wie unzureichend und fehleranfällig die heutzutage eingesetzten Schutzmechanismen sind. Noch schwerer wiegt, dass Route Leaks stets den Internet-Backbone selbst betreffen, wodurch entsprechende Vorfälle eine sehr große Reichweite aufweisen, auch wenn sich deren hohe Auswirkungen durch schnelle Mitigation begrenzen lassen. Empfohlene Detailanalysen sind der Wegbruch von Peering-Sessions am AMS-IX [I57] aufgrund eines Route Leaks sowie weltweite Beeinträchtigungen durch fehlerhafte Routen eines BGP-Optimizers [I58].

Kategorie: **Route Leak**

Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-07-24	Backbone	AMS-IX	Durch DDoS-Schutz deaggregiertes Peering-LAN-Präfix propagiert über Telia und führt zum Ausfall zahlreicher BGP Sessions [I57]	2	3	3	3	2	3
2019-06-24	Backbone	Verizon	Akzeptanz von 20,000 more-specific Präfixen deaggregiert durch BGP Optimizer führt zu nicht erreichbaren OTT-Diensten [I58]	2	3	3	3	3	3
2019-06-06	Backbone	China Telecom	Akzeptanz von 70,000 same-specific Präfixen eines Schweizer Cloud-Anbieters führt zu weltweiten Beeinträchtigungen im Internet [I59]	2	3	2	1	1	3
2018-11-12	Content	Google	Less-specific Cloud Network Präfixe propagieren über IXP in Nigeria und China Telecom und führen zu weltweiten Dienststörungen [I60]	2	2	2	1	2	3
2017-11-06	ISP	Comcast	Reannoncierung von same-specific Kunden-Präfixen durch Level3 führt zu landesweitem Dienstausfall aufgrund überlasteter Router [I61]	2	2	3	1	1	3
2017-08-25	Backbone	Verizon	Akzeptanz von 135,000 Präfixen (teils more-specific) annonciert durch Google führt zu Internet-Ausfällen insbesondere in Japan [I62]	1	3	3	3	1	3
2016-04-22	Backbone	Hurricane	Akzeptanz von 3,500 more-specific Präfixen deaggregiert durch BGP Optimizer eines Schweizer Hosters führt zu weltweiten Störungen [I63]	1	3	3	3	3	3
2015-11-06	Backbone	Cogent	Akzeptanz von 16,000 same-specific Präfixen des indischen ISP Bharti Airtel führt zu weltweiten Beeinträchtigungen im Internet [I64]	2	3	2	1	1	3
2015-06-12	Backbone	Level3	Akzeptanz von 176,000 same-specific Präfixen über Telekom Malaysia führt zu weltweiten Beeinträchtigungen im Internet [I65]	2	3	2	1	1	3
2015-03-12	Content	Google	Same-specific Präfixe aller Google-ASe annonciert durch indischen ISP führen zu Dienstausfällen in Europa und Asien [I66]	1	2	2	1	1	3
2015-03-27	Backbone	Los Angeles IXP	Akzeptanz von 7,000 more-specific Präfixen deaggregiert durch BGP Optimizer eines US-Hosters führt zu weltweiten Störungen [I67]	2	3	3	3	1	3

2014-04-02	Backbone	Hurricane	Akzeptanz von 415,000 same-specific Präfixen des indonesischen ISPs Indosat führt zu weltweiten Beeinträchtigungen im Internet [I68]	2	3	2	1	1	2
2012-08-08	Backbone	Bell	Akzeptanz von 105,000 same-specific Präfixen eines kanadischen ISPs führt zu weltweiten Beeinträchtigungen im Internet [I69]	2	3	2	1	1	2

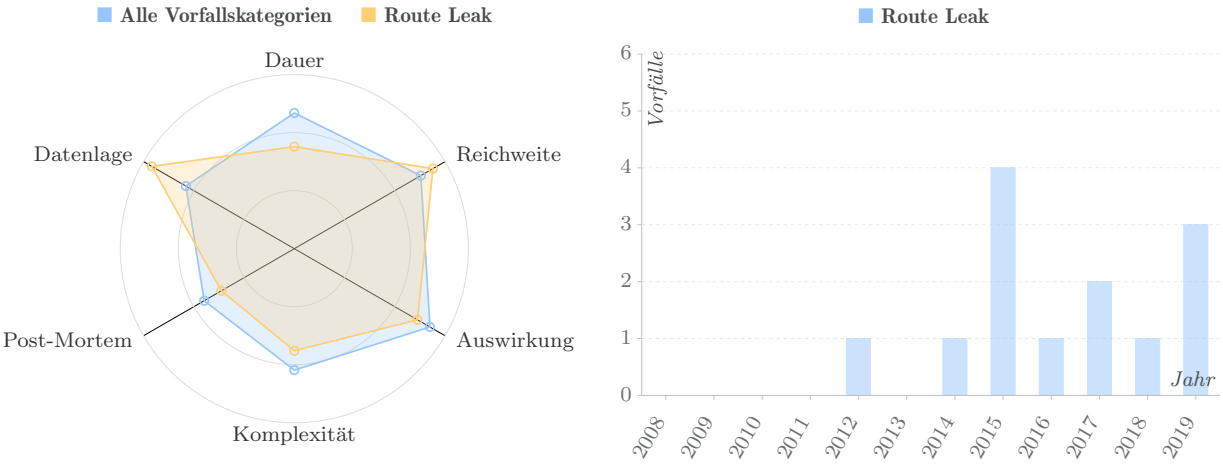
Ursachen Die eigentliche Ursache für Route Leaks sind stets Konfigurationsfehler im weiteren Sinne, bspw. Fehler in der Konfiguration von BGP-Filtern, wodurch betreiberinterne Routen-Updates ungewollt an benachbarte Provider weitergereicht und damit – oft Internet-weit – Verkehrsströme angezogen werden. Die Auswirkungen von Route Leaks reichen von längeren IP-Pfaden (über das Netzwerk der Verursacher) und dadurch erhöhten Latenzen bis hin zu vollständigem Paketverlust durch Überlastung deren Router, die nicht auf das stark erhöhte Verkehrsaufkommen ausgelegt sind. In erster Linie werden Routen in BGP bevorzugt, wenn diese spezifischer sind als bestehende Routen, also zu längeren IP-Präfixen führen. Dementsprechend sind spezifischere Routen die häufigste Ursache für die Akzeptanz und schneller Verbreitung von Route Leaks [I57, I58, I61, I62, I65, I66, I67]. Meist resultieren spezifischere Routen aus dem Einsatz von Route Optimizern zum Zwecke eines Traffic Shapings, aber auch BGP-basierte DDoS-Schutzmechanismen kommen als Ursache für Route Leaks in Frage. Vergleichbare Probleme resultieren aus der weltweiten Verbreitung von Routen zu nicht-öffentlichen Netzbereichen, bspw. dem Peering-LAN von Internet Exchange Points [I59, I60]. Über BGP-spezifische Attribute wie *local preference* können darüber hinaus auch weniger attraktive Routen, d.h. zu gleich- oder weniger-spezifischen IP-Präfixen, von Providern unerwartet bevorzugt werden [I69], was die sonst begrenzte Verbreitung derartiger Route Leaks fördert. Nicht immer sind die Ursachen eines entstehenden Route Leaks offensichtlich [I64, I68] und durch geeignete Filterkonfigurationen zu vermeiden. Bei gleich-spezifischen Routen werden bspw. kürzere AS-Pfade in aller Regel bevorzugt, die von vielen Providern jedoch mittels *AS path prepending* künstlich verlängert werden, um Backup-Routen vorzuhalten oder Verkehrsflüsse zu optimieren. Diese ISPs sind in besonderem Maße anfällig für Route Leaks.

Betroffene Aufgrund der zumindest regionalen, meist jedoch globalen Ausbreitung von Route Leaks ist der Internet-Backbone am häufigsten von entsprechenden Vorfällen betroffen [I57, I58, I59, I62, I63, I64, I65, I67, I68, I69]. Seltener beschränken sich Route Leaks auf Netzwerke einzelner Anbieter oder betreffen nur spezifische Dienste wie Content [I60, I66]. In Einzelfällen können auch nur wenige IP-Präfixe eines ISPs [I61] und damit ausschließlich dessen lokale Kundenbasis beeinträchtigt werden.

Gegenmaßnahmen Konkrete ISP-spezifische Maßnahmen sind nicht immer bekannt oder nur unzureichen dokumentiert, es befindet sich jedoch eine Vielzahl verschiedener Schutzmaßnahmen im Einsatz. Diese basieren meist auf manuell gepflegten Filterlisten oder Schwellwerten, bspw. einer je BGP-Nachbar festgelegten maximalen Anzahl von IP-Präfixen, die über Routen-Updates akzeptiert werden. In überschaubaren Szenarien sind explizite IP-Präfix-Listen durchaus gängige Praxis, über die sowohl eine Einschränkung der Weitergabe als auch der Akzeptanz von IP-Präfixen je BGP-Nachbar realisiert werden kann. Diese Maßnahmen skalieren jedoch nicht für große Provider oder Internet Exchange Points und sind durch ihren manuellen Charakter sehr fehleranfällig. Dementsprechned

werden häufig auch automatisierte Routen-Filter basierend auf dokumentierten Routing Policies in öffentlichen Internet Routing Registries (IRR) eingesetzt. Deren genaue Funktionsweise ist Provider-abhängig, jedoch resultieren auch diese Filter letztlich aus manuell erzeugten IRR-Einträgen, die häufig unvollständig, veraltet oder fehlerhaft sind. Mit zunehmender Verbreitung der Resource Public Key Infrastructure (RPKI), durch die die Gültigkeit von Routen-Updates kryptografisch verifiziert werden kann, wird sich dem Problem von Route Leaks perspektivisch besser begegnen lassen.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.6).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.6: (Route Leak) **Statistische Auswertung**

- *Geringe Dauer*, da die ursächlich an der Verbreitung von Route Leaks beteiligten ISPs meist kurzfristig reagieren können. Oft greifen auch größere Provider mit eigenen Filtern in das Routing ein, was schnell zur Eindämmung des Problems führt.
- *Hohe Reichweite*, da in der Regel unabhängige und geographisch breit gestreute Netzbereiche und damit auch eine Vielzahl an Diensten betroffen sind. Einmal ausgelöst, folgt innerhalb weniger Minuten eine potentiell weltweite Verbreitung.
- *Mittlere Auswirkung*, da sich Route Leaks zwar schnell erkennen und eindämmen lassen, BGP-Konvergenzeffekte aber noch über Stunden durch verminderte Dienstqualität nachwirken können. Verbindungsausfälle beschränken sich meist auf wenige Minuten, Schäden an Diensten oder Infrastruktur sind nicht zu erwarten.
- *Komplexität* mittel, da die Ursachen für Route Leaks vielfältig sind, jedoch zahlreiche Best-Effort Schutzmaßnahmen zu deren Vermeidung eingesetzt werden. Die globale Verbreitung spezifischerer Routen setzt beim Verursacher meist die Verwendung einer komplexe Routen-Optimierung voraus, gleich-spezifische Routen mit nur regionaler Akzeptanz können prinzipiell aus jedem Netzwerk weltweit entweichen.
- *Post-Mortem* unterdurchschnittlich, da meist weder konkrete Ursachen noch kurzfristig getroffene Maßnahmen von den beteiligten Providern kommuniziert werden.
- *Datenlage* überdurchschnittlich, da aus BGP-Nachrichten betroffene Netzbereiche und teilweise auch der genaue Routing-Hergang rekonstruiert werden können.

Risikobewertung Das Schadenspotential von Route Leaks ist im Allgemeinen als mittel zu bewerten. Große Transit-ISPs erzwingen bei überregionalen Verbindungsaufällen schnellste Mitigation. Die generell sehr geringe Dauer von Vorfällen wiegt potentiell hohe Reichweiten auf. Best Practices und Schutzmechanismen sind in große Fülle vorhanden, perspektivisch nimmt das Schadenspotential mit der weiteren Verbreitung von RPKI ab.

Schadenspotential	**Mittel**
Eintrittserwartung	**Hoch**

Kategorie: **Route Leak**

Die Eintrittserwartung von Route Leaks wird als hoch eingeschätzt und nimmt mit dem kontinuierlichen Wachstum des Internets weiter zu. Insbesondere mit weniger komplexen Route Leaks, d.h. einer fälschlichen Verbreitung gleich-spezifischer IP-Präfixe, ist im Tagesgeschäft jederzeit zu rechnen.

Fallbeispiel: Wegbruch von Peering-Sessions am AMS-IX [I57] Durch einen BGP-basierten DDoS-Schutz wird der private Peering-LAN IP-Präfix des weltweit zweitgrößten Internet Exchange Points in Amsterdam deaggregiert und global über den Tier1-ISP Telia verbreitet. Ein Großteil der IXP-Teilnehmer bevorzugt die öffentliche Route, wodurch deren private BGP-Verbindungen am IXP zusammenbrechen. Dieser Vorfall zeigt eindringlich die Verwundbarkeit auch von kritischer Infrastruktur gegenüber Route Leaks und die fragile Natur des Internet-Routings. Die ungewöhnlichen und schwer vorhersehbaren Ereignisse machen diesen Vorfall ebenso wie die Hilflosigkeit der IXP-Betreiber besonders lehrreich. Bemerkenswert ist außerdem, dass trotz der gravierenden Router-Ausfälle keine öffentliche Berichterstattung zu diesem Vorfall erfolgte.

Fallbeispiel: Weltweite Störungen durch fehlerhaften BGP-Optimizer [I58] Eine Deaggregierung von 20.000 IP-Präfixen durch einen BGP Optimizer führt zu zahlreichen nicht mehr erreichbaren OTT-Diensten. Dieser Vorfall ist vor allem aufgrund der Totalausfälle populärer Dienste bemerkenswert. Derart große Auswirkungen wurden durch das Zusammenspiel einer auf verkehrslastige Netze spezialisierten Routen-Optimierung und unzureichender Filtermechanismen eines internationalen Tier1-Providers stark begünstigt. Nicht zuletzt wurde der genaue Vorfallshergang auch von einem betroffenen Anbieter in großem Detail aufgearbeitet und dokumentiert.

2.1.2.7 BGP-Hijacking

Der Vorfallskatalog umfasst 8 Vorfälle, die durch BGP-Hijacking verursacht wurden und im Zeitraum zwischen 2013 und 2019 aufgetreten sind. Dabei zeigt sich, dass nicht immer zwischen einem gezielten Angriff und einer Fehlkonfiguration unterschieden werden kann, vor allem weil vordergründig oft keine Motivation erkennbar ist. Nichtsdestotrotz finden sich auch Angriffe im Vorfallskatalog, bei denen BGP-Hijacking mit großer krimineller Energie zum Einsatz kommt. Empfohlene Detailanalysen umfassen abgefangenen Bitcoin Mining-Verkehr [I75] und BGP-Hijacking durch einen italienischen Geheimdienst [I76].

Kategorie: **BGP-Hijacking**

Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-05-08	DNS	TWNIC	ISP in Brasilien übernimmt kurzzeitig Privacy-fokussierten DNS-Dienst Quad-101 [I70]	1	2	2	2	1	3
2018-07-30	Content	Telegram	Iran Telecommunication übernimmt spezifischere Präfixe des Messenger-Dienstes [I71]	1	2	3	1	1	3
2018-04-24	DNS	Amazon	US-ansässiger ISP übernimmt DNS-Dienst und leitet Bitcoin-Wallets nach Russland um [I72]	2	2	3	3	1	3
2017-12-12	Content	OTTs	Russisches Schläfer-AS übernimmt 80 Präfixe populärer Dienste für wenige Minuten [I73]	1	3	2	1	1	3
2017-04-26	Enterprise	Finanzsektor	Rostelecom übernimmt 50 Präfixe populärer Bezahldienstleister für wenige Minuten [I74]	1	3	2	1	1	3
2014-02-03	Cloud	Amazon	Kanadischer ISP fängt mehrfach Bitcoin Mining-Verkehr im Wert von $83,000 ab [I75]	3	2	2	3	1	3
2013-08-16	Cloud	Santrex	Hacking Team unterstützt italienischen Geheimdienst bei Angriff auf eigenen Server [I76]	3	1	1	1	2	3
2013-03-21	Enterprise	Spamhaus	Übernahme des DNSBL-Dienstes führt zu weitreichender Spam-Markierung von Emails [I77]	3	2	3	3	2	3

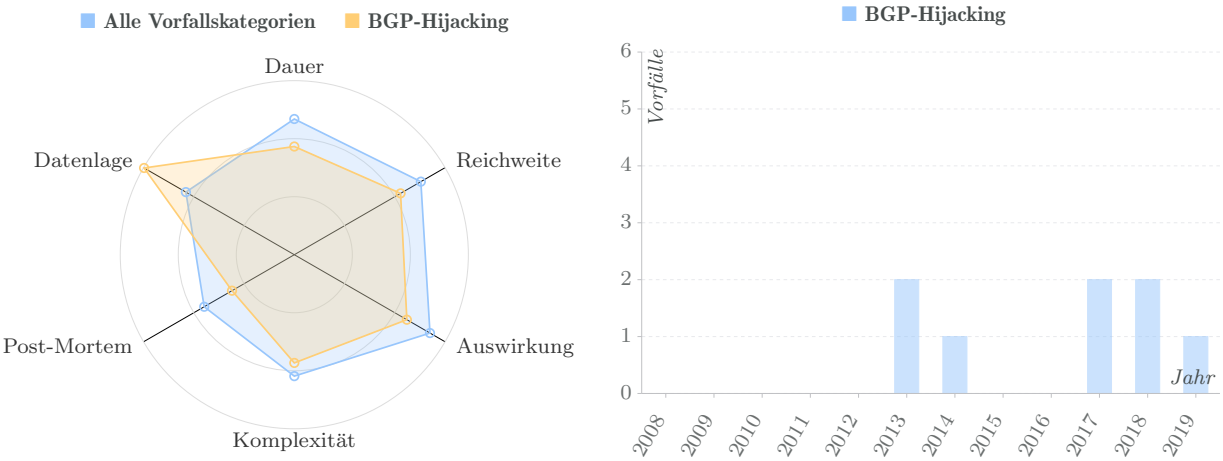
Ursachen Es wird zwischen zwei Ausprägungen von BGP-Hijacking unterschieden. Im einfacheren Fall trennt ein Angreifer einzelne Netzbereiche fremder autonomer Systeme durch gezielte Manipulation der globalen Routing-Tabelle teilweise oder vollständig vom Internet ab [I70, I73, I74, I76, I77]. Dieser Vorgang – technisch äquivalent zu Route Leaks (siehe Abschnitt 2.1.2.6) – führt zur Umleitung von Verkehrsströmen des Betroffenen in das Netz des Angreifers, die dort meist bewusst verworfen werden. In seltenen Fällen lassen sich auch Dienste des Angegriffenen replizieren und in beliebiger Weise manipulieren [I77]. Eine deutlich komplexere BGP-Hijacking Variante stellen Man-in-the-Middle bzw. Interception-Angriffe [I71, I72, I75] dar, bei denen regionale oder weltweite Verkehrsströme zwar ebenfalls vom Angreifer angezogen werden, durch weiterführende BGP-Manipulation jedoch auch eine stabile Rückroute zum Netz des Betroffenen aufrecht erhalten wird. Dies ermöglicht dem Angreifer eine transparente Weiterleitung eingehender Verkehrsströme und damit potentiell auch das Mitlesen oder Manipulieren der jeweiligen Kommunikation. Abgesehen von leicht erhöhten Latenzen lassen sich derartige Angriffe kaum nachweisen. Generell sind BGP-Hijacking Vorfälle nur sehr schwer von Route Leaks zu unterscheiden, sofern keine öffentlichen Stellungnahmen der Betroffenen hinsichtlich möglicher Motive vorliegen. Je zielgerichteter aber eine Verkehrsumleitung, vielfach beschränkt auf einzelne Netzbetreiber, desto wahrscheinlicher ist ein Angriff. Konkrete Motive dafür sind neben einer reinen Störung von Netzwerken bspw. auch die Umleitung von Bitcoin-Verkehr [I72, I75], persönliche Rache [I77] sowie die Übernahme eines Netzbereichs durch einen Geheimdienst [I76]. Im Fall von umgeleiteten Verkehren des populären Messenger-Dienstes Telegram durch den Iran [I71] wird Zensur vermutet.

Betroffene BGP-Hijacking Angriffe fokussieren sich im Gegensatz zu unbeabsichtigten Route Leaks in der Regel nur auf wenige oder einzelne Netzbereiche, in keinem bekannten Fall aber auf den Internet-Backbone als Ganzes. Dienste für DNS [I70, I72], Content [I71, I73], Enterprise [I74, I77] und Cloud [I75, I76] sind dagegen in gleichem Maße betroffen.

Es ist allerdings anzumerken, dass im Falle von umgeleiteten Bitcoin-Verkehren zwar Cloud [I75] und DNS [I72] Dienste angegriffen wurden, das eigentliche Ziel dieser Angriffe jedoch stets der Diebstahl von Crypto-Währung bei Endanwendern war.

Gegenmaßnahmen Die Resource Public Key Infrastructure (RPKI) wurde mit dem Ziel einer kryptografischen Routen-Verifizierung entwickelt und eignet sich demnach prinzipiell auch zur Unterbindung von BGP-Hijacking Angriffen. Während bei technisch vergleichbaren Route Leaks damit in aller Regel der Ursprung illegitimer Routen überprüfbar wird, können versierte Angreifer jedoch auch diese Informationen manipulieren. Ein vollständiger Schutz auch gegen fortgeschrittene Angriffe wird demnach erst durch die Protokollerweiterung BGPsec erreicht, mit der jeglicher Austausch von Routen zwischen autonomen Systemen verifizierbar ist. Auch wenn RPKI als integraler Bestandteil von BGPsec bereits weite Verbreitung findet, ist mit einem flächendeckenden Einsatz einer vollständigen Pfadvalidierung – auch aufgrund der hohen Hardware-Anforderungen für kompatible Router – in absehbarer Zeit nicht zu rechnen. Ein vollumfänglicher Schutz gegen BGP-Hijacking ist zum heutigen Zeitpunkt nicht zu erreichen, allerdings können erfolgreiche Man-in-the-Middle Angriffe durch konsequenten Einsatz von Ende-zu-Ende-Verschlüsselung weitestgehend ausgeschlossen werden. Ungeachtet dessen ist eine Vielzahl an Beobachtungs- und Erkennungssystemen verfügbar, mit deren Hilfe Angriffe schnell erkannt und in Zusammenarbeit mit den Network Operations Centern größerer Transit-ISPs dort durch manuelle Anpassung von Filterlisten mitigiert werden können.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.7).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.7: (BGP-Hijacking) **Statistische Auswertung**

- *Mittlere Dauer*, da BGP-Hijacking Angriffe bis auf wenige schwerwiegendere Ausnahmen nur über kurze Zeiträume aufrecht erhalten werden können. Meist werden illegitime Routen sofort erkannt und durch größere Transit-ISPs schnell ausgefiltert.
- *Mittlere Reichweite*, da Angriffe stets auf einzelne oder wenige Netzbereiche abzielen, davon aber prinzipiell beliebige Dienste oder Kundenkreise abhängen können. Internet-weite Störungen durch Angriffe auf Kerndienste sind theoretisch denkbar.
- *Mittlere Auswirkung*, da zwar generell mit Totalausfällen gerechnet werden muss, in der Regel aber auch schnell erste Gegenmaßnahmen eingeleitet werden können.

- *Komplexität* mittel, da für Angriffe zwar Expertenwissen und eine aktive Teilnahme am BGP-Routing nötig ist, der tatsächliche Ressourcenbedarf jedoch sehr gering ist.
- *Post-Mortem* unterdurchschnittlich, da Angriffe von Betroffenen selten veröffentlicht werden und ergriffene Schutz- und Gegenmaßnahmen stets fallabhängig sind.
- *Datenlage* überdurchschnittlich, da eine Manipulation der globalen Routing-Tabelle stets mit beobachtbaren BGP-Nachrichten einhergehen muss und zahlreiche öffentlich zugänglichen Datenquellen und Erkennungssysteme existieren.

Risikobewertung Das Schadenspotential von BGP-Hijacking ist im Allgemeinen als mittel zu bewerten. Vorfälle dauern aufgrund schneller Mitigation meist nur kurz an, können jedoch fallabhängig auch über lange Zeiträume unbemerkt bleiben. Von Einzelfällen abgesehen sind weder hohe Reichweiten noch gravierende Auswirkungen im Internet zu verzeichnen. Etwaige Folgeschäden durch Datendiebstahl oder Nichtverfügbarkeit von Diensten beschränken sich auf einzelne meist gezielt ausgewählte Netzbetreiber, könnten allerdings grundsätzlich auch an kritischer Infrastruktur hervorgerufen werden.

Schadenspotential	**Mittel**
Eintrittserwartung	**Mittel**

Kategorie: **BGP-Hijacking**

Die Eintrittserwartung von BGP-Hijacking wird als mittel eingeschätzt. Zwar existieren keine zuverlässigen Schutzmaßnahmen, auch sind im Vergleich zu anderen Denial-of-Service-Varianten nur geringe Ressourcen nötig. Gleichzeitig bedürfen Manipulationen in BGP längerer Vorbereitungszeit und sind aufgrund der potentiell globalen Sichtbarkeit kaum für diskrete Angriffe im Verborgenen geeignet.

Fallbeispiel: Abgefangener Bitcoin Mining-Verkehr [I75] Über einen kanadischen ISP werden durch Umleitung von unverschlüsseltem Mining-Verkehr Bitcoins im Wert von $ 83.000 erbeutet. Dieser Vorfall verdeutlicht eindringlich, wie einfach und effektiv BGP-Hijacking für den Diebstahl von sensiblen Daten eingesetzt werden kann. Ferner wird damit belegt, dass Routing-Angriffe grundsätzlich auch auf Endkunden möglich sind. Es wird allerdings ebenso ersichtlich, dass im Vorfeld Detailwissen über den abgefangenen Verkehr notwendig ist und welche generell wichtige Rolle Verschlüsselung zum Schutz gegen Man-in-the-Middle Angriffen im Internet spielt.

Fallbeispiel: BGP-Hijacking durch einen italienischen Geheimdienst [I76] Eine Hacker-Gruppierung unterstützt die italienischen Behörden bei einem Angriff auf deren eigenen, anderweitig nicht mehr zu erreichenden Kontroll-Server. Dieser Vorfall ist vor allem aufgrund der Einblicke in behördliche Hintergründe und technische Fähigkeiten eines NATO-Staats von Interesse. Er zeigt, wie BGP-Hijacking eingesetzt wurde, um einen fremden, nicht mehr gerouteten Netzbereich zu reaktivieren und dadurch essentielle, auf dem so wieder erreichbaren Server gespeicherten Informationen zurück zu erlangen.

2.1.2.8 Denial-of-Service

Der Vorfallskatalog umfasst 11 Vorfälle, die durch DoS-Angriffe verursacht wurden und im Zeitraum zwischen 2012 und 2019 aufgetreten sind. Dabei zeigt sich, dass derartige Überfälle auf populäre Dienste für Angreifer sehr Ressourcen-intensiv sind und in aller Regel Fachwissen und große kriminelle Energie voraussetzen. Gleichzeitig ist das Risiko durch Angriffe als Bezahldienstleistung allgegenwärtig. Von Vorfällen betroffen sind dabei hauptsächlich Web-Dienste und DNS-Infrastruktur. Empfohlene Detailanalysen sind ein Amplification-Angriff auf GitHub.com [I81] sowie ein Botnet-Angriff auf Dyn [I84].

Kategorie: **Denial-of-Service**

Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-08-18	Cloud	servers.com	139 Gbps TCP SYN/ACK Amplification-Angriff mit wechselnden Angriffsvektoren [I78]	3	2	3	3	3	3
2019-09-06	Content	Wikimedia	Gezielter DDoS-Angriff führt zu europaweitem Ausfall von Wikimedia-Diensten [I79]	2	2	3	2	3	3
2019-03-05	Enterprise	Arbor	1.7 Tbps memcached Amplification-Angriff mitigiert ohne Ausfall von Diensten [I80]	?	?	1	3	2	1
2018-02-28	Content	GitHub.com	1.3 Tbps memcached Amplification-Angriff mit mehrstufiger Cloudflare-Mitigierung [I81]	1	2	2	3	3	3
2017-03-02	DNS	GoDaddy	DDos-Angriff auf DNS-Infrastruktur mit minimaler Kommunikation und Datenlage [I82]	2	2	3	2	1	1
2016-11-03	Backbone	Liberia	DDoS-Angriff mit Mirai-Botnet führt zu landesweitem Ausfall der Internet-Infrastruktur [I83]	3	3	3	3	1	1
2016-10-21	DNS	Dyn	1.2 Tbps DDoS-Angriff mit Mirai-Botnet auf DNS-Server mit hohen Kollateralschäden [I84]	2	3	3	3	1	3
2016-06-25	DNS	rootops	17 Gbps TCP SYN Flooding-Angriff gleichzeitig auf alle DNS Root Server [I85]	2	3	2	3	1	3
2016-05-16	DNS	NS1	DDoS-Angriff auf DNS-Infrastruktur über mehrere unterschiedliche Angriffsvektoren [I86]	3	3	3	3	2	1
2016-03-24	DNS	DigitalOcean	DDoS-Angriff auf DNS-Infrastruktur basierend auf ausschließlich gültigen Anfragen [I87]	2	3	3	3	3	2
2012-09-10	DNS	GoDaddy	Vermeintlicher DDos-Angriff von Anonymous-Mitglied entpuppt sich als Netzausfall [I88]	2	3	3	3	1	1

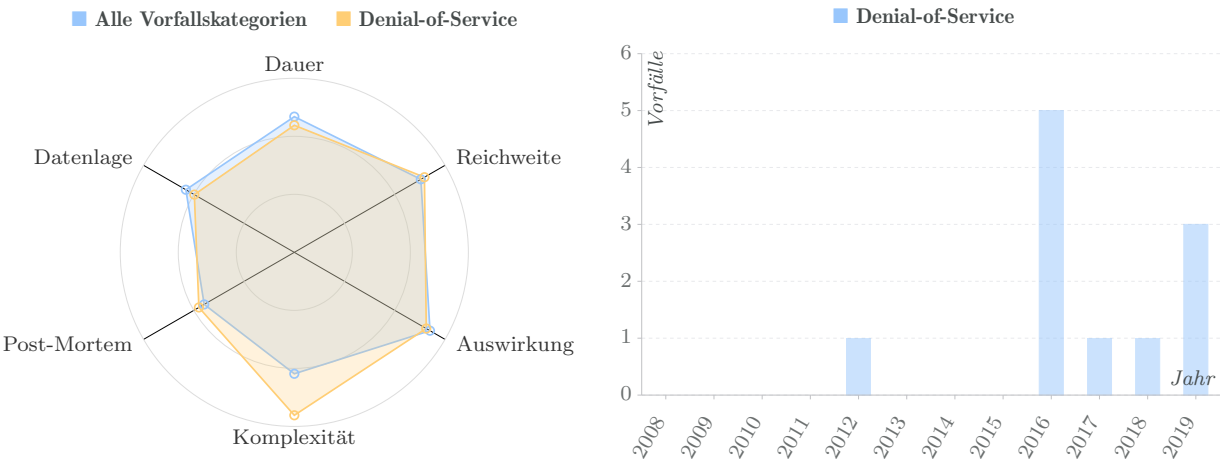
Ursachen Ziel von Denial-of-Service-Angriffen ist stets, einen Dienst oder ein Netzwerk so stark zu überlasten, dass ein normaler Betrieb nicht mehr möglich ist. Die dazu verwendeten Strategien können in mehrere Kategorien eingeteilt werden. Eine weit verbreitete Methode sind Amplification-Angriffe [I78, I80, I81], hierüber kann der Verkehr eines Angreifers durch Missbrauch öffentlich erreichbarer Drittdienste um ein Vielfaches verstärkt werden. Beispiele dafür sind öffentlich erreichbare LDAP- oder memcached-Server, die auf Anfragen mit gefälschter Absenderadresse eine vielfach größere Antwort an das Angriffsziel zurücksenden. Weiterhin werden auch Bot-Netze mit einer großen Zahl gekaperter Systeme eingesetzt, um massenhaft Anfragen an ein Ziel zu senden [I84, I83]. Dazu gehören beispielsweise schlecht gesicherte IoT-Geräte, die leicht durch einen Angreifer übernommen werden können. Zusätzlich können auch Schwachstellen in Diensten

selbst ausgenutzt werden, um mit speziellen Anfragen eine hohe Server-Auslastung hervorzurufen [I86, I87]. So können an einen DNS-Server bspw. massenhaft gültige Anfragen für nicht existierende Domain-Namen gesendet werden, deren Bearbeitung unverhältnismäßig hohe System-Ressourcen aufbraucht. In weiteren Vorfällen wurden keinerlei Details durch die angegriffenen Betreiber bekannt gegeben oder diese nur unspezifisch als volumetrische Angriffe bezeichnet [I79, I82, I85]. Zuletzt wurde auch ein vermeintlicher Denial-of-Service-Angriff im Nachhinein als technischer Fehler identifiziert [I88].

Betroffene Die häufigste angegriffene Dienstklasse ist DNS [I84, I82, I85, I86, I87, I88]. Dieser Dienst bietet für Angreifer zwei Vorteile. Zum einen lassen sich DNS-Server bereits durch gültige Anfragen leicht unter hohe Last setzen, was eine Mitigation erschwert. Zum anderen sind alle Dienste, deren Domain-Namen durch angegriffene DNS-Server aufgelöst werden, gleichermaßen durch einen Angriff betroffen, was dessen Reichweite potentiell erhöht. Regelmäßig werden aber auch Dienste wie Content [I79, I81], Cloud [I78] und Enterprise [I80] direkt angegriffen. Nur in einem Vorfall fand ein Angriff auf den Internet-Backbone [I83] statt, der zu einem Totalausfall in Liberia führte.

Gegenmaßnahmen Ein präventiver Schutz gegen DoS-Angriffe ist aufgrund der Offenheit des Internets generell nicht möglich und muss sich auf vorbereitende Maßnahmen zur Mitigation im Angriffsfall beschränken. Hier ist zwischen einer selektiven Filterung illegitimer Anfragen und der vollständigen Blockierung von schädlichem Verkehr zu unterscheiden. Die Filterung von großen Verkehrsvolumina, mittlerweile im TBit/s Bereich, ist allerdings äußerst aufwändig, weswegen hierfür meist auf eine Auslagerung zu externen Dienstleistern zurückgegriffen werden muss. Diese betreiben nicht selten eigene Rechenzentren, sog. *Scrubbing Center*, die ausschließlich der Filterung von Angriffsverkehr dienen [I80, I81] und dementsprechend hohe Kosten verursachen. Die Aktivierung entsprechender Schutzmechanismen kann über DNS- oder BGP-Umleitungen erfolgen. Eine günstigere Variante stellt die Blockierung jeglichen Verkehrs zu den betroffenen Systemen, in der Regel bereits vor Eintritt in das angegriffene Netz, dar. Dieser Ansatz wird häufig durch ein BGP-gesteuertes Verfahren, dem sog. Remotely Triggered Black Holing (RTBH), ausgelöst. Hierüber lassen sich zwar Kollateralschäden über größere Netzbereiche hinweg zuverlässig vermeiden, gleichzeitig geht die Blockierung naturgemäß aber mit einem vollständigen Konnektivitätsverlust der direkt angegriffenen Systeme einher. RTBH ist bei vielen ISPs und Internet Exchange Points als (meist kostenfreie) Standarddienstleistung verfügbar, wohingegen Scrubbing-Dienste nur von großen Transit-Providern oder unabhängigen Drittanbietern bezogen werden können. In jedem Fall sollten entsprechende Schutzmaßnahmen bei akuter Gefährdung bereits frühzeitig installiert werden, um die Reaktionsgeschwindigkeit im Angriffsfall zu erhöhen. Vordefinierter Verkehr von bestimmten Quell-Adressen und Ports oder auch basierend auf bekannten Verkehrsmustern kann automatisiert blockiert werden. Auch Umleitungen via BGP – entweder zu einem Scrubbing Center oder für RTBH – sollten zum Zeitpunkt eines Angriffes bereits vorbereitet sein. Um Denial-of-Service Angriffe jedoch langfristig zu verhindern, müssen in erster Linie Schwachstellen in Endgeräten und öffentlich erreichbaren Diensten geschlossen werden. Ziel dieser Maßnahmen sollte es sein, sowohl den Aufbau von Bot-Netzen als auch die Durchführung von Amplification-Angriffen wesentlich zu erschweren.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.8).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.8: (Denial-of-Service) **Statistische Auswertung**

- *Mittlere Dauer*, da Angriffe nur unter großem Ressourcenaufwand aufrecht erhalten werden können und sich, eine geeignete Vorbereitung vorausgesetzt, vergleichsweise schnell durch Blockierung oder Filterung schadhaften Verkehrs mitigieren lassen.
- *Hohe Reichweite*, da fast ausschließlich populäre Dienste angegriffen werden und Kollateraleffekte auch unabhängige Dritte in Mitleidenschaft ziehen können.
- *Hohe Auswirkung*, da mit gezielten hochvoluminösen DoS-Angriffen oft anhaltende Totalausfälle und damit wirtschaftliche Schäden einhergehen. Aktive Mitigationsmaßnahmen von Drittanbietern können zudem hohe Folgekosten nach sich ziehen.
- *Komplexität* hoch, da neben Fachwissen über Dienstschwachstellen und verwundbare Systeme auch große Ressourcen und/oder kriminelle Energie vonnöten sind.
- *Post-Mortem* durchschnittlich, da die Betreiber von Mitigationslösungen in eigenem Interesse meist nur erfolgreiche Maßnahmen nach einem Angriff veröffentlichen.
- *Datenlage* durchschnittlich, da die angegriffenen Netzbereiche in der Regel zwar nicht explizit veröffentlicht werden, bei populären Diensten aber bekannt sind.

Risikobewertung Das Schadenspotential von Denial-of-Service ist im Allgemeinen als hoch zu bewerten. Angriffe erstrecken sich zwar selten über lange Zeiträume, deren Reichweite ist bei Ausfall populärer Dienste jedoch meist hoch. Zusätzlich zu hohen Folgekosten durch Totalausfälle und Mitigation besteht auch kollaterale Gefahr für unbeteiligte Dritte.

Schadenspotential	**Hoch**
Eintrittserwartung	**Hoch**

Kategorie: **Denial-of-Service**

Die Eintrittserwartung von Denial-of-Service wird als hoch eingeschätzt, da sich trotz der hohen Komplexität von Angriffen vielfältige kriminelle und politische Motive finden. Zudem lassen sich fertige Bot-Netze wie auch individuell dimensionierbare DDoS-Angriffe immer öfter im Rahmen von günstigen Dienstleistungsmodellen mit einem Klick bestellen.

Fallbeispiel: Amplification-Angriff auf GitHub.com [I81] Ein massiver Amplification-Angriff mit einem Volumen von 1,3 TBit/s auf die populäre Code-Plattform GitHub wird von Cloudflare mittels einer mehrstufigen Mitigation abgewehrt. Dieser Angriff ist vor allem deshalb interessant, weil er mit einer bis dato unerreichten Bandbreite ausgeführt wurde. Erreicht wurde dieser Techniksprung durch Ausnutzen einer unbekannten Schwachstelle in memcached-Servern, wodurch die Bandbreite des Angriffsverkehrs um den Faktor 50.000 gesteigert werden konnte. Trotz dieses extremen Verkehrsaufkommens zeigt der Vorfall nichtsdestotrotz eine erfolgreiche und schnelle Mitigationsstrategie, die durch den Anbieter auch in großem Detail aufbereitet wurde.

Fallbeispiel: Botnet-Angriff auf Dyn [I84] Ein massiver DDoS-Angriff unter Zuhilfenahme des Mirai-Botnets legt mit einem Volumen von 1,2 TBit/s den populären DNS-Dienstleister Dyn lahm und zieht hohe Kollateralschäden nach sich. Bemerkenswert an diesem Vorfall ist, dass nicht ein einzelner Dienst, sondern stark frequentierte DNS-Infrastruktur angegriffen wurde, wodurch in der Folge zahlreiche populäre Webseiten nicht mehr erreicht werden konnten. Da der Angriff mithilfe von gültigen DNS-Anfragen ausgeführt wurde, war eine effektive Mitigation nur schwer zu realisieren. Der Vorgang wurde vom Betreiber der betroffenen Infrastruktur sehr umfangreich aufgearbeitet.

2.1.2.9 Hacking-Angriff

Der Vorfallskatalog umfasst 10 Vorfälle, die durch Hacking-Angriffe verursacht wurden und im Zeitraum zwischen 2011 und 2019 aufgetreten sind. Die Vorfälle sind äußerst vielfältig und reichen von Systemübernahmen und Lösegelderpressung bis hin zu physischer Sabotage. Empfohlene Detailanalysen sind ein Malware-Angriff auf staatliche und kommerzielle Dienste [I91] sowie ein Cryptomining-Angriff über infizierte ISP-Router [I92].

Kategorie: **Hacking-Angriff**

Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-10-19	Enterprise	Pitney Bowes	Ransomware-Angriff legt britische Online-Plattform des Versanddienstleisters lahm [I89]	3	2	3	3	2	1
2019-07-16	Cloud	iNSYNQ	Ransomware-Angriff verhindert Zugang zum Buchhaltungsdienst des Cloud-Anbieteres [I90]	3	2	3	3	3	2
2018-09-13	Enterprise	Naher Osten	Malware-basierter DNS Redirection-Angriff auf staatliche und kommerzielle Dienste [I91]	3	3	3	3	3	3
2018-08-01	Anwender	MikroTik	Weltweiter Cryptomining-Angriff durch Web-Injection über infizierte ISP-Router [I92]	3	3	3	3	2	3
2017-09-28	Enterprise	OpenSRS	Komplexer DNS-Angriff führt zu massiver Störung von Mail- und DNS-Diensten [I93]	2	2	3	3	1	1
2016-12-26	Backbone	PTCL	Vermutete Sabotage bei Pakistan Telecom führt zu landesweitem Internet-Ausfall [I94]	3	3	3	3	1	1
2016-05-18	ISP	Telstra	Mutwillige Kabelbeschädigung führt zu Internet-Ausfall an Nordküste Australiens [I95]	3	2	3	1	1	1
2016-03-01	ISP	Pa Online	Sabotage durch ehemaligen Administrator führt zu Totalausfall des regionalen ISPs [I96]	3	2	3	2	2	1

2013-07-01	DNS	MYNIC	Sabotage an Name Servern führt zu Umleitung aller Zonen der .my Top-Level-Domain [I97]	3	3	3	3	1	1
2011-02-28	ISP	Vodafone UK	Totalausfall von Internet-Anschlüssen nach Hardware-Diebstahl in Rechenzentrum [I98]	3	3	3	3	1	1

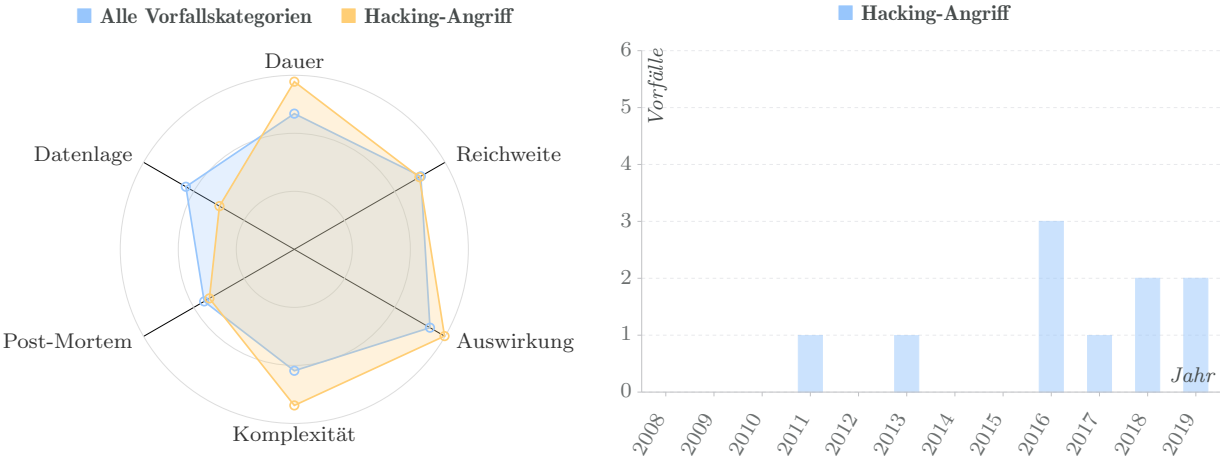
Ursachen Eine häufige Ursache für Ausfälle in dieser Kategorie ist ein Befall von Dienstanbietern durch Ransomware [I89, I90], die Systeme mittels Verschlüsselung vorübergehend unbrauchbar macht und zur Zahlung eines Lösegelds auffordert. Derartige Angriffe erfolgen in der Regel nicht gezielt, sondern nutzen weit verbreitete Sicherheitslücken aus, um möglichst viele Systeme zu befallen. In einem anderen Fall wurde ebenso eine Sicherheitslücke missbraucht, um Schadsoftware an eine große Zahl an Endkunden auszuliefern, hier allerdings mit dem Ziel der (rechenintensiven) Erzeugung von Crypto-Währung [I92]. Auch zielgerichtete Angriffe auf DNS-Infrastrukturen sind zu verzeichnen, die zu Ausfällen [I93] und Umleitungen auf fremde Webseiten [I97] führten, oder als Unterstützung für komplexe Angriffe auf handverlesene Einzelziele [I91] dienten. Neben der Übernahme von Systemen mit Hilfe von Sicherheitslücken ist auch gezielte Sabotage eine mögliche Ursache für Störungen. In einem Fall erzwang ein früherer Mitarbeiter den Totalausfall eines regionalen ISPs [I96], bei landesweiten Störungen in Pakistan wurde ebenfalls Sabotage vermutet [I94]. Neben digitalen Angriffen werden an dieser Stelle auch physische Übergriffe abgehandelt. Diese umfassen unterbrochene Verbindungen durch Vandalismus [I95] sowie Dienstausfälle durch Hardware-Diebstahl aus einem Rechenzentrum [I98].

Betroffene Die Motivation für Hacking-Angriffe unterliegt einem breiten Spektrum, daher wirken sich die identifizierten Vorfälle auf nahezu alle Dienstklassen aus. So wurden Enterprise-Dienste in Mitleidenschaft gezogen [I89, I93] oder auch gezielt angegriffen [I91]. Ebenso häufig betroffen sind ISPs [I95] [I96] [I98], was zur weitflächigen Störung von privaten und gewerblichen Internet-Anschlüssen führen kann. Daneben sind auch Cloud [I90], Anwender [I92], Backbone [I94] und DNS [I97] immer wieder Ziel von Angriffen.

Gegenmaßnahmen Abhängig von der konkreten Gefährdung müssen Sicherheitsmaßnahmen unter Umständen sehr individuell gewählt werden. So können beispielsweise DNS-Basierte Angriffe in vielen Fällen über den durchgehenden Einsatz von DNSSEC verhindert werden. Personenbezogene Angriffsvektoren wie Phishing und Social Engineering lassen sich im Netz durch Zonenkonzepte und auf Systemebene durch Zwei-Faktor-Authentifizierung erschweren und sollten sowohl scheidende Mitarbeiter als auch Besucher und externe Dienstleister berücksichtigen. Um Befall durch Schadsoftware zu vermeiden, müssen Software-Lösungen darüber hinaus stets aktuell gehalten und Sicherheitslücken zeitnah durch verfügbare System-Updates geschlossen werden. In jedem Fall ist auch der Einsatz einer leistungsfähigen Firewall an allen Netzgrenzen sowie eines Netz- oder Host-basierten Intrusion Detection (bzw. Intrusion Prevention) Systems anzuraten.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.9).

- *Hohe Dauer*, da viele Angriffe über längere Zeiträume unentdeckt bleiben und eine Wiederherstellung betroffener Systeme oft mit großen Aufwänden verbunden ist.
- *Hohe Reichweite*, da sowohl zielgerichtet einzelne Dienste oder kritische Infrastrukturen als auch wahllos Endanwender und Firmen in großem Stil angegriffen werden.



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.9: (Hacking-Angriff) **Statistische Auswertung**

- *Hohe Auswirkung*, da Angriffe regelmäßig zu Totalausfällen führen und eine Mitigation, bspw. bei Ransomware, nicht immer möglich ist. In vielen Fällen ergeben sich erhebliche finanzielle Folgeschäden, auch mit einem lang anhaltenden Vertrauensverlust in die betroffenen Anbieter ist bei Bekanntwerden von Vorfällen zu rechnen.
- *Komplexität* hoch, da für viele Angriffe große kriminelle Energie, tiefgehendes wie praxiserprobtes Fach- und Insiderwissen oder fallabhängig auch Zugang zu bisher unveröffentlichten Sicherheitslücken, sog. Zero-Day-Exploits, vonnöten ist.
- *Post-Mortem* durchschnittlich, da vielfältige Schutzmaßnahmen bekannt sind, deren konkreter Einsatz jedoch nur in Einzelfällen in vollem Detail dokumentiert wird. Sorgen um die eigene Reputation hindern eine Aufarbeitung erfolgreicher Angriffe.
- *Datenlage* unterdurchschnittlich, da genaue Hergänge und betroffene Netzbereiche selten kommuniziert werden (können) und von außen nicht nachvollziehbar sind.

Risikobewertung Das Schadenspotential von Hacking-Angriffen ist im Allgemeinen als hoch zu bewerten. Alle betrachten Fälle zeugen von hoher Dauer, Reichweite und Auswirkung. Lediglich bei zielgerichteten Angriffen ist fallabhängig eine verminderte Reichweite möglich. Finanzielle Schäden und Reputationsverlust gehen stets mit Angriffen einher.

Schadenspotential	**Hoch**
Eintrittserwartung	**Hoch**

Kategorie: **Hacking-Angriff**

Die Eintrittserwartung von Hacking-Angriffen wird als hoch eingeschätzt. Trotz der überdurchschnittlich hohen Komplexität sind Angriffe finanziell oft äußerst lukrativ oder anderweitig ohne Limitierung des Ressourcenbedarfs motiviert. Aufgrund der überaus großen Angriffsfläche heutiger Netzwerke und Systeme ist ein flächendeckender Schutz unmöglich, vorbeugende Maßnahmen erlauben meist nur eine Abmilderung von Folgeschäden.

Fallbeispiel: Angriff auf staatliche und kommerzielle Dienste [I91] Unter Zuhilfenahme einer Malware wird ein erfolgreicher DNS Redirection-Angriff auf staatliche und kommerzielle Dienste durchgeführt. Dieser Vorfall ist von besonderem Interesse, da er auf mehreren aufeinander aufbauenden Teilangriffen basiert und hinsichtlich Umfang und Komplexität weit über bisher bekannte Fälle hinausgeht. Der Fall zeigt auch die Wichtigkeit einfacherer Schutzmaßnahmen, wie Zwei-Faktor-Authentifizierung und lückenlosem Einsatz von DNSSEC, die den Angriff bereits im Vorfeld stark abschgeschwächt hätten.

Fallbeispiel: Cryptomining-Angriff über infizierte ISP-Router [I92] Durch einen Angriff auf proprietäre DSL-Router eines Internet-Anbieters gelingt es, Schadcode über Heim-Router an Endkunden auszuliefern. Der Fall ist bemerkenswert, weil mittels Web-Injection spezielle Cryptominer-Software direkt in den Browsern der betroffenen Kunden zur Ausführung gebracht werden sollte, um damit in großem Umfang Crypto-Währung für den Angreifer zu generieren. Die Sicherheitslücke konnte dabei nicht vonseiten des ISPs geschlossen werden, da Endkunden ein manuelles Update anstoßen mussten. Aufgrund eines Implementierungsfehlers des Angreifers entstand kein Schaden.

2.1.2.10 Staatliche Aktion

Der Vorfallskatalog umfasst 9 Vorfälle, die als staatliche Aktionen eingestuft wurden und im Zeitraum zwischen 2011 und 2019 aufgetreten sind. Ein Großteil der Fälle ist durch Zensur und Überwachung motiviert und spielt sich in den Regionen des Nahen Ostens ab. Empfohlene Detailanalysen sind landesweit getrennte Internet-Verbindungen vor Schulprüfungen im Irak [I102] sowie umgeleitete DNS-Anfragen in der Türkei [I104].

Kategorie: **Staatliche Aktion**

Datum	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
2019-04-02	Content	Yandex	Vermutete staatliche Choke-Point-Filterung bei populärer russischer Suchmaschine [I99]	2	2	2	3	1	2
2017-01-05	Content	Blue Content	Iran leitet asiatischen Verkehr zu Erwachsenenseiten durch BGP-Zensurversuch um [I100]	3	1	2	1	1	3
2016-07-15	Backbone	Irak	Irakische Regierung trennt landesweite Internet-Verbindung als Reaktion auf Proteste [I101]	2	3	3	3	1	3
2015-06-27	Backbone	Irak	Irakische Regierung trennt landesweite Internet-Verbindung vor Schulprüfungen [I102]	2	3	3	3	1	3
2014-05-20	Backbone	Neuseeland	Vollständige Verkehrsausleitung am Southern Cross Cable zur Überwachung durch USA [I103]	3	3	3	3	2	1
2014-03-29	DNS	Türkei	Türkische Regierung leitet Anfragen an populäre DNS-Resolver zu eigenen Servern um [I104]	3	3	2	3	1	3
2012-11-29	Backbone	Syrien	USA trennen syrische Internet-Verbindung bei mutmaßlicher Infiltrierung im Bürgerkrieg [I105]	3	3	3	3	2	3
2011-06-03	Backbone	Syrien	Syrische Regierung trennt landesweite Internet-Verbindung als Reaktion auf Aufstände [I106]	3	3	3	3	1	3
2011-01-27	Backbone	Ägypten	Ägyptische Regierung trennt landesweite Internet-Verbindung während Protesten [I107]	3	3	3	3	3	3

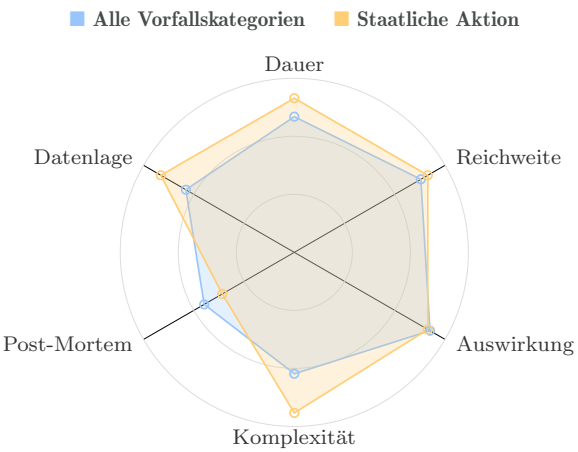
Ursachen Die untersuchten Vorfälle sind sowohl aus technischer als auch politischer Sicht sehr vielfältig. Dennoch ist den meisten Fällen ein Bestreben nach Ausübung staatlicher Kontrolle gemein. Oft spielt Zensur [I99, I100, I101, I104, I106, I107] eine tragende Rolle, teils um staatskritische Informationen zu unterdrücken, aber auch um die Kommunikation zwischen erklärten Staatsfeinden – meist als Reaktion auf Proteste oder Aufstände – kurzfristig zu unterbinden. Ebenso erwähnenswert sind wiederholte landesweite Abschaltungen des Internets im Irak [I102], um Betrugsversuche während der Schulprüfungen (ungeachtet der hohen wirtschaftlichen Folgekosten) zu erschweren. Schließlich kommen auch nachrichtendienstliche oder militärische Operationen fremder Staaten zum Tragen. So wurde durch Enthüllungen bekannt, dass die USA mit der neuseeländischen Regierung kooperieren, um dort anlandende Seekabel flächendeckend zu überwachen [I103]. Auch ein landesweiter Internet-Ausfall in Syrien wird mutmaßlich den USA zugeschrieben.

Betroffene Durch die in der Regel landesweiten Eingriffe in Kommunikationsflüsse ist vor allem der Internet-Backbone [I101, I102, I103, I105, I106, I107] von Vorfällen betroffen. Nur dort lassen sich flächendeckende Überwachung, Zensur und Abschaltungen realisieren. Allerdings ist zu beachten, dass insbesondere in autoritär geführten Staaten die landesweite Internet-Infrastruktur oft nur von einzelnen, meist staatlich kontrollierten ISPs betrieben wird. Ungeachtet dessen wurden in Einzelfällen auch zielgerichtete Aktionen gegen DNS [I104] oder Content [I99, I100] Dienstanbieter bekannt.

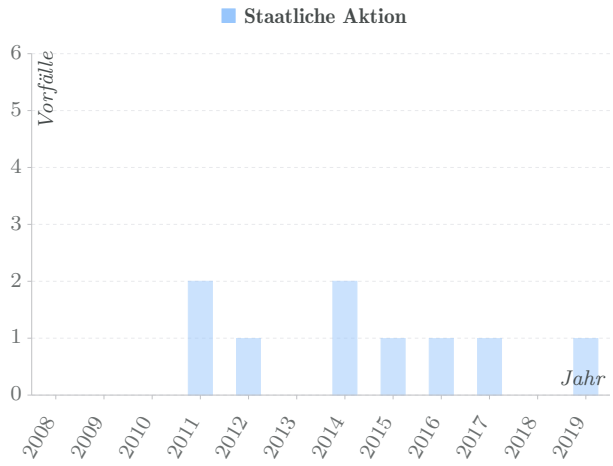
Gegenmaßnahmen Aus technischer Sicht werden staatliche Aktionen meist landesintern angeordnet, d.h. nationale ISPs zur Umsetzung der Maßnahmen verpflichtet [I99, I101, I106, I107]. Ist dies in Einzelfällen nicht möglich oder ausreichend, kommen auch BGP-Hijacking Angriffe [I100, I104] zur Manipulation des weltweiten Internet-Routings (siehe Abschnitt 2.1.2.7) zum Einsatz. Fallabhängig können einzelne Gegenmaßnahmen betroffener Endanwender zu einer erfolgreichen Umgehung staatlicher Aktionen führen. So lässt sich DNS-basierte Zensur einzelner Dienste von deren Nutzern durch Einsatz alternativer DNS-Resolver umgehen. Zensur und Überwachung kann auch durch Aufbau eines Virtual Private Networks (VPN) umgangen werden, jedoch sind gerade solche Dienste oft Ziel staatlicher Aktionen. Zensur per BGP-Hijacking kann von *unabhängigen* ISPs durch Einsatz der Resource Public Key Infrastructure (RPKI) erkannt und verhindert werden. Bei landesweiten Infrastruktur-Abschaltungen besteht für den überwiegenden Teil betroffener Bürger dagegen kaum Handlungsspielraum. Mögliche Gegenmaßnahmen beschränken sich auf die Verwendung alternativer Internet-Anbindungen, bspw. über Satellit oder über ISPs in Nachbarländern. Eingriffe durch fremde Staaten können generell nur durch politische Prozesse oder eine geeignete internationale Gesetzgebung verhindert werden.

Statistische Auswertung Die nachfolgenden Diagramme geben einen Überblick über charakteristische Eigenschaften der betrachteten Internet-Vorfälle (Abb. 2.10).

- *Hohe Dauer*, da keine behebbaren technischen Probleme oder mitigierbare Angriffe vorliegen. Insbesondere Zensur und Überwachung sind meist langfristig ausgelegt.
- *Hohe Reichweite*, da meist ganze Regionen oder Länder und deren Bürger in den Fokus von staatlichen Aktionen geraten. Auch Effekte auf Drittstaaten sind möglich.
- *Hohe Auswirkung*, da staatliche Eingriffe kaum abgeschwächt und selten umgangen werden können. Zum Teil werden auch wirtschaftliche Schäden in Kauf genommen.
- *Komplexität* hoch, da tiefgreifende Eingriffe in nationale Internet-Infrastruktur nur von wenigen Akteuren realisierbar sind und ein politischer Rahmen dafür nötig ist.



(a) Korrelation



(b) Zeitverlauf

Abbildung 2.10: (Staatliche Aktion) **Statistische Auswertung**

- *Post-Mortem* unterdurchschnittlich, da Eingriffe meist nicht in vollem Umfang bekannt sind und unabhängige Berichte oft mit politischen Gefahren verbunden sind.
- *Datenlage* überdurchschnittlich, da die betroffenen, in der Regel landesweiten Netzbereiche generell bekannt sind und sich Abschottungen von außen beobachten lassen.

Risikobewertung Das Schadenspotential staatlicher Aktionen ist im Allgemeinen als hoch zu bewerten. In betroffenen Ländern ist sowohl mit dauerhafter Blockierung kontroverser Dienste als auch mit spontanen landesweiten Internet-Abschaltungen zu rechnen. Wirtschaftliche Folgeschäden im Land und bei Dritten werden in Kauf genommen.

Schadenspotential	**Hoch**
Eintrittserwartung	**Hoch**

Kategorie: **Staatliche Aktion**

Die Eintrittserwartung staatlicher Aktionen wird als hoch eingeschätzt. Zwar ist Zensur überwiegend in autoritär geführten Staaten zu erwarten. Brüche der Netzneutralität und Kommunikationsüberwachung durch Drittstaaten werden jedoch zur weltweiten Praxis.

Fallbeispiel: Landesweite Internet-Trennung vor Prüfungen [I102] Im Irak werden vor Schulprüfungen regelmäßig landesweite Internet-Verbindungen getrennt, um Betrugsversuche zu unterbinden. Dies ist bemerkenswert, da massiven staatlichen Eingriffen mit hohen wirtschaftlichen Schäden ein geringer praktischer Nutzen gegenübersteht.

Fallbeispiel: Umgeleitete DNS-Anfragen in der Türkei [I104] Die türkische Regierung manipuliert Anfragen an populäre DNS-Resolver, um eine Umgehung der landesinternen Zensur westlicher Social-Media-Dienste zu erschweren. Besonders interessant ist die effektive technische Umsetzung basierend auf BGP-Hijacking, wodurch jeglicher Verkehr türkischer Bürger zu den Netzbereichen der betroffenen DNS-Anbieter an staatseigene zensierende DNS-Resolver umgeleitet wird.

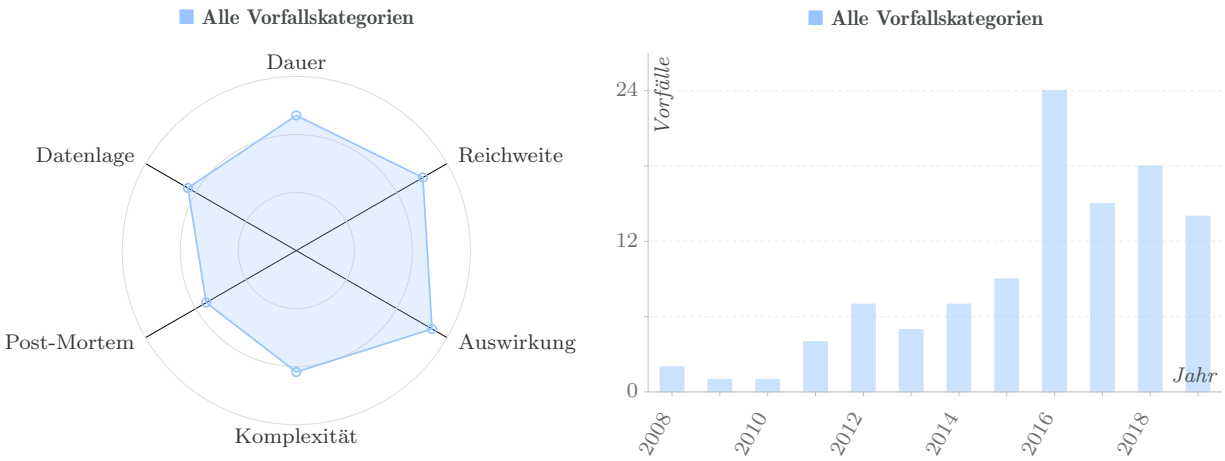
2.1.3 Gegenüberstellung und Bewertung

Mit Abschluss des Vorfallskatalogs steht eine umfassende Datenbasis zur Diskussion von Schutzdefiziten der Internet-Infrastruktur zur Verfügung. Im Folgenden werden Vorfälle aller Kategorien gegenübergestellt und daraus konkrete Gefahrenpotentiale abgeleitet. Daran anschließend können existierende Schutz- und Gegenmaßnahmen bewertet und Handlungsmöglichkeiten aufgezeigt werden.

Statistischer Überblick

Der Vorfallskatalog umfasst insgesamt 107 Vorfälle im Zeitraum zwischen 2008 und 2019. Deren zeitliche Verteilung zeigt einen eindeutigen Trend hin zu mehr Vorfällen pro Jahr (Abb. 2.11). Dabei könnte allerdings auch eine zunehmende Berichterstattung über Vorfälle im digitalen Raum eine Rolle spielen, da Ausfälle durch die fortschreitende Digitalisierung immer größere Auswirkungen auf alle Lebensbereiche nach sich ziehen und daher mehr mediale Aufmerksamkeit generieren. Zusätzlich entstehen durch die zunehmende Digitalisierung auch immer größere Angriffsflächen und mehr potentielle Gefahrenquellen.

Betrachtet man die durchschnittlichen Ergebnisse der erarbeiteten Bewertungskriterien über alle Vorfälle hinweg (Abb. 2.11), so zeigt sich, dass die Kriterien Dauer ($\varnothing$ 2,3), Reichweite ($\varnothing$ 2,5) und Auswirkungen ($\varnothing$ 2,7) bei den betrachteten Fällen am höchsten eingestuft wurden. Im Gegensatz zu den verbleibenden Kriterien tragen diese unmittelbar zu einem insgesamt hohen Schadenspotential der untersuchten Internet-Vorfälle bei.



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.11: (Alle Fälle) **Statistische Auswertung**

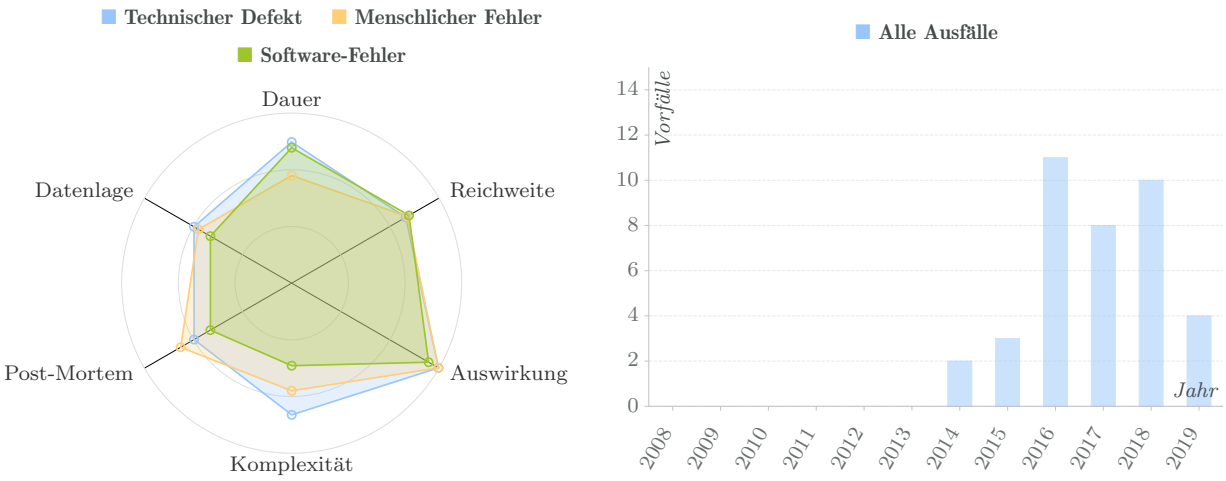
Obige Verteilung zeigt aber auch, dass Post-Mortem-Analysen ($\varnothing$ 1,8) trotz akzeptabler Datenlage ($\varnothing$ 2.2) selten zufriedenstellen, da genaue Vorfallshergänge von den Betroffenen häufig nicht aufbereitet bzw. veröffentlicht werden. Vor allem im Hinblick auf indikativ steigende Fallzahlen mit hohem Schadenspotential besteht hier eine Handlungslücke. Unter Berücksichtigung verfügbarer Gegen- und Schutzmaßnahmen sowie fallspezifischer Komplexität ($\varnothing$ 2.1) sollte diesen Gefahrenquellen mittelfristig begegnet werden. Als Grundlage dafür wird im Folgenden eine differenzierte Risikobewertung durchgeführt.

Abschließende Risikobewertung

Über alle Vorfallskategorien hinweg zeigt sich der Internet-Backbone in 34.6% aller Fälle am häufigsten von Störungen betroffen. Mit größerem Abstand folgen die Dienstklassen Content (15.9%), DNS (13.1%), ISP (13.1%) und Cloud (11.2%). Deutlich seltener von Vorfällen betroffen sind Enterprise und Anwender mit 8.4% bzw. 3.7%. Aber auch wenn Endkunden selbst nicht unmittelbar mit einem Vorfall in Verbindung stehen, so sind sie nichtsdestotrotz oft indirekt Leidtragende, insbesondere bei Vorfällen im Internet-Backbone. Dessen Überrepräsentation lässt sich mit einer Vielzahl von infrastrukturellen Gefahrenquellen – sowohl technischer, administrativer als auch politischer Natur – erklären. Gleichzeitig führen Internet-weite Störungen allerdings auch zu umfassender Berichterstattung und damit generell höherer Sichtbarkeit von Vorfällen. Insbesondere bei gezielten Angriffen ist von einer hohen Dunkelziffer auszugehen. Im Folgenden wird eine zusammenfassende Risikobewertung für die drei Vorfallsgruppen Ausfälle, Umleitungen und Angriffe (siehe Abschnitt 2.1.1) vorgenommen. Dabei werden auch auffällige Abweichungen von den bisherigen fallübergreifenden Bewertungsergebnissen diskutiert sowie Schadenspotential und Eintrittserwartung je Vorfallsgruppe abschließend eingeschätzt. *Hinweis:* um der Diversität einzelner Vorfallskategorien besser gerecht zu werden, werden hierzu Mittelwerte aus den Ergebnissen der finalen Risikobewertung je Kategorie gebildet.

Anzahl Vorfälle	**38**
Schadenspotential	**Mittel**
Eintrittserwartung	**Hoch**

Ausfälle Zu dieser Vorfallsgruppe zählen die Kategorien technische Defekte, menschliche Fehler sowie Software-Fehler. Die mittlere Dauer ($\varnothing$ 2, 3) der betrachteten Vorfälle gleicht hier dem Gesamtdurchschnitt, auch wenn sich Ausfälle aufgrund menschlichen Versagens meist in etwas kürzerer Zeit beheben lassen. Auffällig sind neben der geringeren Reichweite ($\varnothing$ 2, 4) jedoch deutlich höhere Auswirkungen ($\varnothing$ 2, 9). Interessanterweise steigt die Qualität von Post-Mortem-Analysen ($\varnothing$ 2, 0) bei gleichzeitiger schlechterer Datenlage ($\varnothing$ 1, 8). Zudem reduziert sich der Anteil an Ausfällen im Internet-Backbone auf 21,1%. In vergleichbarem Maße nehmen die Fälle für Cloud (21,1%) und ISP (18.4%) Dienste zu. Die zeitliche Entwicklung dieser Vorfallsgruppe lässt einen deutlichen Trend hin zu mehr Ausfällen pro Jahr erkennen (Abb. 2.12).

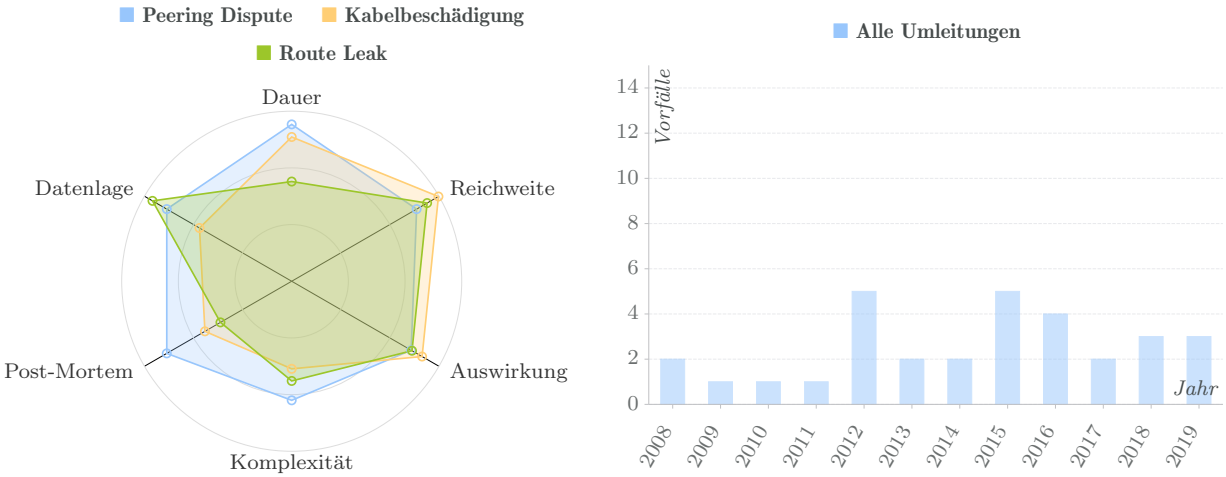


(a) Korrelation (b) Zeitverlauf

Abbildung 2.12: (Ausfälle) **Statistische Auswertung**

Anzahl Vorfälle	**31**
Schadenspotential	**Hoch**
Eintrittserwartung	**Mittel**

Umleitungen Diese Vorfallsgruppe fasst Internet-weite Verkehrsumleitungen aufgrund von Kabelbeschädigungen, Peering Disputes und Route Leaks zusammen. Dementsprechend weisen die betrachteten Vorfälle auch eine deutlich höhere Reichweite (⌀ 2, 8) gegenüber dem Gesamtdurchschnitt auf. Nicht immer führen Umleitungen jedoch zu gravierenden Störungen, was sich naturgemäß an geringeren Auswirkungen (⌀ 2, 5) zeigt. Hinsichtlich der Vorfallsdauer (⌀ 2, 3) und Post-Mortem-Qualität (⌀ 1, 8) sind keine nennenswerten Abweichungen vom Mittelwert festzustellen, auch wenn bei Route Leaks nur mit kürzeren Störungen zu rechnen ist. Datenlage (⌀ 2, 5) und Komplexität (⌀ 1, 8) der Vorfälle schlagen dagegen deutlich nach oben bzw. unten aus. Erwartungsgemäß spielen sich Umleitungen zum überwiegenden Teil im Internet-Backbone (67.7%) ab, in selteneren Fällen können auch nur einzelne Content (19.4%) und ISP (12.9%) Dienste betroffen sein. Zeitliche Trends oder Häufungen lassen sich für diese Vorfallsgruppe im betrachteten Zeitraum nicht feststellen (Abb. 2.13).

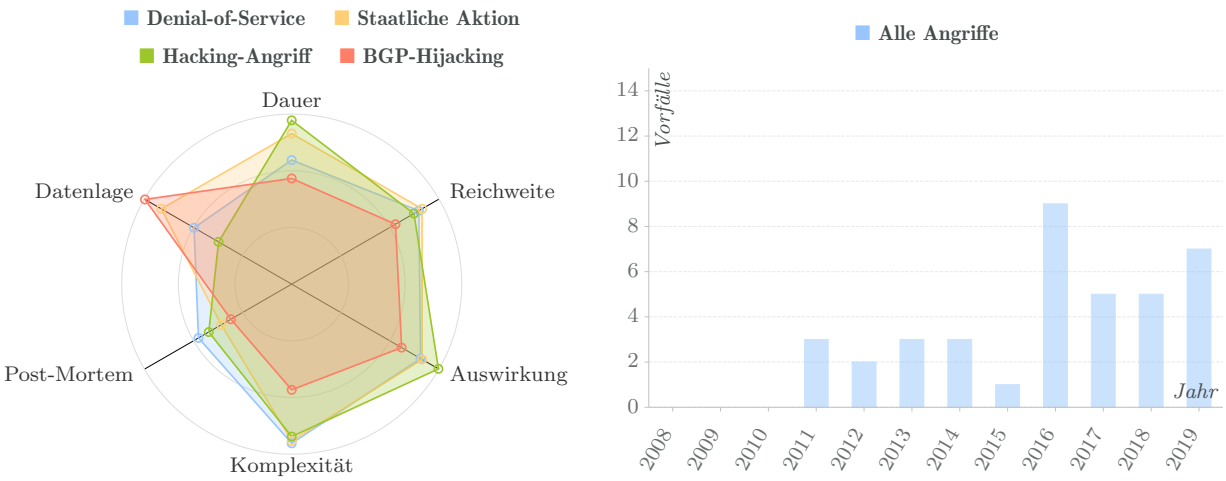


(a) Korrelation (b) Zeitverlauf

Abbildung 2.13: (Umleitungen) **Statistische Auswertung**

Anzahl Vorfälle	**38**
Schadenspotential	**Hoch**
Eintrittserwartung	**Hoch**

Angriffe Zu dieser Gruppe von Vorfällen zählen BGP-Hijacking, Denial-of-Service, Hacking-Angriffe und staatliche Aktionen. Auch wenn bei diesen meist gezielten Übergriffen im Mittel keine höheren Auswirkungen (⌀ 2, 7) zu erwarten sind, entsteht vor allem durch Hacking-Angriffe überproportional hoher Schaden. Hinsichtlich der Reichweite (⌀ 2, 4), Dauer (⌀ 2, 4) und Datenlage (⌀ 2, 2) sind keine nennenswerten Abweichungen festzustellen, wenngleich aber größere Unterschiede in den einzelnen Vorfallskategorieren zu verzeichnen sind. Die Verfügbarkeit von Post-Mortem-Analysen (⌀ 1, 6) liegt deutlich unter dem Durchschnitt. Trotz der signifikanten Komplexität (⌀ 2, 6) der betrachteten Vorfälle wird deren Eintrittserwartung hoch eingestuft. Dies gilt insbesondere auch im Hinblick auf neue *Attack-as-a-Service*-Geschäftsmodelle und die im Betrachtungszeitraum in analoger Weise zunehmende Zahl an Vorfällen (Abb. 2.14).



(a) Korrelation

(b) Zeitverlauf

Abbildung 2.14: (Angriffe) **Statistische Auswertung**

Schutz- und Gegenmaßnahmen

Basierend auf den bisherigen Erkenntnissen zu realen Internet-Vorfällen lässt sich der allgemeiner Zustand verfügbarer Schutz- und Gegenmaßnahmen bewerten. Hierfür wird im Folgenden zunächst ein Überblick über die einzelnen Vorfallskategorien und daraus resultierenden Schutzdefizite gegeben. Abschließend können konkrete Maßnahmen und weiterführende Denkanstöße zur zukünftigen Entwicklung des Internets formuliert werden.

Hoher Schutz Die folgenden Vorfallskategorien lassen sich tendenziell gut gegen Vorfälle schützen oder können durch Gegenmaßnahmen effektiv mitigiert werden.

- *Menschlicher Fehler* Meist werden Fehler ereits durch den Verursacher selbst bemerkt und zeitnah behoben. Präventivmaßnahmen sind mittels einschlägiger Wartungs, Rollout- und Backup-Konzepten in nahezu beliebigem Umfang möglich und werden in vielen Fällen zumindest rudimentär auch eingesetzt.
- *Peering Dispute* Zwar lassen sich wirtschaftliche Differenzen kaum zuverlässig verhindern, dennoch können sich Netzbetreiber durch unabhängige Anbindungen über mehrere ISPs effektiv gegen Leistungseinbrüche und Netzfragmentierung schützen. Abhängigkeiten von Content-Anbietern zu Drittnetzen nehmen zudem stetig ab.
- *Denial-of-Service* Zahlreiche Filtertechniken ermöglichen eine effektive Mitigation von DoS-Angriffen. Lediglich sehr voluminöse oder komplexe Angriffe führen zu Ausfällen. Da eine Filterung stark frequentierter Dienste jedoch nur durch spezialisierte Dienstleister realisiert werden kann, ist zuverlässiger Schutz sehr kostenintensiv.

Eingeschränkter Schutz Für folgende Vorfallskategorien sind Schutz- und Gegenmaßnahmen nur eingeschränkt verfügbar oder finden keine ausreichende Verbreitung.

- *Technischer Defekt* Viele Gefahrenquellen können über Frühwarn- und Hot-Standby-Systeme sowie durch Brandschutz und Notstrom neutralisiert werden. Restrisiken bleiben durch die zufällige Natur von Ausfällen und Komplexität großer Systeme.
- *Route Leak* Zahlreiche Best Practices zur Vermeidung von Routing-Fehlern sind bekannt, mit RPKI ist ein zuverlässiger Schutzmechanismus vorhanden. Die größte

Herausforderung liegt im fehlenden Einsatz in der Fläche, so dass Route Leaks in entlegenen Teilen der Welt nach wie vor globale Störungen nach sich ziehen können.
- *Hacking-Angriff* Bereits einfachste Präventivmaßnahmen, wie regelmäßige Software-Updates und die Errichtung von Firewalls und Netzzonen, können einen Großteil der heutigen Angriffen abwehren. Gleichzeitig ist ein effektiver Schutz gegen zielgerichtete Angriffe unter Einbezug von Zero-Day-Exploits kaum zu bewerkstelligen.

Unzureichender Schutz Internet-Vorfälle in den verbleibenden Kategorien lassen sich in der Regel nur schwer verhindern oder sind aufwändig in der Beseitigung.

- *Software-Fehler* Die hohe Komplexität heutiger Software führt zu mannigfaltigen und meist nicht vorhersehbaren Fehlerquellen. Viele Systeme, vor allem eingebettete, verfügen über keinen automatisierten Update-Mechanismus. Schutzmaßnahmen müssten bereits in Herstellungsprozesse integriert werden. Jedoch stehen immer kürzer werdende Entwicklungszyklen einer zureichenden Qualitätssicherung entgegen.
- *Kabelbeschädigung* Eine Reparatur von See- und Landkabeln ist generell sehr zeit- und kostenintensiv. Flächendeckender Schutz ist aufgrund der großen Kabelstrecken und vielfältigen Schadensursachen jedoch nicht praktikabel und muss sich auf besonders gefährdete Abschnitte, d.h. auf Küsten und Metropolen, beschränken.
- *BGP-Hijacking* Eine gezielte Manipulation des globalen Internet-Routings, und damit nahezu beliebige Umleitungen internationaler Verkehrsströme, lassen sich im heutigen Stand der Technik nicht unterbinden. Der flächendeckende Schutz durch das in der Theorie geeignete BGPsec ist auch in weiterer Zukunft nicht abzusehen.
- *Staatliche Aktion* Politisch motivierte Aktionen lassen sich allenfalls durch persönliche Maßnahmen umgehen, da Regierungen meist über weitreichende Machtbefugnisse und Ressourcen verfügen. Gesetzgebung und Außenpolitik sind ausschlaggebend.

Verbesserungspotential Zahlreichen bestehenden Gefahrenquellen und Schutzdefiziten ließe sich durch eine weitere Verbreitung gängiger Präventivmaßnahmen effektiv begegnen.

Einhaltung von Best Practices und Standards
- Durchführung schnellerer und umfassenderer Software- und System-Aktualisierungen
- Präventivschutz populärer Dienste durch Einbindung von Mitigationsdienstleistern
- Routing-Sicherheit durch RPKI sowie Pflege von Routing Registries und Filter
- Aufbau einer redundanten Internet-Anbindung zum Schutz vor Peering-Änderungen
- Regelmäßige Software-Audits, automatisierte Tests und stufenweise Ausrollung

Verbesserung von materiellem und personellem Schutz
- Konsequenter Schutz gegen Umwelteinflüsse wie Brände und Stromausfälle
- Besserer Schutz von Anlandungspunkten internationaler Kabelverbindungen
- Vorhaltung alternativer Langstreckenverbindungen, bspw. Satelliten/Starlink
- Schulungen von Mitarbeitern und Kunden zu Social Engineering und Phishing
- Aufbau von Emergency Response Teams, Ernennung von Sicherheitsbeauftragten

Stärkung der Gesetzgebung und Regulierung
- Hilfe zum Selbstschutz vor Einfluss und Überwachung fremder Staaten
- Aktive Förderung einer weiten Verbreitung von Ende-zu-Ende-Verschlüsselung
- Pflicht für Netz- und Dienstbetreiber zu Backups, Dokumentation und Forensik
- Regulierung der Netzneutralität zum Schutz vor wirtschaftlich motivierter Störung
- Ausbau des Kartellrechts zur Beschränkung monopolartiger Marktmacht

Handlungsmöglichkeiten und Ausblick

Basierend auf den gesammelten Vorfällen und der vorangehenden quantitativen Risikobewertung wird im Folgenden die Gefährdungslage für Deutschland diskutiert. Zwar unterliegt die Zusammenstellung der Vorfälle im Katalog einer gewissen Verzerrung durch Überpräsenz schwerwiegenderer Fälle in den Medien, dennoch können Defizite identifiziert und Empfehlungen zu Handlungsmöglichkeiten abgegeben werden.

Ein größerer Teil der betrachteten Vorfälle lässt sich entweder direkt oder indirekt auf die deutsche Internet-Landschaft übertragen. Äußere Einflüsse wie Stromausfälle, Brände und Naturkatastrophen sind unmittelbar für Einrichtungen wie Internet Exchange Points und große Rechenzentren relevant. Dies wird auch am Fallbeispiel Interxion [I5] klar, in dem weitreichende Störungen für deutsche Internet-Nutzer durch Ausfall eines wichtigen Rechenzentrums in Frankfurt zu Tage traten. Der weltweite Ausfall des CDN-Betreibers Cloudflare [I13] betraf zahlreiche deutsche Webseiten und zeigt eindringlich die Nachteile einer Abhängigkeit von ausländischen Anbietern auf. Ausfälle vernetzter IoT-Geräte [I26] und Software-Störungen bei Fahrzeugen [I35] können Endanwender auch hierzulande unmittelbar beeinträchtigen. Sowohl gezielte Angriffe [I91] als auch Befall durch Schadsoftware [I90] sind eine reale Gefahr für deutsche Firmen. Zudem begünstigen Unzulänglichkeiten in der globalen Routing-Infrastruktur unerwünschte Umleitungen und Ausfälle für deutsche Netze und essentielle internationale Dienste gleichermaßen. Zuletzt zeigt der Fall eines staatlichen Eingriffs in neuseeländische Kabelverbindungen [I103], dass selbst unter Verbündeten Bürger einer steten Gefahr durch Überwachung ausgesetzt sind.

Einige der aufgedeckten Defizite wie Kabelanfälligkeit, Routing-Probleme und unerwünschte staatliche Aktionen lassen sich nur durch großen Investitions- und Forschungsaufwand sowie durch politische Prozesse abmildern. Nichtsdestotrotz gibt es zahlreiche weitere Handlungsmöglichkeiten, um die Sicherheit der deutschen Internet-Landschaft zu verbessern. So können konkrete Auflagen zum Schutz kritischer Einrichtungen sowie verpflichtende Wartungen und Tests von Schutzsystemen Ausfälle in der Infrastruktur verhindern. Schulungen von Mitarbeitern und Kunden zum Thema digitale Sicherheit erschweren gezielte Angriffe durch Social Engineering und Phishing. Weitere Vorschriften zur Aktualisierung und Absicherung von Systemen sind sowohl gegen automatisierbare Angriffe, wie bspw. Ransomware, als auch gegen gezielte Angriffe nötig. Durch den verstärkten Einsatz von Mitigationsdienstleistern kann die Erreichbarkeit von wichtigen Diensten gewährleistet werden. Nicht zuletzt hier ist auch die Förderung deutscher Anbieter erstrebenswert, um Abhängigkeiten von ausländischen Diensten zu verringern. Endanwender sollten durch höhere Anforderungen an vernetzte Produkte geschützt werden, indem Sicherheit langfristig zu gewährleisten ist. Schließlich sind weiterhin kontinuierliche Bemühungen nötig, um Monopolstellungen zu unterbinden und die Netzneutralität sicherzustellen.

Abschließend lässt sich festhalten, dass für nahezu alle Bereiche des deutschen Internets Bedrohungspotentiale nachweisbar sind. Diese Situation könnte durch einen konsequenten Ausbau von Schutz- und Gegenmaßnahmen durchaus abgemildert werden, erfordert aber ein hohes Maß an Aufklärung, Schulung und finanzieller Investition. In Anbetracht der fortschreitenden Digitalisierung nimmt der Handlungsbedarf jedoch stetig und mit wachsender Geschwindigkeit zu, so dass zumindest über die Sicherstellung eines minimalen, aber flächendeckenden Basisschutzes für Deutschland nachgedacht werden sollte.

2.2 Detailanalysen

Im vorangehend erarbeiteten Vorfallskatalog wurden quantitative Erkenntnisse über verschiedenartige Ausfallrisiken im Internet Backbone gewonnen. Für eine qualitative Erörterung von technischen und administrativen Schutzdefiziten und den damit einhergehenden Verbesserungspotentialen ist darüber hinaus auch eine detaillierte Einzelfallbetrachtung zweckmäßig. Die nachfolgend beschriebenen Internet-Vorfälle wurden für entsprechende Detailanalysen ausgewählt.

Großflächiger Stromausfall in Südamerika Im Juni 2019 führt die Beschädigung einer regionalen Hochspannungsleitung bei Bauarbeiten in der Nähe von Buenos Aires zu einem landesweiten Stromausfall in Argentinien und weiteren Störungen in benachbarten Ländern. Unter anderem werden 23% aller argentinischen Netzbetreiber für mehrere Stunden vollständig vom Internet getrennt.

Brand in Kabelschacht bei Korea Telecom Im November 2018 werden in Seoul zahlreiche Netzwerkkabel der Korea Telecom durch einen Brand in einem Kabelschacht zerstört. Dies führt zu einem städteweiten Ausfall von Mobilfunk, Festnetz und Internet. Konsequenzen für das globale Internet-Routing ergeben sich über den regional begrenzten Netzausfall hinaus nicht.

Schweizer Route Leak über China Telecom Im Juni 2019 werden durch ein Route Leak eines Schweizer Cloud-Anbieters BGP-Routen von mehr als 300 Internet Service Providern über China Telecom umgeleitet. Dies führt zu verschiedenartigen Beeinträchtigungen weltweiter Internet-Dienste. Der etwa 40-minütige Vorfall wiederholt sich wenige Stunden später mit leicht höherer Intensität.

Cloudflare-Ausfall durch Fehlkonfiguration Im Juli 2019 führt eine Fehlkonfiguration an der zentralen Web Application Firewall von Cloudflare zu einem weltweiten Totalausfall des Content Delivery Networks. Ebenfalls betroffen sind interne Cloudflare-Systeme, wodurch sich die Behebung des Fehlers verzögert. Zahlreiche populäre Webseiten sind weltweit für über eine Stunde nicht mehr erreichbar.

Peering-Streit zwischen Netflix und Verizon Im Jahr 2014 führt ein Verkehrsungleichgewicht zwischen Netflix und Verizon zu einer Qualitätsminderung des Streaming-Dienstes für Verizon-Kunden. Netflix ist nicht bereit, für die Übergabe des Verkehrs, wie von Verizon gefordert, zu bezahlen und leitet diesen über das Netz von Level3 um. Verizon nimmt die resultierende Überlastung der eigenen Peering-Verbindung mit Level3 billigend in Kauf. Der öffentlich ausgetragene Streit wird erst nach mehreren Monaten beigelegt.

Im Folgenden werden für die ausgewählten Fallbeispiele öffentlich zugängliche Informationen zusammengeführt und durch eigene datengestützte Routing-Analysen vertieft. Neben einer detaillierten Rekonstruktion der jeweiligen Vorfallshergänge lassen sich über dieses Vorgehen auch explizite Auswirkungen im Internet Backbone sowie geeignete Schutz- und Gegenmaßnahmen diskutieren.

2.2.1 Methodisches Vorgehen

Für die Durchführung der Fallstudien wird ein einheitliches Vorgehensmuster festgelegt, um stets nachvollziehbare und vergleichbare Ergebnisse zu ermöglichen. In einem ersten Schritt werden hierbei alle verfügbaren Informationen zusammengetragen und im Rahmen einer Vorfallsübersicht gebündelt. Dies schließt auch Vergleiche mit verwandten Vorfällen sowie eine Aufarbeitung vorhandener wissenschaftlicher Arbeiten mit ein. Zur Vertiefung der gewonnenen Erkenntnisse werden Routing-Daten des Border Gateway Protocols ausgewertet, um Aussagen über die globale Erreichbarkeit von betroffenen Netzbereichen treffen zu können. Mit Hilfe einer Analyse von IP-basierten Messungen werden schließlich konkrete Auswirkungen auf Netzdienste untersucht. Anhand der gewonnenen Erkenntnisse erfolgt eine abschließende Bewertung der Vorfälle mitsamt einer Diskussion möglicher Folgen. Die für die beschriebenen Arbeitsschritte zugrundeliegende Methodik wird im Folgenden näher erörtert.

Übersicht und Einordnung

Mit Hilfe einer manuellen Recherche in öffentlich zugänglichen Quellen (wie Suchmaschinen, Blog-Posts, Mailing-Listen etc.) erfolgt zunächst eine Bestandsaufnahme für die betrachteten Internet-Vorfälle. Im Zuge der Identifikation von betroffenen bzw. beteiligten Netzbereichen wird zudem auch eine erste Sichtung von Routing-Daten vorgenommen, um Vorfallshergänge möglichst vollständig und präzise zu rekonstruieren. Darüber hinaus werden auch Vergleiche zu ähnlich gelagerten Ereignissen des erarbeiteten Vorfallskatalogs gezogen und relevante wissenschaftliche Veröffentlichungen zum Vorfall kurz zusammengefasst. Dieses Vorgehen liefert die nachfolgend beschriebenen Ergebnisse.

Vorfallshergang Über eine Online-Recherche wird zunächst der grobe Zeitrahmen eines Internet-Vorfalls – stets in UTC-Weltzeit – abgesteckt. Bekannte Meilensteine wie bspw. der Zeitpunkt getroffener Gegenmaßnahmen werden ebenfalls mit aufgenommen. Zudem erfolgt eine Identifikation von Verursacher, betroffenen Netzbereiche sowie weiteren beteiligten Parteien. Soweit möglich werden diese auf konkrete Internet-Ressourcen, d.h. entsprechende IP-Netzbereiche oder Autonome Systeme, abgebildet. Mit Hilfe dieser Informationen erfolgt ein erster Abgleich mit Routing-Auffälligkeiten zur zeitlichen Konkretisierung des Vorfallshergangs. Ferner werden anhand von Pressemeldungen oder öffentliche Stellungnahmen auch mögliche Ursachen, zusätzlich eingeleitete Maßnahmen sowie mittel- und langfristige Folgen des Vorfalls untersucht.

Direkte Folgen Aus der öffentlichen Berichterstattung werden direkte Folgen des Internet-Vorfalls zusammengetragen. Dies umfasst sowohl unmittelbare Auswirkungen auf Verursacher und Betroffene des Vorfalls als auch Ankündigungen von mittel- und längerfristigen Konsequenzen vonseiten der Betreiber und zuständigen Behörden.

Verwandte Vorfälle Für eine weitere Einordnung der betrachteten Internet-Vorfälle werden die Bewertungskriterien des Vorfallskatalogs herangezogen. Durch Abgleich von Dauer, Reichweite und Auswirkung mit den Durchschnittswerten der jeweiligen Vorfallskategorie lässt sich die Tragweite der analysierten Vorfälle einordnen. Im Rahmen einer Gegenüberstellung mit vergleichbaren Vorfällen werden Gemeinsamkeiten und Unterschiede hinsichtlich der Vorfallshergänge und direkten Folgen diskutiert.

Wissenschaftliche Arbeiten Im Rahmen einer Literatur-Recherche werden wissenschaftliche Veröffentlichungen im Umfeld der betrachteten Internet-Vorfälle identifiziert. Für die darin beschriebenen Erkenntnisse wird eine Kurzzusammenfassung erstellt. Der Fokus dieser Recherche liegt insbesondere auf einer Darstellung möglicher Schutz-, Erkennungs- und Gegenmaßnahmen. Etwaige neue Erkenntnisse über einzelne Vorfälle fließen in die Rekonstruktion der Vorfallshergänge und Folgen mit ein.

Analyse der Control Plane

Für eine vorfallsbezogene Auswertung von Änderungen in der Routing-Topologie, der sog. Control Plane, kann auf eigene Router zurückgegriffen werden. Diese unterhalten über das Border Gateway Protocol (BGP) zahlreiche Verbindungen zu global agierenden Internet Service Providern (Tier1-ISP) sowie zu bedeutsamen Internet Exchange Points (IXP). Für eine zielgerichtete Analyse von Auswirkungen einzelner Vorfälle auf das deutsche Internet sind hier insbesondere Verbindungen zur Deutschen Telekom (DTAG) und zum weltweit größten Internet Exchange Point DE-CIX in Frankfurt hervorzuheben. Darüber hinaus werden für einen Abgleich mit globalen Routing-Änderungen fallbezogen auch öffentlich zugängliche Datensätze des RouteViews-Projekts herangezogen. Im Folgenden werden zentrale Aspekte der erarbeiteten Routing-Analysen näher beleuchtet.

Technische Hintergründe Mittels BGP, einem verteilten Pfad-Vektor-Routing-Protokoll, werden Pfadinformationen zur Erreichbarkeit von Netzbereichen (IP-Präfixen) im Internet zwischen direkt verbundenen Routern ausgetauscht. Diese Pfade bestehen aus einer Abfolge von eindeutigen Nummern von Autonomen Systemen (AS), die auf dem Weg zu beliebigen Zielnetzen durchquert werden. Bei einer Routing-Entscheidung über alternative Weiterleitungspfade werden stets Routen zu spezifischeren IP-Präfixen, d.h. zu kleineren Netzblöcken bevorzugt (Longest Prefix Match). Stehen mehrere Pfade pro IP-Präfix zur Verfügung, so wird u.a. die Länge des AS-Pfades für die Entscheidungsfindung herangezogen, wobei kürzere Pfade begünstigt werden (Best Path Selection). Im Zuge der Weitergabe von Routen wird die Router-eigene AS-Nummer an AS-Pfade angehängt, eine mehrfache Angabe zur künstlichen Pfadverlängerung ist möglich (AS Path Prepending).

Im BGP-Protokollablauf teilt jeder Router allen direkten Nachbar-Routern dessen jeweils beste Route zu allen erreichbaren IP-Präfixen mit. Diese Routen werden lokal in der sog. Routing Information Base (RIB) vorgehalten und können von geeignet konfigurierten Routern exportiert werden. RIB-Exporte repräsentieren demnach eine vollständige – standortbezogene – Sicht auf das globale Internet-Routing. Auch eine Erfassung des Stroms von Update-Nachrichten aller Nachbarn, mit denen Routen-Änderungen im Protokollablauf übermittelt werden, ist möglich. Hier lassen sich generell zwei Arten von Informationen unterscheiden: neu gelernte bzw. geänderte AS-Pfade zu IP-Präfixen (enthalten in sog. Announcement-Nachrichten) sowie zurückgezogene IP-Präfixe, die die Nichterreichbarkeit von Netzwerken nach sich ziehen (enthalten in sog. Withdraw-Nachrichten).

Für die Detailanalyse von Internet-Vorfällen werden ein vollständiger RIB-Export zu Beginn des betrachteten Zeitrahmens sowie alle Update-Nachrichten bis zu dessen Ende herangezogen. Damit lassen sich die Auswirkungen eines Vorfalls auf das globale Internet-Routing – aus Sicht des jeweiligen Router-Standortes – zuverlässig analysieren und vergleichen. Diese Standorte werden stets fallabhängig gewählt, um die für den jeweiligen Vorfall

relevanten Fragestellungen zielgerichtet beantworten zu können. RIB-Einträge und BGP-Nachrichten weisen darüber hinaus eine Vielzahl an weiteren Attributen und manuell konfigurierbaren Parametern auf, mit deren Hilfe Routing-Entscheidungen sehr feingranular beeinflusst werden können. Im Allgemeinen ermöglichen diese zumeist nur lokal relevanten Datenpunkte jedoch keine neuen Erkenntnisse über strukturelle Änderungen in der globalen Routing-Topologie des Internets. Im weiteren Verlauf der Fallstudien werden diese Attribute daher nicht näher beleuchtet.

Alle für das globale Routing notwendigen numerischen Internet-Ressourcen, d.h. IP-Netzbereiche und AS-Nummern, werden von fünf Regionalen Internet Registraren (RIR) mit im Wesentlichen kontinentaler Verantwortlichkeit verwaltet. Entsprechende Registrierungsinformationen werden in Form von tagesaktuellen Vergabe- bzw. Delegationslisten veröffentlicht und beinhalten u.a. Länderzuordnungen und menschenlesbare Namen für vergebene Ressourcen. In Europa ist die nicht-kommerzielle Organisation Réseaux IP Européens (RIPE) für die Verwaltung von Internet-Ressourcen zuständig. Entsprechende historisch archivierte Datensätze fließen in die Analyse der Control Plane mit ein.

Zielanalyse Für die im Vorfeld identifizierten betroffenen Internet-Ressourcen wird deren Erreichbarkeit im Internet-Routing im zeitlichen Verlauf ausgewertet. Mittels einer quantitativen Analyse der entsprechenden BGP-Aktivität lassen sich genaue Vorfallshergänge rekonstruieren. Dazu wird die Anzahl empfangener BGP-Nachrichten für alle betroffenen IP-Präfixe während der Dauer eines Vorfalls untersucht. Announcement-Nachrichten weisen auf Pfadänderungen, d.h. Routing-Umleitungen, hin. Withdraw-Nachrichten signalisieren dagegen eine weltweite Nichterreichbarkeit von IP-Präfixen. Häufungen derartiger BGP-Ereignisse beschreiben demnach wichtige Eckpunkte des Vorfallshergangs.

Anhand der resultierenden Datenlage wird die Anzahl erreichbarer Autonomer Systeme aller beteiligten Parteien für jeden Zeitpunkt des Betrachtungszeitraums bestimmt. Dies entspricht der Menge aller Autonomen Systeme an den Enden der betrachteten BGP-Pfade. Ein Wegfall von Autonomen Systemen über alle Pfade hinweg beschreibt demnach einen Totalausfall entsprechender Netzanbieter im Internet-Routing.

Analog dazu wird die Anzahl erreichbarer IP-Präfixe über die Zeit hinweg betrachtet. Dabei erfolgt zunächst keine Unterscheidung zwischen überdeckten Präfixen, d.h. zwischen More/Less Specifics. Das Ergebnis beschreibt also alle tatsächlich aktiven BGP-Routen hin zu den betroffenen Netzbereichen. Der Wegfall entsprechender Routen impliziert lokale Netz- oder Router-Ausfälle, weniger spezifische Ausweich-Routen bleiben aber prinzipiell möglich. Um darüber hinaus auch Totalausfälle quantifizieren zu können, wird zudem das erreichbare /24 bzw. /48 IP-Äquivalent für alle betroffenen IPv4- bzw. IPv6-Präfixe bestimmt, d.h. durch Vereinigung aller betroffenen More/Less Specifics ergibt sich so die Zahl der tatsächlich (nicht-)erreichbaren IP-Addressen.

Transitanalyse Analog zur Zielanalyse werden alle betroffenen Internet-Ressourcen auch hinsichtlich der darüber laufenden Transit-Routen zu unbeteiligten Netzbereichen ausgewertet. Dies entspricht der Menge aller BGP-Routen mit betroffenen Autonomen Systemen auf den jeweiligen AS-Pfaden, jedoch mit nicht-betroffenen Zielnetzen an deren Enden. Im Ergebnis zeigen sich demnach Reichweite und Auswirkungen der Vorfälle im globalen Internet-Routing. Wie zuvor werden für alle zugehörigen Routen Teilanalysen zur BGP-Aktivität sowie zur Erreichbarkeit von Autonomen Systemen und IP-Präfixen über den Betrachtungszeitraum hinweg durchgeführt.

Änderungsanalyse Neben dem Totalausfall von Autonomen Systemen und Netzbereichen werden auch Routing-Änderungen ohne explizite Nichterreichbarkeiten näher beleuchtet. Durch eine Analyse von Transit-Änderungen im Routing betroffener Netzbereiche lassen sich Internet-weite Auswirkungen analysieren. Dazu wird eine Rangfolge wichtiger Transit-ASe nach deren Zahl an BGP-Routen hin zu den betrachteten Internet-Ressourcen im zeitlichen Verlauf generiert. Die Ergebnisse sind aufgrund von zumeist mehreren beteiligten Transit-ASen pro BGP-Pfad nicht kumulativ, zeigen aber deutlich qualitative Änderungen im Internet-Routing. Entsprechende Analysen werden auch für Transitländer über eine RIR-basierte AS-zu-Land-Zuordnung durchgeführt. Alle Ergebnisse werden hinsichtlich der Zahl an erreichbaren Ziel-ASen, IP-Präfixen und dem /24 bzw. /48 IP-Äquivalent für IPv4- bzw. IPv6-Präfixe gewichtet und verglichen.

In einem weiteren Schritt werden Änderungen in der Routing-Topologie für betroffene Internet-Ressourcen im zeitlichen Verlauf näher beleuchtet. Dazu kann die Anzahl neuer, bisher nicht beobachteter BGP-Pfade und AS-Verbindungen seit Beginn des jeweiligen Analyseintervalls herangezogen werden. Das Ergebnis stellt dementsprechend ein absolutes Maß für Topologieänderungen hin zu den betrachteten Netzen dar. Ein Rückgang dieser Werte im Vorfallsverlauf bedeutet eine graduelle Wiederherstellung des Ausgangszustandes, andernfalls liegen längerfristige Änderungen vor.

Pfadanalyse Eine erste Indikation zu Auswirkungen von Internet-Vorfällen auf die Dienstqualität betroffener Netzdienste lässt sich aus der Analyse von BGP-Pfadlängen zu den betrachteten Netzbereichen ableiten. Je länger die Pfade (ohne Berücksichtigung von AS Path Prepending), d.h. je mehr Autonome Systeme an der Weiterleitung beteiligt sind, desto schlechtere Dienstqualität ist in der Regel zu erwarten. Um möglichst breit gefasste Aussagen auch ohne Einzelbetrachtung von BGP-Pfaden zu ermöglichen, werden neben Durchschnittswerten auch Streuungsmaße der Pfadlängenverteilung berechnet. Mit Hilfe von 5/25/50/75/95%-Quantilen lassen sich so belastbare Rückschlüsse auf das Ausmaß der Pfadveränderungen im zeitlichen Verlauf ziehen.

Betroffene Länder Für eine bessere Einschätzung der Reichweite von Internet-Vorfällen wird eine geographische Verortung aller betroffenen Netzbereiche vorgenommen. Dies erfolgt über eine RIR-basierte Zuordnung von IP-Präfixen und Autonomen Systemen auf Länder. Je nach fallspezifischem Szenario werden verschiedene Routing-Fragestellungen für die betroffenen Länder ausgewertet. Von besonderem Interesse sind dabei Umleitungen hin zu bzw. weg von den betrachteten Internet-Ressourcen sowie darüber neu geroutete bzw. ausgefallene Netzbereiche einzelner Länder. Alle Ergebnisse werden hinsichtlich der Zahl an betroffenen Ziel-ASen, IP-Präfixen und dem /24 bzw. /48 IP-Äquivalent für IPv4- bzw. IPv6-Präfixe gewichtet und länderbezogen ausgewertet.

Analyse der Data Plane

Konkrete Auswirkungen von Routing-Änderungen und Netzausfällen auf Netzdienste lassen sich mit Hilfe von aktiven IP-Pfadmessungen näher untersuchen. Für die nachfolgenden Vorfallsanalysen wird dazu auf die von RIPE betriebene ATLAS-Messinfrastruktur zurückgegriffen. Diese Infrastruktur besteht aus etwa 600 leistungsstarken Anchor-Messknoten und weiteren ca. 12,000 kleineren Probe-Messknoten. Damit werden über 3,500 Autonome Systeme in 175 Ländern abgedeckt, die als Quelle für IP-Pfadmessungen zur Verfü-

gung stehen. Neben manuellen Einzelmessungen ermöglicht die ATLAS-Messinfrastruktur kontinuierliche periodisch ausgeführte Messungen (sowohl vorkonfiguriert als auch benutzerdefiniert), die sich in besonderem Maße für forensische Detailanalysen eignen.

Technische Hintergründe Eine Erhebung von Router-Pfaden im Internet erfolgt generell mit Hilfe aktiver IP-Messungen. Dazu werden ausgehend von einer Messstation IP-Pakete zu Messzielen mit steigender Time-To-Live (TTL) beginnend bei Wert 1 versendet. Das zugehörige TTL-Feld in den IP-Kopfdaten der Pakete wird von allen Routern entlang des durchlaufenen Pfades sukzessive um 1 verringert. Gemäß der ursprünglichen Intention dieses Mechanismus – einer Begrenzung der Lebensdauer von IP-Paketen – führt ein TTL-Wert von 0 zum Verwurf des Datenpakets am verarbeitenden Router. Über das Internet Control Message Protocol (ICMP) wird dabei eine Fehlernachricht mit Informationen zum verworfenen Paket zurück an den Absender gesendet. Mittels Zuordnung der Fehlernachrichten zu den versandten Messpaketen, meist anhand von eindeutigen Port-Nummern je Paket, lässt sich der vollständige IP-Pfad zum Messziel rekonstruieren.

Aufgrund der individuellen Paketvermittlung im Internet – Weiterleitungsentscheidungen werden für alle IP-Pakete stets unabhängig getroffen – können Messpakete auf unterschiedlichen Pfaden zum Messziel gelangen und somit zu verfälschten Messergebnissen führen. Um diesen in der Praxis meist durch Lastausgleichspfade hervorgerufenen Messartefakten zuverlässig entgegenzuwirken, kann auf den sog. Paris-traceroute Ansatz zurückgegriffen werden. Diesem Verfahren liegt die Annahme zugrunde, dass eine lastausgleichende Wegewahl meist auf Basis von Quell/Ziel-Adressen und -Ports basiert. Die herkömmliche Pfadzuordnung mittels individueller Port-Nummern je Messpaket wird daher durch andere, grundsätzlich frei wählbare Felder in den Kopfdaten der Transportschicht, wie bspw. Sequenznummern, ersetzt. In der Konsequenz werden IP-Pakete einer Messung meist über gleiche Lastausgleichspfade geleitet und die Qualität der Messergebnisse somit deutlich erhöht. Ein vergleichbares Verfahren steht auch in der RIPE ATLAS-Messinfrastruktur und damit für die vorliegenden Fallstudien zur Verfügung.

Die konzeptuellen Rahmenbedingungen für IPv6-basierte Pfadmessungen entsprechen denen von IPv4-Messungen, der vorgestellte Ansatz kann demnach in analoger Weise auch für IPv6-Messungen eingesetzt werden. Das TTL-Feld von IPv6-Paketen (hier Hop Limit genannt) funktioniert nach gleichem Prinzip wie für IPv4-Pakete, ebenso können die aus ablaufenden TTL-Werten resultierenden ICMPv6 Router-Fehlernachrichten zur Rekonstruktion von Pfadinformationen verwendet werden. In der Praxis sind Pfadmessungen in beiden Protokollvarianten allerdings nur selten vollständig, da nicht alle Router die benötigten Fehlernachrichten generieren. Auch ICMP-Ratenlimitierungen können derartige – meist mittels „Sternchen“ dargestellte – nicht-responsive Router hervorrufen.

Im Rahmen der Datenanalysen werden aus den resultierenden IP-Pfadinformationen unter Zuhilfenahme einer aus BGP abgeleiteten Abbildung von IP-Präfixen auf zugehörige Quell-ASe weiterhin auch AS-Pfade abgeleitet. Nicht-auflösbare IP-Addressen sowie Sternchen verbleiben dabei als Pfadlücken im Ergebnis. Über diese strukturellen Pfadinformationen hinaus werden im Zuge des Messprozesses auch Zeitstempel für alle ein- und ausgehenden IP-Pakete protokolliert. Über deren Differenz können somit Umlaufzeiten, sog. Round Trip Times (RTT) zum Messziel und zu allen Routern auf dem Pfad gemessen werden. Um negative Effekte kurzfristiger Lastspitzen und damit potentiell verfälschte Zeitmessungen zu vermindern, werden in der Praxis mehrere Messpakete mit gleichem TTL-Wert versendet und daraus eine minimale Umlaufzeit berechnet.

Pfadanalyse Für eine belastbare Bewertung der Auswirkung von Internet-Vorfällen auf Netzdienste werden IP-Pfadmessungen für die betroffenen Internet-Ressourcen ausgewertet. Dafür lassen sich analog zur Control Plane zunächst Pfadlängen, d.h. die Zahl der an der Weiterleitung beteiligten IP-Router, heranziehen. Auch hier gilt: je länger diese Pfade, desto schlechtere Dienstqualität ist zu erwarten. Darüber hinaus können in der Data Plane aber auch Änderungen an Umlaufzeiten und nicht-responsiven Routern betrachtet werden. Aufgrund der breit gestreuten ATLAS-Messinfrastruktur lassen sich alle Ergebnisse zudem auch explizit auf Messquellen, Messziele und Transit-Router einschränken und getrennt analysieren. Eine Auswertung über Messquellen nach Kontinent wird ebenfalls realisiert. Daraus ergeben sich vielfältige Bewertungsperspektiven, die detaillierte Rückschlüsse auf Konsequenzen für Internet-Verkehr aus/über/zu den Netzen betroffener Parteien zulassen. Eine separate Betrachtung von IP-Pfaden mit ausschließlich antwortenden, d.h. erreichbaren Messzielen, wird zur Abgrenzung von Dienstausfällen und Qualitätsminderungen ebenfalls vorgenommen. Unter Berücksichtigung von Durchschnittswerten und 5/25/50/75/95%-Quantilen für alle Teilergebnisse lassen sich somit umfassende Erkenntnisse über die konkreten Konsequenzen der Vorfälle gewinnen.

Messanalyse Für eine weitere Quantifizierung netzinterner Ausfälle von betroffenen Parteien, die nicht zwangsläufig bereits in der Control Plane ersichtlich sind, werden erfolgreich durchgeführte IP-Pfadmessungen denen mit ausbleibenden Antwortpaketen der Messziele gegenübergestellt. Über diese Analysen wird das Ausmaß von Ausfällen absolut und insbesondere auch relativ zum Normalzustand ersichtlich. Die erzielten Ergebnisse werden analog zur Pfadanalyse separat nach Messquellen, Messziele und Transit-Router sowie nach Kontinent betrachtet und im zeitlichen Verlauf ausgewertet.

Betroffene Länder Analog zur Control Plane wird für eine weitere Einschätzung der Reichweite von Internet-Vorfällen eine geographische Verortung aller betroffenen IP-Pfadmessungen vorgenommen. Einzelne IP-Adressen werden dabei zunächst auf entsprechende in BGP geroutete IP-Präfixe und diese wiederum über eine RIR-basierte Zuordnung von IP-Präfixen auf Länder abgebildet. Alle betroffenen IP-Pfadmessungen werden separat für Messquellen, Messziele und Transit-Router ausgewertet und nach deren Länderzugehörigkeit gegenübergestellt. Aus dem Ergebnis lassen sich Auswirkungen auf Internet-Verkehre aus/über/zu betroffenen Ländern ablesen und somit detaillierte Schlüsse über das geographische Ausmaß der betrachteten Vorfälle ziehen.

Bewertung und Folgen

Anhand einer detaillierten Rekonstruktion der Vorfallshergänge und unter Berücksichtigung von Analyseergebnissen der Control Plane und Data Plane werden die untersuchten Internet-Vorfälle abschließend bewertet. Dies umfasst die folgenden Fragestellungen.

Charakteristische Besonderheiten Basierend auf den gewonnenen Erkenntnissen werden charakteristische Vorfallsmerkmale zusammengefasst und etwaige Auffälligkeiten diskutiert. Hierunter kann bspw. das Auftreten mehrerer – unabhängiger oder zusammenhängender – Teilvorfälle oder auch eine notwendige Bewertungskorrektur aufgrund von datengestützten Ergebnissen fallen. Ebenso lassen sich anhand der empirischen Erkenntnisse Medienberichte überprüfen oder tiefergehende Ursachenforschung betreiben.

Konsequenzen und Auswirkungen Die öffentlich dokumentierte Perspektive zu den betrachteten Internet-Vorfällen wird um Erkenntnisse der datengestützten Analysen hinsichtlich Dienstausfälle und Qualitätsminderungen ergänzt. Unter Berücksichtigung aller Ergebnisse werden dabei auch mittel- und längerfristige Konsequenzen betrachtet.

Schutz- und Gegenmaßnahmen Die Effektivität der im Verlauf der Vorfälle getroffenen Maßnahmen wird unter Einbezug charakteristischer Falleigenschaften und der erzielten Analyseergebnisse diskutiert. Anhand des Stands der Technik – sowohl in wissenschaftlichen Arbeiten als auch kommerziellen Produkten – werden fallbezogene Möglichkeiten für Schutz- und Gegenmaßnahmen erörtert und bestehende Defizite aufgezeigt.

Wesentliche Erkenntnisse In einer abschließenden Zusammenfassung werden die zentralen Erkenntnisse der Detailanalysen kurz und prägnant aufbereitet. Dabei werden auch neuartige Vorfallsqualitäten sowie generelle Risiken für kritische Infrastrukturen hervorgehoben. Zudem erfolgt eine Bewertung der Eintrittserwartung und praktischen Relevanz des jeweils betrachteten Internet-Vorfalls. Im Rahmen einer subjektiven Einschätzung werden schließlich konkrete Gefahren und Handlungsalternativen insbesondere im Hinblick auf die deutsche Internet-Infrastruktur diskutiert.

Interaktive Darstellung

Alle im Zuge der Detailanalysen erarbeiteten Informationen und Ergebnisse können neben der Aufarbeitung in diesem Dokument auch über die interaktive Web-Anwendung zum Projekt abgerufen werden:

`https://zwiback.leitwert.net`

Auf entsprechenden Detailseiten werden die zur Beschreibung der Internet-Vorfälle herangezogenen Diagramme mit zahlreichen Interaktionsmöglichkeiten bereitgestellt. Die zugrundeliegenden Daten lassen sich auf betroffene Netzbereiche und Länder, auf einzelne Datenkollektoren bzw. Messstandorte sowie auf IPv4- und IPv6-Daten einschränken. Zudem können verschiedene Darstellungsarten gewählt und Zusatzinformationen mit Hilfe von Einblendungen manuell abgerufen werden.

2.2.2 Fallstudie: Großflächiger Stromausfall in Südamerika

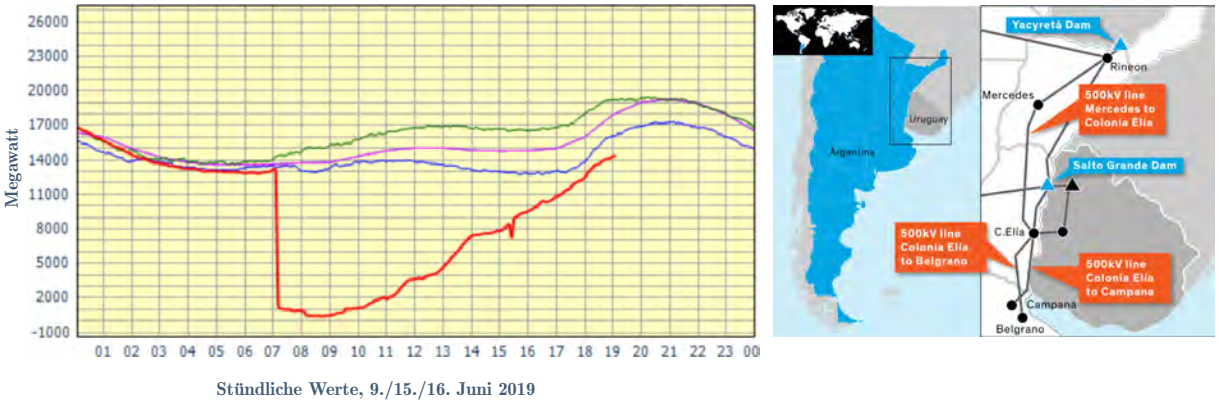
2.2.2.1 Übersicht und Einordnung [4]

Am 16. Juni 2019 kam es zu langanhaltenden, großflächigen Stromausfällen in Südamerika. Ausgelöst wurde der Totalausfall im argentinischen Hochspannungsnetz Sistema Argentino de Interconexión (SADI), das vom Energieversorger Transener betrieben wird. SADI ist sowohl für die landesweite Energieversorgung als auch für den Energieaustausch mit den Nachbarländern Paraguay und Uruguay zuständig, die ebenfalls betroffen waren.

Vorfallshergang [1] Am 16. Juni 2019 tritt um 07:06 Uhr Ortszeit (10:06 Uhr UTC) ein Kurzschluss in einer 500kV Leitung zwischen Colonia Elia und Belgrano in Buenos Aires auf. Der Fehler breitet sich im gesamten SADI-Netz aus und führt innerhalb von 30

[1] `http://carlosstjames.com/renewable-energy/argentinas-june-2019-blackout-what-went-wrong/`

Sekunden zum Totalausfall. Die an das Netz angeschlossenen Nachbarländer Uruguay und Paraguay sind ebenfalls betroffen. In Uruguay bricht die Energieversorgung ebenfalls vollständig zusammen, Paraguay hingegen ist nur teilweise betroffen. Dass der Kurzschluss trotz Schutzmaßnahmen zu derart katastrophalen Auswirkungen führen konnte, hat mehrere Gründe. Zunächst betrug der Stromverbrauch zum Zeitpunkt des Kurzschlusses an diesem Sonntag Morgen nur ca. 70% gegenüber einem normalen Wochentag. Abb. 2.15a zeigt den Verbrauch am Vorfallstag (Rot) im Vergleich zum Vortag (Grün), der vorherigen Woche (Blau) und dem Dispatch, d.h. der tatsächlichen Leistungseinspeisung (Pink).



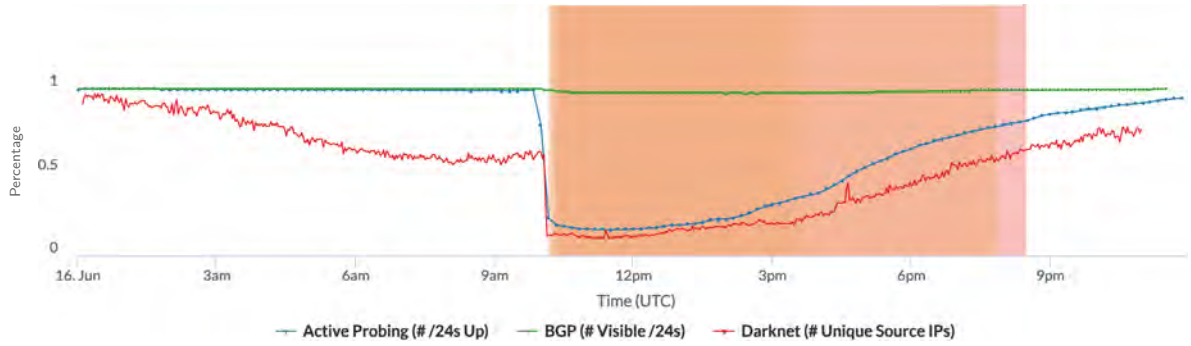
(a) Stromverbrauch (Tagesvergleich) (b) Betroffene Kabel

Abbildung 2.15: [I2] **Stromausfall in Argentinien**, SADI-Netz [4]

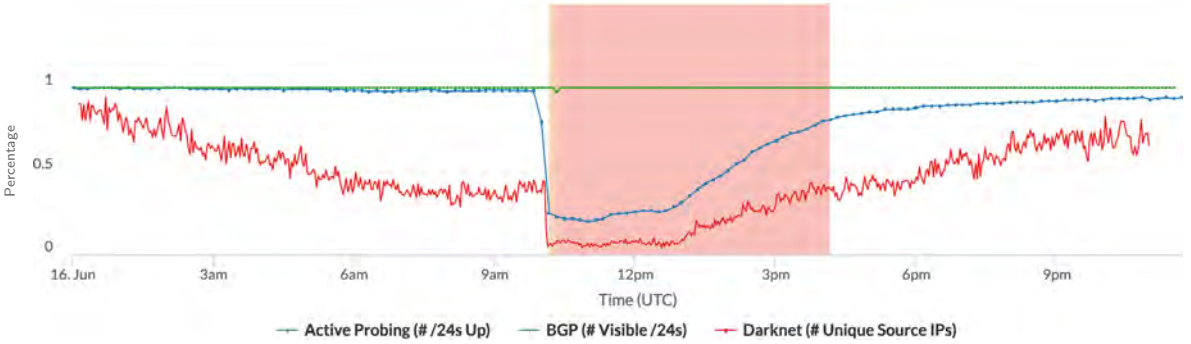
Weiterhin wurde durch hohe Wasserstände in zwei Wasserkraftwerken im Norden des Landes überdurchschnittlich viel Energie produziert. Die betroffene Hochspannungsleitung verbindet die Kraftwerke mit der Metropolregion Buenos Aires, wodurch der Ausfall verstärkt wurde. Nachfolgende Untersuchungen haben weiterhin ergeben, dass die Schutzmaßnahmen, die einen solchen Ausfall verhindern sollen, fehlerhaft waren. Diese bestehen aus redundanten Hochspannungsleitungen und einem System namens Automatic Generation Disconnection (DAG), das Generatoren bei starken Lastabfällen innerhalb von 200 Millisekunden vom Netz trennen soll, um eine Überlast zu verhindern. Durch Bauarbeiten an einem Strommasten war die parallel zur betroffenen Leitung verlaufende Verbindung zwischen Colonia Elia und Campana nicht einsatzbereit (Abb. 2.15b). Zusätzlich wurde das DAG-System nach den Bauarbeiten nicht an die neue Situation angepasst, weswegen die Generatoren zu spät vom Netz getrennt wurden und es zu einer Überlast kam.

Durch Einsatz von Sub-Frequency Relays (SFR), die bei Unregelmäßigkeiten wie Überlast automatisch Leitungen trennen, wurde SADI in zwei separate Netze geteilt: den nördlichen Netzbereich mit hoher Produktion, sowie den südlichen Bereich mit großem Bedarf. Nach der eingetretenen Netzseparierung wurden schließlich weitere Kraftwerke manuell von den Betreibern vom Netz getrennt, um Schäden an den Anlagen zu verhindern. Durch die extreme Unterversorgung im Süden und die hohe Überproduktion im Norden folgte unausweichlich der vollständige Ausfall des landesweiten Stromnetzes.

Direkte Folgen Die Energieversorgung wurde laut Betreiber bis ca. 22:00 Uhr Ortszeit des selben Tages wieder vollständig hergestellt. Bis zu diesem Zeitpunkt hatten bis zu 48 Millionen Menschen in Argentinien, Uruguay und Paraguay keine Energieversorgung. Da ein solcher Ausfall mit funktionstüchtigen Schutzmaßnahmen nicht möglich gewesen wäre, kündigte die Regierung in der Folge Strafen für die beteiligten Parteien an. Diese



(a) Argentinien



(b) Uruguay

Abbildung 2.16: [I2] **CAIDA-Datenlage**, IODA [5]

sollen sowohl gegen Transener für die fehlerhafte DAG-Konfiguration als auch gegen die Betreiber der SFR und der manuell getrennten Kraftwerke verhängt werden. Weitere mittel- oder langfristigen Folgen sind nicht bekannt, insbesondere auch nicht im Hinblick auf Konsequenzen für die Internet-Infrastruktur.

Verwandte Vorfälle Die aus den vergleichsweise schnellen Reaktionszeiten resultierende mittlere Vorfallsdauer liegt unter dem Durchschnitt von technischen Defekten (siehe Abschnitt 2.1.2.1), die Reichweite ist mit landesweiten Beeinträchtigungen dagegen überdurchschnittlich hoch. Bei den zu verzeichnenden hohen Auswirkungen ergeben sich keine Abweichungen vom Durchschnitt. Ein ähnlich gelagerter Vorfall trat am 9. April 2018 in einem Frankfurter Rechenzentrum des Betreibers Interxion auf [I5]. Analog zum Fall in Südamerika wurde die Stromversorgung durch einen technischen Defekt in Kombination mit versagenden Schutzmechanismen ausgelöst und hielt für mehrere Stunden an. Der Stromausfall war zwar beschränkt auf ein einzelnes Rechenzentrum, jedoch hatte der Vorfall ebenfalls weitreichende Folgen: unter den betroffenen Kunden von Interxion befanden sich zahlreiche Netzbetreiber, darunter die Deutsche Telekom und große Teile der DE-CIX-Plattform, beides zentrale Bestandteile der deutschen Internet-Infrastruktur.

Wissenschaftliche Arbeiten Aufgrund des seltenen Auftretens großflächiger und länger anhaltender Stromausfälle existieren nur wenige empirische Studien über deren Auswirkungen auf die Internet-Infrastruktur [6, 7, 8]. Der *I-Seismograph* [9] wurde konzipiert, um weitreichende Internet-Störfälle frühzeitig zu erkennen und deren Tragweite einzustufen. Weitere Arbeiten befassen sich mit den Konsequenzen großflächiger Blackouts im Allgemeinen [10, 11, 12]. Darüber hinaus wurden auch Ansätze für eine Erhöhung

der Internet-Resilienz gegenüber entsprechenden Vorfällen erarbeitet [13, 14, 15, 16]. Die oben stehende Datenauswertung der Forschungseinrichtung CAIDA (Abb. 2.16) zeigt erste konkrete Auswirkungen des Stromausfalls auf deren Messverkehr [5]. Während ein Rückgang der im globalen Internet-Routing sichtbaren IP-Präfixe (BGP) für die betroffenen Länder nicht zu verzeichnen ist, bricht der Anteil aktiv vermessener Netzwerke (Active Probing) sowie der IP-Adressen, die im Hintergrundrauschen eines unbenutzten /8-Präfix beobachteten wurden (Darknet), während des Vorfallszeitraumes deutlich ein.

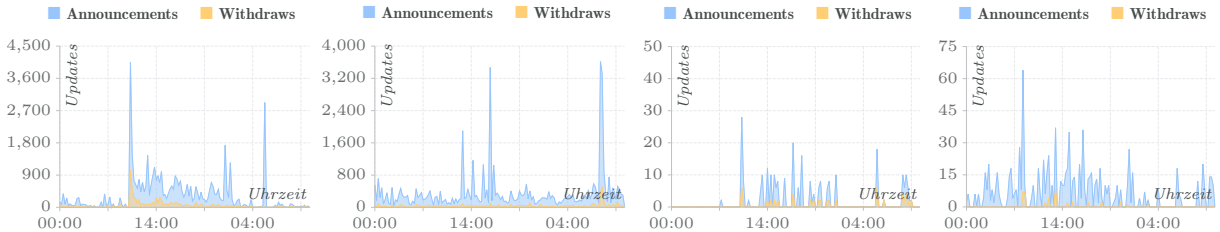
Dieser qualitativen Betrachtung des argentinischen Stromausfalls werden im Folgenden quantitative Ergebnisse anhand einer datengestützten Analyse gegenübergestellt, um konkrete Auswirkungen auf einzelne Teile der Internet-Infrastruktur näher zu beleuchten.

2.2.2.2 Analyse der Control Plane

Anhand einer Analyse von BGP-Tabellen lassen sich größere Auswirkungen im Internet-Routing, wie bspw. ISP-Ausfälle, Verkehrsumleitungen oder Topologieänderungen, untersuchen. Die Erwartungshaltung im Hinblick auf die hohe Reichweite des Stromausfalls wären spürbare Konsequenzen auf das argentinische Internet, möglicherweise jedoch aufgefangen durch Ausweich-Routen über das Nachbarland Brasilien.

Für die folgenden Auswertungen wird stets der Zeitraum von 16. Juni 2019 um 00:00 Uhr UTC bis 17. Juni 2019 um 12:00 Uhr UTC zugrunde gelegt. Sofern nicht anders angegeben, erfolgt die Analyse des Vorfalls aus Sicht der Deutschen Telekom (DTAG) als außenstehender Beobachtungspunkt, d.h. anhand der BGP Routing-Tabellen von AS3320. Alle Diagramme und Ergebnisse beziehen sich zunächst nur auf IPv4, im Falle von signifikanten Unterschieden oder interessanten Zusatzerkenntnissen werden entsprechende Daten zu IPv6 ebenfalls mit aufgenommen. Alle IPv4/IPv6-Ergebnisse lassen sich (auch aus der Perspektive weiterer BGP-Standorte) auf der interaktiven Projekt-Webseite abrufen.

Zielanalyse In einem ersten Schritt werden Netzausfälle in direkt und indirekt betroffenen Ländern, d.h. in Argentinien und Uruguay bzw. Brasilien und Paraguay, betrachtet. Ein einfaches Indiz für Änderungen im Internet-Routing von Zielnetzwerken stellt die BGP-Aktivität für entsprechende IP-Präfixe dar (Abb. 2.17).

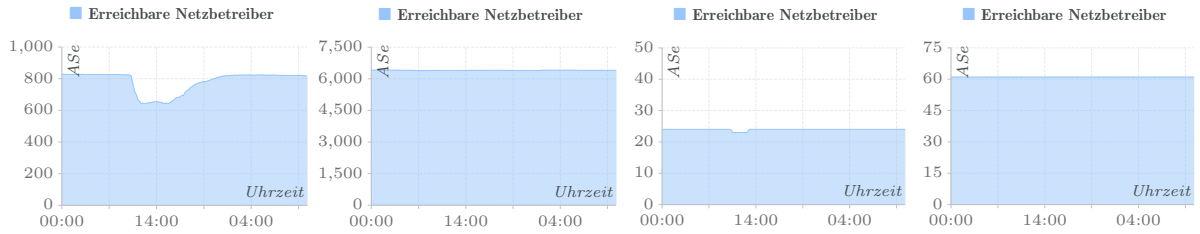


(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.17: [I2] **BGP-Aktivität**, Zielanalyse (Control Plane)

Für Argentinien und Brasilien zeigt sich eine hohe Zahl an Routing-Änderungen während des Vorfalls (ab 10:00 UTC) und auch darüber hinaus (ab 01:00 UTC). Uruguay und Paraguay sind aufgrund deren geringer Zahl an Routing-Teilnehmern in der globalen BGP-Aktivität nur untergeordnet vertreten. Nichtsdestotrotz finden sich auch dort Indizien für Änderungen. Im Ergebnis dieser Analyse ist insbesondere eine nicht unwesentliche

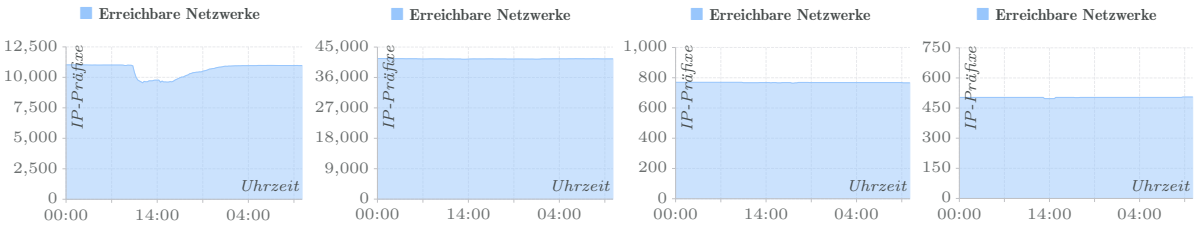
Zahl an BGP Withdraw Nachrichten für Argentinien und Uruguay hervorzuheben. Deren Folgen auf die Erreichbarkeit Autonomer Systeme ist nachfolgend ersichtlich (Abb. 2.18).



(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.18: [I2] **Autonome Systeme**, Zielanalyse (Control Plane)

Argentinien verzeichnet während des Stromausfalls einen Einbruch erreichbarer Autonomer Systeme um 22,5% (absolut: 186), in Uruguay ist ein einzelnes (von 24) Autonomen Systemen betroffen. In den beiden anderen Ländern ist erwartungsgemäß kein nennenswerter Effekt zu beobachten. Im Hinblick auf die argentinische IPv6-Konnektivität sind 15 Ausfälle (bei insgesamt 116 IPv6-fähigen Autonomen Systemen) zu verzeichnen, im Falle von Uruguay keine. Für Brasilien und Paraguay wurden interessanterweise 34 bzw. 2 IPv6-Ausfälle zwischen 12:00 und 15:00 UTC erfasst. Ein Vergleich mit den erreichbaren IP-Präfixen zeigt das Ausmaß aller beobachteten Ausfälle (Abb. 2.19).



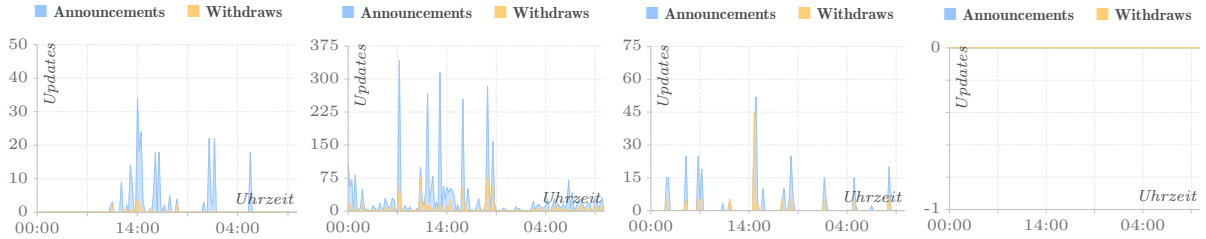
(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.19: [I2] **IP-Präfixe**, Zielanalyse (Control Plane)

Für Argentinien ist eine Zurücknahme von 13,3% aller vor dem Stromausfall gerouteten IP-Präfixe (IPv6: 11,7%) ersichtlich. Die dabei tatsächlich nicht mehr erreichbaren IP-Adressen, d.h. ohne *less specific* Ausweich-Routen, entsprechen in etwa dem Äquivalent eines /13-Netzbereichs bzw. 3,0% aller argentinischen IP-Adressen (IPv6: /28-Netzbereich bzw. 0,36%). Ausfälle von IP-Präfixen der anderen Länder treten analog zu Ausfällen Autonomer Systeme kaum in Erscheinung und sind im Wesentlichen vernachlässigbar.

Mit der Wiederherstellung größerer Teile der Stromversorgung um 01:00 UTC folgt auch eine nahezu vollständige Wiedererreichbarkeit der betroffenen Netzbereiche. Einzelne Autonome Systeme und IP-Präfixe bleiben allerdings auch darüber hinaus unerreichbar, hier ist von technischen Folgedefekten oder auch mangelhaften bzw. wenig erprobten Wiederanlaufprozeduren bei den jeweiligen Netzbetreibern auszugehen.

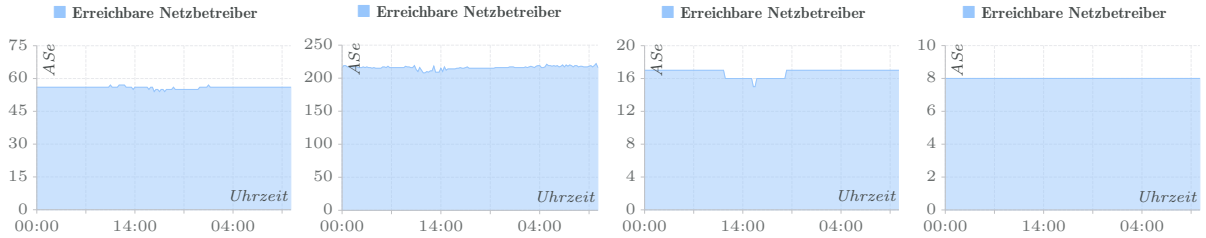
Transitanalyse Mit Hilfe einer Analyse von Transitänderungen lassen sich Ausweich-Routen und kollaterale Effekte des Stromausfalls im Internet-Routing untersuchen. Dazu wird nach obigem Schema zunächst wieder die BGP-Aktivität Autonomer Systeme betrachtet, in diesem Fall allerdings für solche mit vorfallsunabhängigem Ursprungsland, jedoch mit Transitverbindungen über die betroffenen Länder (Abb. 2.20).



(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.20: [I2] **BGP-Aktivität**, Transitanalyse (Control Plane)

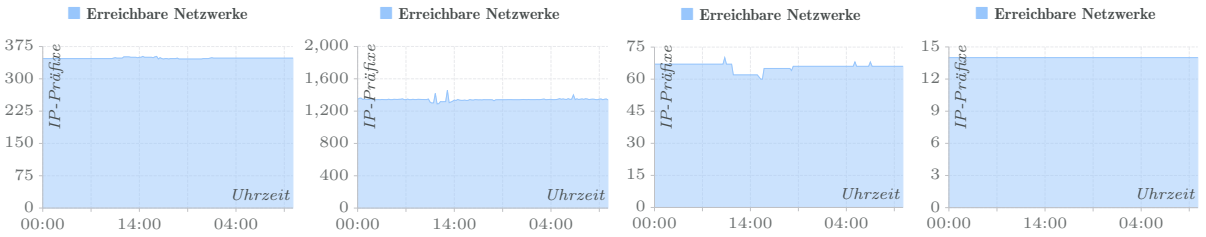
Gemessen an der absoluten Zahl der Routing-Änderungen ist außer für Brasilien keine nennenswerte BGP-Aktivität zu verzeichnen. Eine wesentliche Änderung am Transitverhalten der direkt betroffenen Länder Argentinien und Uruguay ist weder für IPv4 noch für IPv6 erkennbar, lediglich einzelne BGP-Routen unterliegen Änderungen. Dies wird insbesondere auch durch die nur unwesentlich fluktuierende Zahl der über die betrachteten Länder erreichbaren Autonomen Systeme bestätigt (Abb. 2.21).



(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.21: [I2] **Autonome Systeme**, Transitanalyse (Control Plane)

Die Annahme, dass Verkehre für eine größere Anzahl Autonomer Systeme über das vom Stromausfall kaum betroffene Nachbarland Brasilien umgeleitet werden, lässt sich anhand der IPv4/IPv6-Datenlage nicht bzw. nur für einzelne ISPs belegen. Eine ergänzende Perspektive ergibt sich aus der Betrachtung von Transit-IP-Präfixen (Abb. 2.22).

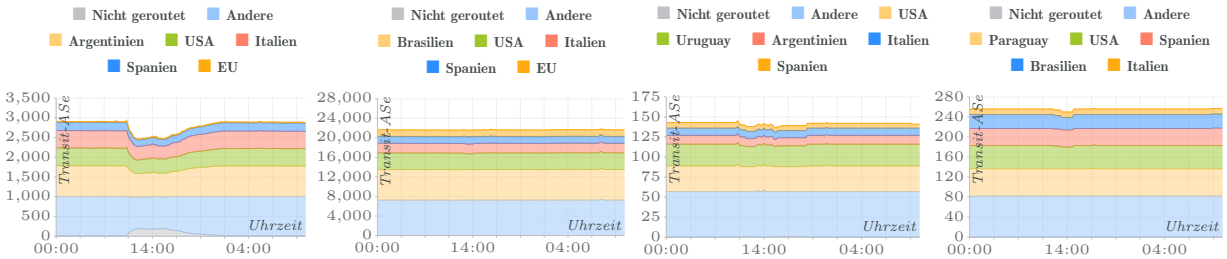


(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.22: [I2] **IP-Präfixe**, Transitanalyse (Control Plane)

In den ersten Stunden des Stromausfalls werden bis zu 100 IP-Präfixe neu über Brasilien geroutet, dies entspricht einem Plus von 7,0%. Für IPv6 fällt die Zahl der Transit-IP-Präfixe über Brasilien dagegen um 10,7% ab. Zusammenfassend sind in den betroffenen Ländern allerdings Änderungen an deren Transitverhalten nur in geringem Maße zu beobachten. Dieser Umstand ist aber naturgemäß auch in der generell weniger bedeutsamen Rolle dieser Länder für das länderübergreifende Internet-Routing zu begründen.

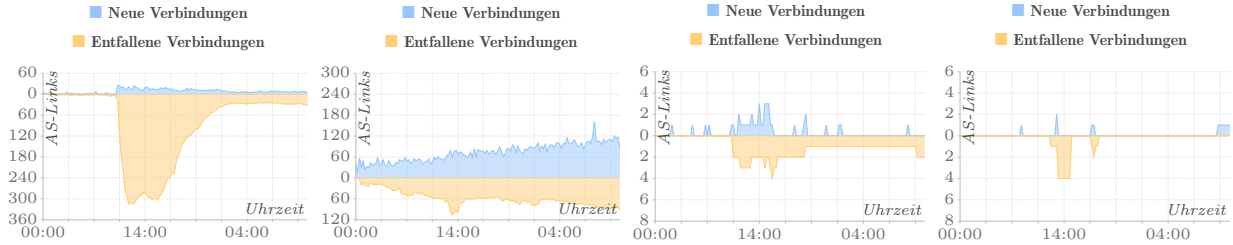
Änderungsanalyse Im Folgenden sollen explizite Änderungen des Internet-Routings vom Standort Deutschland bzw. der Deutschen Telekom aus hin zu den betroffenen Ländern quantifiziert werden. Dazu werden zunächst die Anteile internationaler Autonomer Systeme am Routing zu diesen Ländern qualitativ gegenübergestellt (Abb. 2.23).



(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.23: [I2] **Transitverlauf**, Länder nach Ziel-ASen (Control Plane)

Die Einbrüche in der Zahl an erreichbaren Autonomen Systemen (insbesondere in Argentinien) spiegeln sich auch in dieser Darstellung wieder. Die Zusammensetzung der wichtigsten am Routing beteiligten Transit-Provider ändert sich allerdings nicht. Gleiches gilt für die verbleibenden weniger betroffenen Länder. Der Stromausfall in Südamerika führte demnach zu keinen relevanten Umschichtungen im globalen Internet-Routing. Regional lassen sich dagegen deutliche topologische Verschiebungen feststellen (Abb. 2.24).

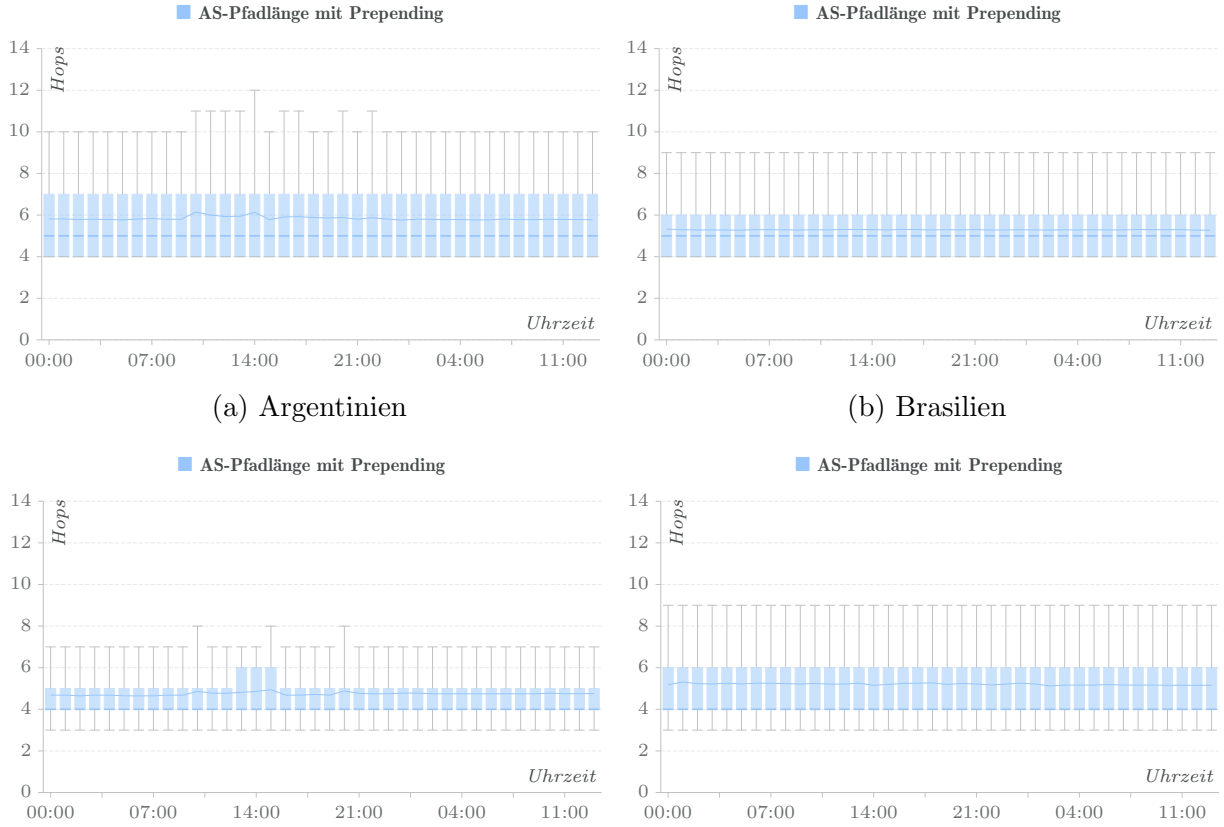


(a) Argentinien (b) Brasilien (c) Uruguay (d) Paraguay

Abbildung 2.24: [I2] **Topologieverlauf**, AS-Links (Control Plane)

Für das Routing von argentinischen IP-Präfixen lassen sich innerhalb der ersten 12 Stunden des Stromausfalls über 300 weggefallene sowie bis zu 60 neue, bis dahin nicht sichtbare AS-Verbindungen verzeichnen. Diese Verbindungen entstehen zusätzlich zu den bereits vorhandenen und werden mit Wiederherstellung der Stromversorgung wieder rückgebaut, weggefallene Verbindungen werden ebenfalls zu einem Großteil wiederhergestellt. Für brasilianische IP-Präfixe dagegen können ebenfalls etwa 100 neue AS-Verbindungen beobachtet werden, die frühere bestehende Verbindungen ablösen und sich auch nach der Wiederherstellung nicht zurückbilden. Aufgrund der deutlich höheren Zahl an Netzanbietern im Land und dem Einsetzen des beschriebenen Verhaltens bereits vor dem Stromausfall ist hier jedoch zum überwiegenden Teil von regulären, d.h. nicht vorfallsbezogenen, Routing-Änderungen auszugehen. Zweifelsfrei auf den Stromausfall lässt sich nur eine kleinere temporäre Spitze von etwa 40 ausgefallenen AS-Verbindungen zurückführen. Für die verbleibenden Länder Uruguay und Paraguay zeigen sich abgesehen von Einzelfällen keine nennenswerten Topologieänderungen.

Pfadanalyse Der Ausfall einer größeren Anzahl von ISPs kann bei Umleitung über bestehende, weniger günstige Alternativ-Routen längere AS-Pfade und damit eine schlechtere Verbindungsqualität – auch für nicht direkt betroffene Netzbereiche – nach sich ziehen. Dies wird für den vorliegenden Ausfall im Folgenden näher untersucht (Abb. 2.25).



(a) Argentinien

(b) Brasilien

(c) Uruguay

(d) Paraguay

Abbildung 2.25: [I2] **Pfadanalyse**, inkl. AS Path Prepending (Control Plane)

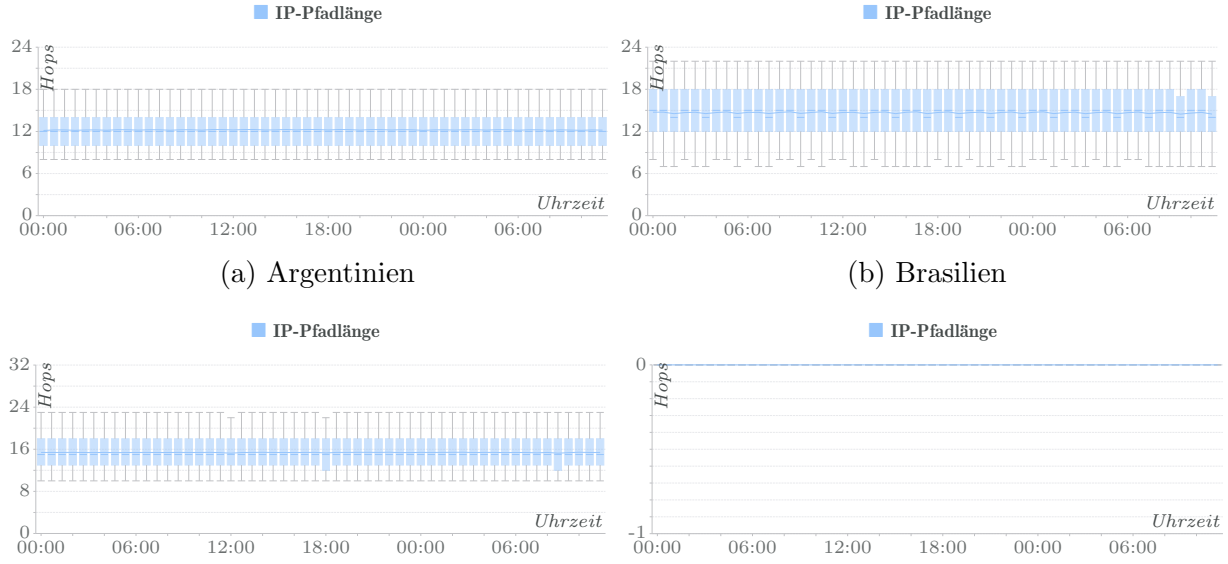
Während des Stromausfalls ist für die vorrangig betroffenen Länder Argentinien und Uruguay in der Tat ein gewisser Anstieg der durchschnittlichen AS-Pfadlänge zu beobachten. Für Argentinien betrifft dies allerdings nur 5% aller Netzbereiche, d.h. es sind lediglich Änderungen im 95%-Quantil ersichtlich. Aufgrund der geringen Zahl an Autonomen Systemen in Uruguay sind dort längere Pfade für 25%, d.h. Änderungen am 75%-Quantil, zu verzeichnen. Bei genauerer Analyse zeigt sich allerdings, dass es sich hierbei nur um Policy-basierte AS-Pfadverlängerungen mittels AS Path Prepending handelt; die Länge der *tatsächlich* durchquerten AS-Pfade ändert sich für beide Länder nur marginal. Dieses Muster deutet auf bestehende, für den Normalbetrieb bewusst weniger attraktiv gestaltete Ausweich-Routen hin, die bei Ausfall der Haupt-Routen automatisch zum Einsatz kommen. In Bezug auf Brasilien und Paraguay sind dagegen keinerlei Änderungen festzustellen. Zusammenfassend ist demnach für die vom Stromausfall nicht unmittelbar betroffenen Autonomen Systeme in den betrachteten Ländern von keiner wesentlichen Beeinträchtigung der internationalen Verbindungsqualität auszugehen.

2.2.2.3 Analyse der Data Plane

Ein dienstnäherer Betrachtungswinkel für die Auswirkungen des Stromausfalls ergibt sich aus der Analyse von IP-basierten Messungen. Zu diesem Zweck können alle über die RIPE ATLAS Messinfrastruktur verfügbaren IP-Pfadmessungen (90.831.316 Datensätze) und Ping-Messungen (285.480.577 Datensätze) im Betrachtungszeitraum für die betroffenen Länder ausgewertet werden. In diesen Daten finden sich 4.299.099 IP-Pfadmessungen und 7.057.779 Ping-Messungen mit Bezug zum vorliegenden Ausfall. Die Verteilung von Messzielen wird dabei durch die Infrastruktur der Plattform selbst und in geringerem Maße auch von dessen Nutzern festgelegt und ist demnach prinzipiell nicht gleichverteilt. Für diese Netzbereiche können die verfügbaren Daten jedoch nicht zuletzt aufgrund deren großen Umfangs nützliche Einblicke in praktische Konsequenzen des Ausfalls liefern.

Alle Ergebnisse beziehen sich analog zum Vorgehen für die Control Plane zunächst nur auf IPv4, bei wesentlichen Abweichungen werden entsprechende Hinweise für IPv6 aufgenommen. Alle IPv4/IPv6-Ergebnisse lassen sich (über die nachfolgende Analyse hinaus auch weiter parametrisier- und filterbar) auf der interaktiven Projekt-Webseite abrufen.

Pfadanalyse Über eine Analyse aller vorfallsbezogenen IP-Pfadmessungen werden mögliche Auswirkungen auf Messziele und Messquellen in den betrachteten Ländern untersucht. Änderungen an Pfadlängen können dabei auf Verkehrsumleitungen sowie Router- oder Netzausfälle hinweisen. Im Folgenden werden zunächst eingehende Messungen weltweit verteilter Messstandorte zu den betroffenen Ländern analysiert (Abb. 2.26).

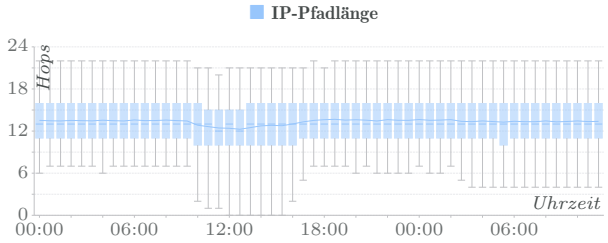


(a) Argentinien (b) Brasilien

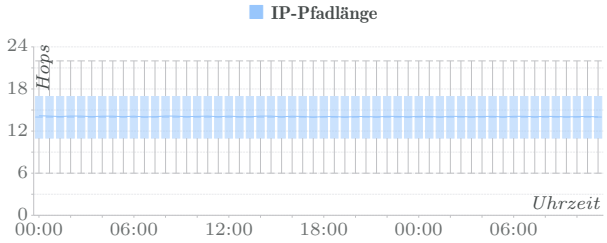
(c) Uruguay (d) Paraguay

Abbildung 2.26: [I2] **Pfadlängen**, betroffene Messziele (Data Plane)

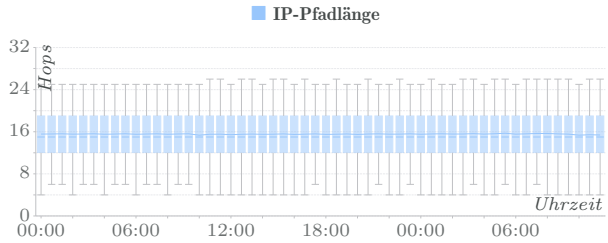
Für das Zielland Paraguay sind im Betrachtungszeitraum keine IP-Pfadmessungen über RIPE ATLAS vorhanden. Bei den verbleibenden Länder zeigen sich keine besonderen Auffälligkeiten. Da entsprechende Messknoten tendenziell eher von einem progressiven und technisch besser ausgestatteten Teil der Netzbetreibergemeinschaft betrieben werden, können ausbleibende Ausfalleffekte in den Daten durchaus auf eine verzerrte Stichprobe zurückzuführen sein. Es ist daher sinnvoll, auch die von den betroffenen Ländern ausgehenden Quellmessungen zu betrachten (Abb. 2.27).



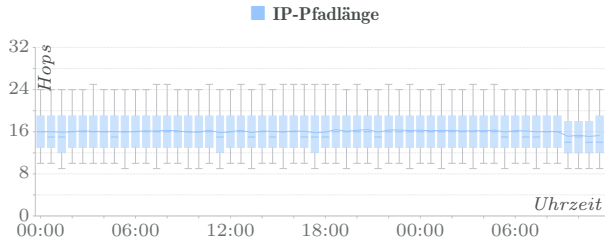
(a) Argentinien



(b) Brasilien



(c) Uruguay

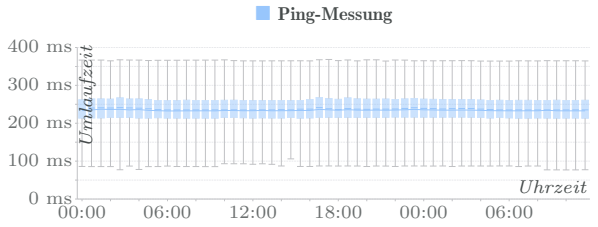


(d) Paraguay

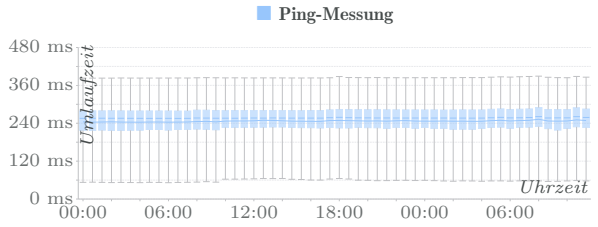
Abbildung 2.27: [I2] **Pfadlängen**, betroffene Messquellen (Data Plane)

In der Tat zeigt sich für ausgehende Messungen aus Argentinien eine deutliche Verkürzung gemessener IP-Pfade im Vorfallszeitraum aufgrund nur mehr unvollständig durchführbarer Messungen. Die Ergebnisse weisen zweifelsfrei auf Ausfälle entlang des Transitpfades hin, zumal eine Verlängerung von IP-Pfaden bei den bis zum jeweiligen Ziel erfolgreichen Messungen nicht auftritt. Im Falle von IPv6-Messungen sind hingegen längere IP-Pfade zu verzeichnen, was auf Routing-Umleitungen hindeutet.

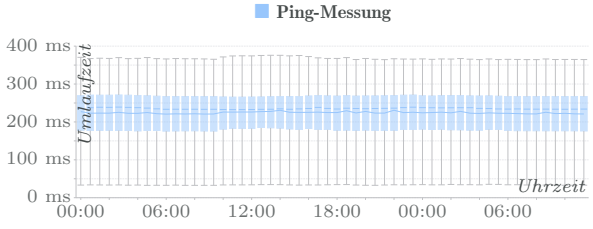
Für Uruguay nehmen Pfadlängen mit Beginn des Stromausfalls nur unwesentlich im 95%-Quantil zu, bei den anderen beiden Ländern sind keine mit dem Ausfall in Zusammenhang stehenden Auswirkungen zu beobachten. Die nachfolgende Analyse von Ping-Umlaufzeiten (Abb. 2.28) wie auch alle weiteren Analysen der Data Plane werden daher nur mehr für Argentinien und Uruguay betrachtet.



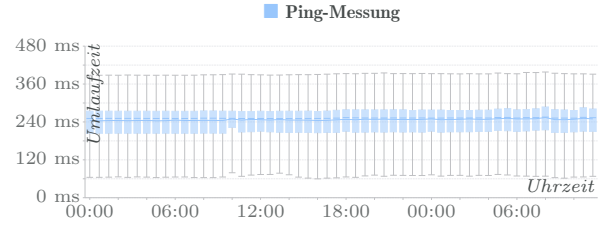
(a) Argentinien, Messziele



(b) Uruguay, Messziele



(c) Argentinien, Messquellen

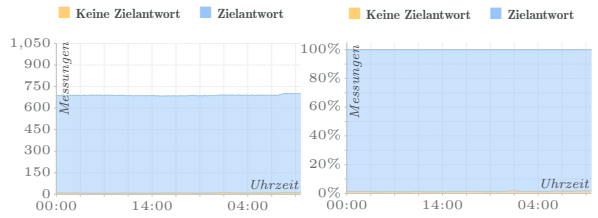


(d) Uruguay, Messquellen

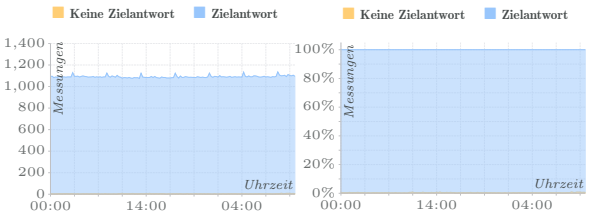
Abbildung 2.28: [I2] **Ping-Messungen**, Umlaufzeit (Data Plane)

Für die beiden betroffenen Länder sind in 25% aller ein- und ausgehenden IPv4/IPv6-Messungen Latenzzuwächse bei Ende-zu-Ende-Verbindungen von bis zu 10 Millisekunden nachweisbar. Da wie vorangehend geschildert jedoch keine entsprechenden Pfadlängenänderungen für Messungen mit erreichbaren Zielen zu Tage treten, kann von einem gesteigerten Verkehrsaufkommen auf den Transitverbindungen ausgegangen werden.

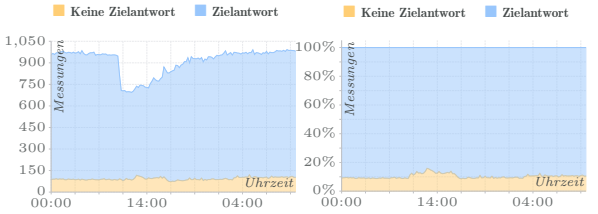
Messanalyse Ein weiterer Blick auf die Konsequenzen des Ausfalls ergibt sich durch eine Gegenüberstellung von durchgeführten und erfolgreichen Messungen (Abb. 2.29).



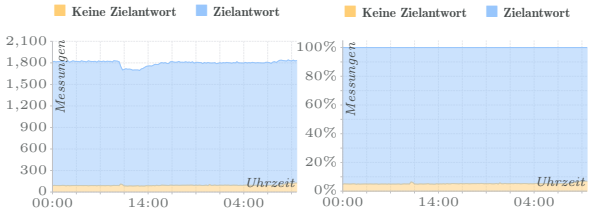
(a) Argentinien, Messziele



(b) Uruguay, Messziele



(c) Argentinien, Messquellen



(d) Uruguay, Messquellen

Abbildung 2.29: [I2] **Messanalyse**, absolut/relativ (Data Plane)

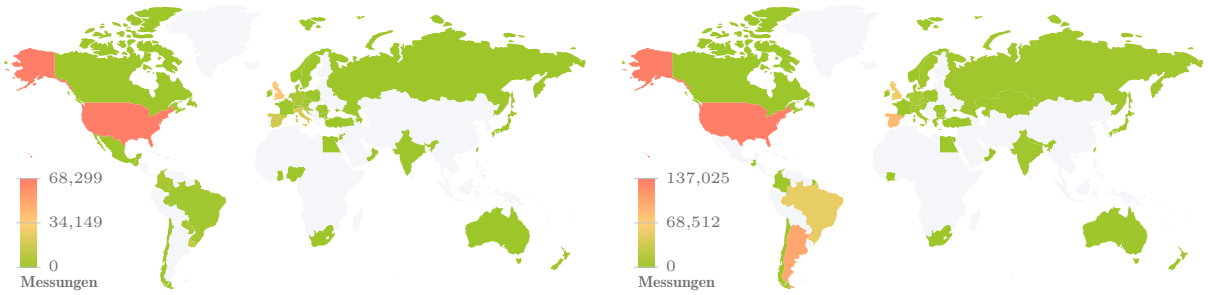
Zunächst lässt sich festhalten, dass die absolute Zahl an eingehenden Messungen, d.h. zu Messzielen in den betrachteten Ländern, um etwa 20% für Argentinien bzw. 40% für Uruguay niedriger liegt als die Zahl der von den jeweiligen Ländern ausgehenden Messungen (Messquellen). Dieser Sachverhalt weist allerdings lediglich auf ein anteilig geringeres Interesse der RIPE ATLAS Nutzer an diesen Ländern hin und hat keinen Einfluss auf die weiteren Betrachtungen. Gleiches gilt für einen konstanten Anteil nicht erfolgreicher Messungen, d.h. Messungen ohne Zielantwort, die sich über den gesamten Analysezeitraum erstrecken und somit nicht in Verbindung zum vorliegenden Stromausfall stehen.

Im Hinblick auf die Menge der zu den betrachteten Ländern hin durchgeführten Messungen zeigen sich keinerlei Auffälligkeiten. Zusammen mit der anteilig geringeren Zahl an Messungen deutet dies erneut auf eine Fokussierung der RIPE ATLAS Messinfrastruktur – und damit entsprechender Messziele – auf herausstehende und technisch versierte Netzbetreiber hin. Die von Argentinien aus durchgeführten Messungen, im Gegensatz dazu mit Messzielen nach mehr regionalen Interessen ausgewählt, zeigen deutliche Einbrüche. Dies gilt sowohl für die Zahl der durchgeführten Messungen selbst, d.h. der Zahl an verfügbaren Messknoten, als auch der Zahl an erfolgreich durchgeführten Messungen.

Für Uruguay sind zwar ebenfalls Messknotenausfälle zu verzeichnen, die Zahl der anteilig erfolgreich durchgeführten Quellmessungen ändert sich dagegen nicht. Eine mögliche Erklärung hierfür kann in einer robusteren Transitanbindung des Landes begründet liegen. Diese Hypothese wird im Folgenden näher untersucht.

Betroffene Länder Für alle IP-Pfadmessungen lassen sich aus den dabei beobachteten Routern auch die an der Weiterleitung beteiligten Transitländer identifizieren. Die

resultierenden Ergebnisse sind aufgrund mehrerer beteiligter Router je Pfadmessung nicht disjunkt, geben aber Aufschluss über die generelle Beschaffenheit der Wegewahl. Die folgende Karte zeigt entsprechende Ergebnisse für Messungen ausgehend von Argentinien und Uruguay (Abb. 2.30), Router im jeweiligen Land selbst werden dabei ausgeblendet.



(a) Argentinien (b) Uruguay

Abbildung 2.30: [I2] **Transitländer**, Messquellen (Data Plane)

Für Argentinien treten US-amerikanische, britische, italienische und spanische Router in der weltweiten Verkehrsweiterleitung hervor. Aufgrund der großen geographischen Distanz zu Argentinien lässt sich – auch unter Berücksichtigung von international agierenden Transitanbietern und Ungenauigkeiten in der IP-zu-Land-Zuordnung – annehmen, dass diese Weiterleitungsländer für Transitverkehr in Südamerika selbst noch keine entscheidende Rolle spielen und überwiegend an interkontinentaler Konnektivität beteiligt sind. Zusammen mit den in Südamerika vernachlässigbaren Transitländern kann demnach auf eine große Beteiligung von argentinischen Autonomen Systemen am Routing des Messverkehrs geschlossen werden. In gleichem Maße muss sich auch der Stromausfall negativ auf Messungen auswirken, was die vorangehenden Beobachtungen bestätigt.

Im Gegensatz dazu zeigt sich für Uruguay auch eine hohe Abhängigkeit von argentinischen und insbesondere brasilianischen Transitverbindungen. Da Brasilien vom Stromausfall nicht betroffen war, scheint eine Umleitung des Messverkehrs über dieses Land – und damit der zuvor beobachtete ausbleibende Effekt – plausibel. Dieser Umstand ergänzt die Perspektive der Control Plane, in der sich nur eine geringe Zahl an Transit- und Topologieänderungen für Uruguay nachweisen ließ.

2.2.2.4 Bewertung und Folgen

Basierend auf den vorangehenden Analysen und Recherchen lassen sich folgende zentralen Ergebnisse für den betrachteten Vorfall festhalten.

Charakteristische Besonderheiten Ein an sich isoliert auftretender Fehler konnte sich aufgrund ungewöhnlicher Gegebenheiten und menschlichem Fehlverhalten über das Starkstromnetz ausbreiten und führte in der Folge zu einem landesweiten Stromausfall. Betroffen waren neben 48 Millionen Einwohnern und zahllosen Firmen auch kritische Infrastruktur wie Wasserversorgung, Festnetz und Mobilfunknetze.

Konsequenzen und Auswirkungen Der Vorfall zeigt eindringlich eine erfolgreiche BGP-Selbstregulierung mit einer verhältnismäßig niedrigen Zahl an ISP- und Netzausfäl-

len. Da die betroffenen Regionen kaum für weltweiten Internet-Transit verantwortlich sind, sind auch keine Konsequenzen für das globale Internet-Routing nachweisbar. Kollateraleffekte für nicht direkt betroffene regionale Netzbetreiber sind ebenfalls vernachlässigbar. Ausfälle und Qualitätseinbußen traten überwiegend in Argentinien auf, jedoch auch hier nicht flächendeckend. Die finanzielle Folgen eines landesweiten Stromausfalles sind ungeachtet der Robustheit des Internets immens. Im Hinblick auf die Stromversorgung selbst unterlagen insbesondere kleine Kraftwerksbetreiber hohem wirtschaftlichen Schaden.

Schutz- und Gegenmaßnahmen Die vorangehende Analyse lässt keine offenkundigen Defizite aus Sicht der Internet-Infrastruktur erkennen, da es weder zu flächendeckenden noch zu langanhaltenden Routing-Ausfällen kam. Die unterschiedlich langen Wiederanlaufphasen hängen nicht zuletzt von individuellen Vorsorgemaßnahmen der einzelnen Betreiber ab, lassen sich aber auch mit der schrittweise wiederhergestellten Stromversorgung begründen. Um weitere Ausfälle dieser Größenordnung zu verhindern, sind besser koordinierte Wartungsarbeiten und eine gewissenhaftere Überwachung und Umsetzung von Schutzmechanismen nötig. Zusätzlich hätten sich Schäden durch einen konsequenten Einsatz von redundanter Stromversorgung für kritische Infrastrukturen mindern lassen, was nicht zuletzt auch als Fehlverhalten der Kraftwerksbetreiber selbst zu werten ist.

Wesentliche Erkenntnisse Die Störungen im Zusammenhang mit dem landesweiten Stromausfall hielten für etwa 12 Stunden an, jedoch waren nur 23% aller Netzbetreiber direkt davon betroffen. Analog zur Stromversorgung konnte auch deren Konnektivität nicht unmittelbar, sondern nur sukzessive wiederhergestellt werden. Mit der endgültigen Behebung des Störfalls fand eine nahezu vollständige Rückkehr des Routings zur Ausgangssituation statt, es kam demnach zu keinen langfristigen Dienststörungen oder strukturellen Verschiebungen der Internet-Anbindung. Es zeigte sich allerdings, dass die Robustheit eines Landes gegenüber flächendeckenden Internet-Ausfällen in hohem Maße abhängig ist von der Diversität der zur Verfügung stehenden Transitverbindungen.

Einschätzung: Ob sich ein Szenario dieses Ausmaßes auch auf Deutschland übertragen lässt, ist fraglich. Durch die dezentrale Stromerzeugung und den ständigen Energieaustausch mit Nachbarländern sowie durch ein robusteres und redundantes Hochspannungsnetz ist nicht mit einem landesweiten Ausfall zu rechnen. Dennoch zeigen Vorfälle in der Vergangenheit, dass auch großflächige Störungen im deutschen Netz möglich sind [2,3]*. In Anbetracht von folgenschweren Fallbeispielen wie der versagenden Notstromversorgung im Rechenzentrum des Betreibers Interxion [I5] stellen jedoch auch isolierte Ausfälle eine große Gefahr für die deutsche Internet-Landschaft dar. Dies gilt in besonderem Maße auch für europäische Nachbarländer, die auf Deutschland als Transitland in nicht unerheblichem Maße angewiesen sind.*

[2] https://www.dw.com/de/blackout-experte-stromausfall-stoppt-nicht-an-deutschen-grenzen/a-46482752
[3] https://www.dw.com/de/droht-auch-in-europa-ein-mega-blackout/a-49238551

2.2.3 Fallstudie: Brand in Kabelschacht bei Korea Telecom

2.2.3.1 Übersicht und Einordnung

Am 24. November 2018 kam es zu anhaltenden Störungen im Netz der Korea Telecom (KT). Diese wurden ausgelöst durch ein Feuer in einer KT-Einrichtung in Seoul [4], in der Kommunikationstechnik für mehrere Stadtteile und umliegende Gebiete betrieben wird.

Vorfallshergang Am 24. November 2018 um 11:12 Uhr Ortszeit (02:12 Uhr UTC) bricht in einer KT-Einrichtung im Stadtteil Ahyeon von Seoul ein Feuer aus. Der Brand konzentriert sich auf einen unterirdischen Kabelschacht und kann aufgrund der schlechten Zugänglichkeit erst um 21:26 Uhr Ortszeit gelöscht werden. In der Folge werden 168.000 Telefonleitungen und 220 optische Kabel zerstört, wodurch Internet, Festnetz, Mobilfunk und IPTV-Dienste der Korea Telecom in mehreren Stadtteilen Seouls und teilweise auch in den umliegenden Gebieten Goyang-si, Gyeonggi-do und Samseong-gu ausfallen. Notfallnachrichten des Fire and Disaster Headquarters werden gegen 12:00 Uhr an betroffene Einwohner versendet, können von KT-Kunden aufgrund des Zusammenbruchs der Telekommunikationsinfrastruktur jedoch nicht mehr empfangen werden. Der Ausfall betrifft darüber hinaus auch Bankautomaten und Kreditkarten-Terminals [5]. Zudem sind mehrere unabhängige Web-Dienste nicht mehr erreichbar, weil Hardware im anliegenden Rechenzentrum durch Hitze und Rauchentwicklung teilweise zerstört wird (Abb. 2.31).

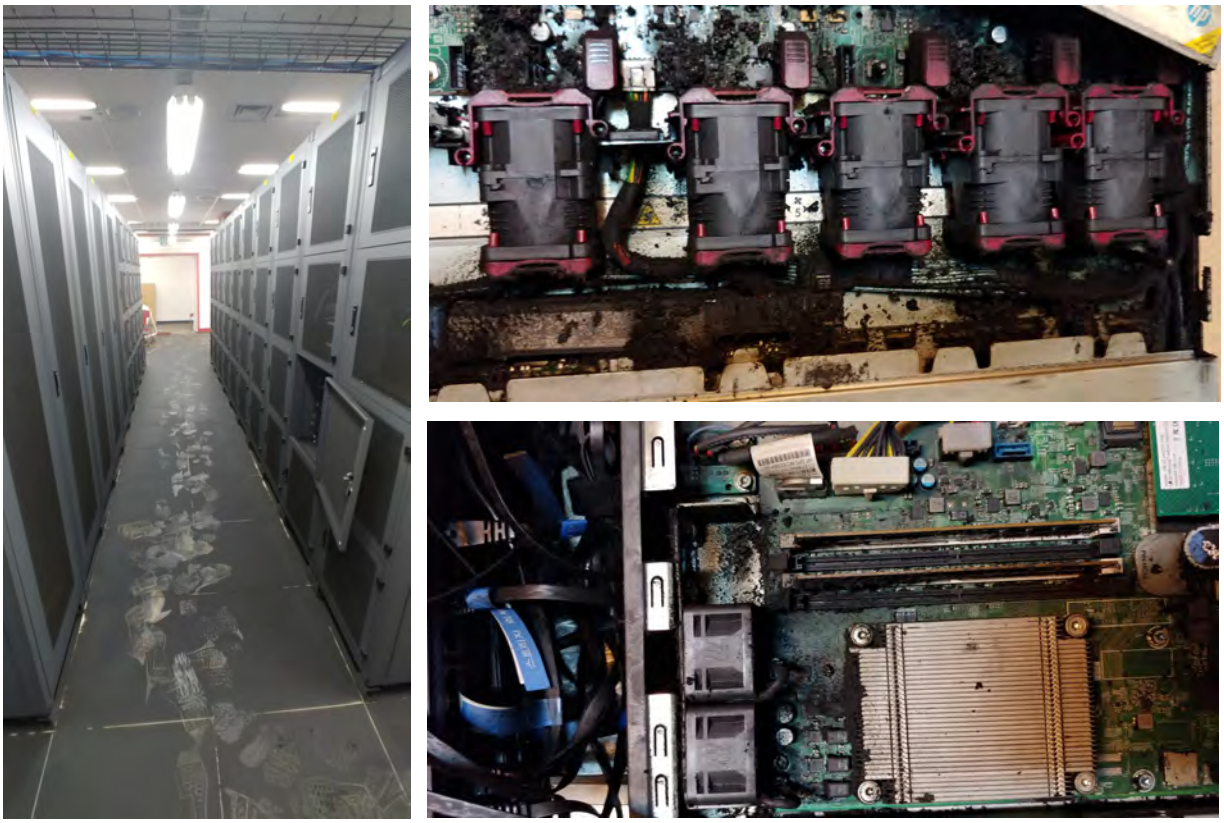


Abbildung 2.31: [I3] **Hardware-Schäden im Rechenzentrum** [17]

[4] Korea Telecom Ahyeon, Chungjeong-ro 3-ga, Seodaemun-gu, Seoul

[5] `http://www.koreaherald.com/view.php?ud=20181125000202`

Der Hauptgrund für die vergleichsweise hohen Auswirkungen des Vorfalls liegt in der regulatorischen Klassifizierung der betroffenen KT-Einrichtung. Telekommunikationseinrichtungen werden in Korea abhängig von verschiedenen Faktoren, u.a. aufgrund deren Wichtigkeit, in die Kategorien A bis D eingeteilt. Diese Klassifizierung bestimmt die erforderlichen Schutzmaßnahmen, die der Betreiber für einen möglichst unterbrechungsfreien Betrieb zu treffen hat. Die Einrichtung in Ahyeon war zum Zeitpunkt des Brandes in Kategorie D eingestuft, wodurch weder Backup-Verbindungen noch Brandschutzmaßnahmen wie Sprinkleranlagen oder Rauchmelder vorgeschrieben waren. Dadurch konnte sich der Brand einerseits lange Zeit unbemerkt ausbreiten, andererseits war keine Möglichkeit zur Überbrückung der beschädigten Kabel vorhanden. Späteren Untersuchungen zufolge wurden im Zuge einer Privatisierung mehrere Einrichtungen zusammengelegt, wodurch eine erneute Klassifizierung zu einer Einstufung in Kategorie C und damit zu den notwendigen Schutzmaßnahmen geführt hätte [6]. Um den Betrieb schneller wiederherzustellen, wurden temporäre Ausweichleitungen oberirdisch verlegt, wodurch bis zum Folgetag 60% der Mobilfunkstationen, 70% der privaten Internet-Anbindungen und 50% der gewerblichen Anschlüsse wiederhergestellt werden konnten.

Direkte Folgen Die vollständige Wiederherstellung des Netzbetriebs dauerte für einen Teil der KT-Kunden noch mehrere Tage an. Den betroffenen Kunden wurde zur Kompensation ein Monat der Gebühren für die ausgefallenen Dienste erlassen, bei anhaltenden Störungen teilweise auch für einen Zeitraum von 3 bis 6 Monaten. Dennoch kam es in der Folge vermehrt zu Anbieterwechseln [7]. Als Folge der fälschlichen Klassifizierung des KT-Standorts wurden viele Telekommunikationseinrichtungen landesweit neu eingestuft, darunter auch der betroffene Standort in Ahyeon [8]. Zu den Brandursachen lagen auch nach mehreren Monate keine belastbaren Erkenntnisse vor, offiziellen Angaben zufolge können Brandstiftung oder andere externe Einwirkungen jedoch ausgeschlossen werden [9].

Verwandte Vorfälle Der Vorfall entspricht mit hoher Dauer und Auswirkung dem Durchschnitt von technischen Defekten (siehe Abschnitt 2.1.2.1), weist aber aufgrund der zentralen Rolle der Korea Telecom für die koreanische Kommunikation und der hohen Bevölkerungsdichte Seouls eine überdurchschnittlich hohe Reichweite auf. Ein weiterer Vorfall dieser Art ereignete sich am 16. November 2015 in Aserbaidschan, als eine wichtige Überlandleitung durch Feuer beschädigt wurde [I12]. Der Brand trat in einem Rechenzentrum des Betreibers Delta Telecom auf, der für die landesweite Anbindung an das globale Internet von großer Bedeutung ist. Durch die starke Marktstellung der Delta Telecom waren bis zu 94% von Aserbaidschan für mehrere Stunden ohne Internet-Verbindung, wobei auch hier die Auswirkungen durch fehlendene Ausweich-Routen verstärkt wurden.

Wissenschaftliche Arbeiten Zum aktuellen Zeitpunkt ist nur eine Studie bekannt, die sich mit der Ausbreitung von Bränden in Kabelschächten beschäftigt und dabei Bezug zum vorliegenden Fall der Korea Telecom nimmt [18]. Weitere Arbeiten beschäftigen sich mit der Flammenausbreitung in Wartungstunneln [19, 20] sowie geeigneten Mitigationsmöglichkeiten, bspw. einer Löschung mittels Flüssig-Stickstoff [21], oder mit Techniken zur Bekämpfung von Rauch- und Staubentwicklung [22].

[6] https://www.tellerreport.com/life/--kt--ahyeon-branch-after-the-fire-rating-facility--rear-book-adjustment-------%22violation-of-statute%22-.rJJxMgW-E.html

[7] https://www.azertelecom.az/en/news/2015/12/25/23.html

[8] https://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3057793

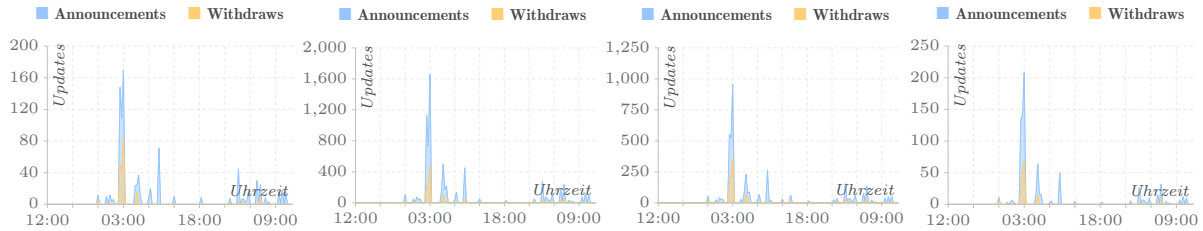
[9] http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=141106

2.2.3.2 Analyse der Control Plane

Anhand einer Analyse von BGP-Tabellen lässt sich untersuchen, ob der Vorfall lediglich lokale Störungen zur Folge hatte, oder ob größere Auswirkungen im globalen Internet-Routing nachweisbar sind. Einschlägigen Medienberichten über den Verlauf des Vorfalls zufolge ist nur mit geringen bzw. lokal beschränkten Konsequenzen zu rechnen.

Für die folgenden Auswertungen wird stets der Zeitraum von 24. November 2018 bis 25. November 2018 jeweils um 12:00 Uhr UTC zugrunde gelegt. Die Analysen basieren auf einem Vergleich der Routing-Tabellen mehrerer BGP-Kollektoren, d.h. der Sicht der Deutschen Telekom (DTAG) sowie von RouteViews Singapore (RV-SG), Sydney (RV-SYDNEY) und Japan (RV-WIDE). Da IPv6 von Korea Telecom im Analysezeitraum nur rudimentär eingesetzt wurde, beschränken sich die folgenden Betrachtungen auf IPv4. Die vollständigen Ergebnisse lassen sich auf der interaktiven Projekt-Webseite abrufen.

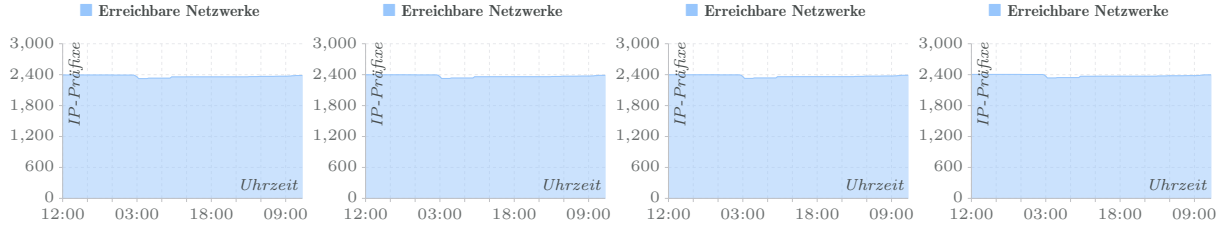
Zielanalyse Zunächst werden global sichtbare Auswirkungen des Brands auf das Netz der Korea Telecom mithilfe einer Analyse von Ziel-Routen untersucht. Im ersten Schritt wird dazu ein Vergleich der BGP-Aktivität der Korea Telecom (AS4766) aus Sicht verschiedener BGP-Standorte vorgenommen (Abb. 2.32).



(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.32: [I3] **BGP-Aktivität**, Zielanalyse (Control Plane)

Qualitativ zeigt sich über alle Standorte hinweg stets das gleiche Aktivitätsbild. Die absoluten Zahlen unterscheiden sich aufgrund individueller Teilnehmerzahlen der öffentlichen BGP-Kollektoren – im Falle der der Deutschen Telekom handelt es sich jedoch um genau eine Routing-Sicht und damit um aussagekräftige Absolutwerte. Der vorliegende Brand spiegelt sich an allen Standorten zweifelsfrei in der weltweiten BGP-Aktivität wieder. Allerdings sind bereits gegen 06:00 Uhr UTC (15:00 Uhr Lokalzeit) weitere Routing-Änderungen ersichtlich, d.h. wenige Stunden nach dem Ausfall und noch vor Beendigung der Löscharbeiten. Eine weitere Häufung von Änderungen fällt zusammen mit der Wiederinbetriebnahme größerer Teile der Infrastruktur (00:00 Uhr UTC). Die Betrachtung der erreichbaren IP-Präfixe während des Vorfalls gibt darüber Aufschluss (Abb. 2.33).

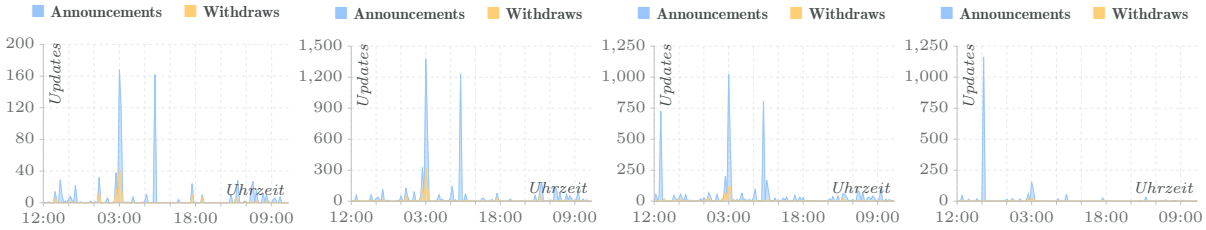


(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.33: [I3] **IP-Präfixe**, Zielanalyse (Control Plane)

Die Auswirkungen des Brands im Netz der Korea Telecom beschränken sich auf etwa 2,9% dessen IP-Präfixe. Bezogen auf dessen Gesamtzahl an gerouteten IP-Adressen in der Größenordnung eines /7-Netzwerks ist der Ausfall in Summe mit einem /18-Netzwerk (0.05%) wenig bedeutsam. Zudem zeigt sich gegenüber dem 24-stündigen Ausfall der Telekommunikation in Seoul bereits nach 8 Stunden eine teilweise Wiederherstellung von Netzbereichen der Korea Telecom ab 10:00 Uhr UTC bzw. 19:00 Uhr Ortszeit, was auf einen kurzfristigen Aufbau von Ausweich-Routen hindeutet. Der (nahezu) vollständige Wiederanschluss aller ausgefallenen IP-Präfixe steht im Einklang mit öffentlichen Bekanntmachungen zu größeren Reparaturfortschritten und zur beobachteten BGP-Aktivität.

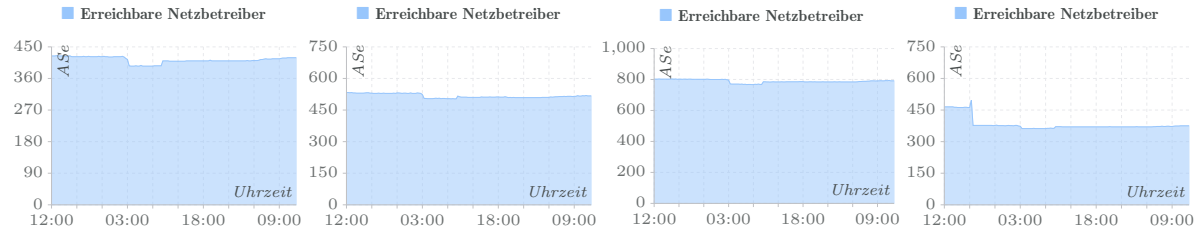
Transitanalyse Im Folgenden werden weitere Auswirkungen des Brands auf das Transitverhalten der Korea Telecom untersucht, wodurch auch Kollateralschäden für umliegende Regionen betrachtet werden können. Hierzu wird zunächst wieder die BGP-Aktivität von unterschiedlichen Standorten aus analysiert (Abb. 2.34).



(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.34: [I3] **BGP-Aktivität**, Transitanalyse (Control Plane)

Für alle betrachteten BGP-Kollektoren zeigt sich ein ähnliches Ausfall- und Wiederherstellungsmuster wie im Falle der vorangehenden Zielanalyse. Daraus lässt sich schließen, dass die Korea Telecom auch für Transitkunden eine schnelle Mitigation noch vor der vollständigen Brandlöschung umsetzen konnte. Die hervortretende Aktivitätsspitze bei RV-WIDE (Japan) tritt einige Stunden vor dem Brand zu Tage und erscheint demnach davon unabhängig. Weitere Details hierzu werden in der nachfolgenden Auswertung des Transitverhaltens für Autonome Systeme ersichtlich (Abb. 2.35).

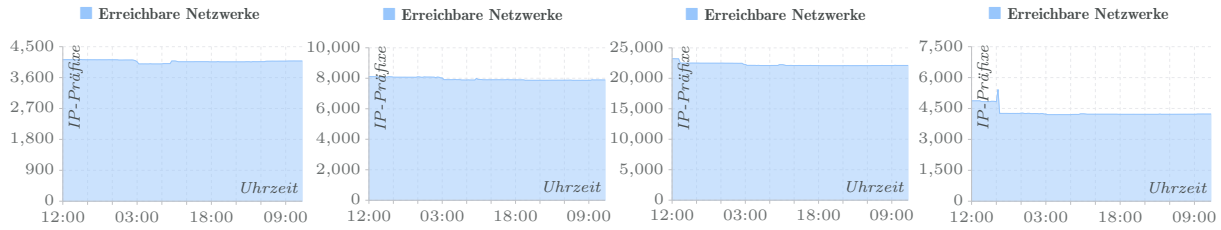


(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.35: [I3] **Autonome Systeme**, Transitanalyse (Control Plane)

Die Bedeutsamkeit der Korea Telecom als Transitanbieter in der globalen Routing-Tabelle variiert naturgemäß in Abhängigkeit des betrachteten BGP-Kollektors. Aus Sicht von RouteViews Sydney sind etwa 800 Autonome Systeme über die Korea Telecom an das Internet-Routing angeschlossen, hingegen verzeichnen die anderen Kollektoren nur etwa die Hälfte davon. Unabhängig von der absoluten Zahl an erreichbaren Autonomen Systemen bewegt sich der Transitausfall über Korea Telecom in der Größenordnung von

6,8% (LW-DTAG) bis 3,5% (RV-WIDE). Die vorangehend diskutierte Routing-Aktivität bei RV-WIDE führte allerdings bereits kurz vor dem Brand zu einer nicht erklärbaren Umleitung von ca. 100 Autonomen Systemen (23,3%). Aus Sicht der betroffenen Transit-IP-Präfixe ergibt sich ein dazu vergleichbares Bild (Abb. 2.36).

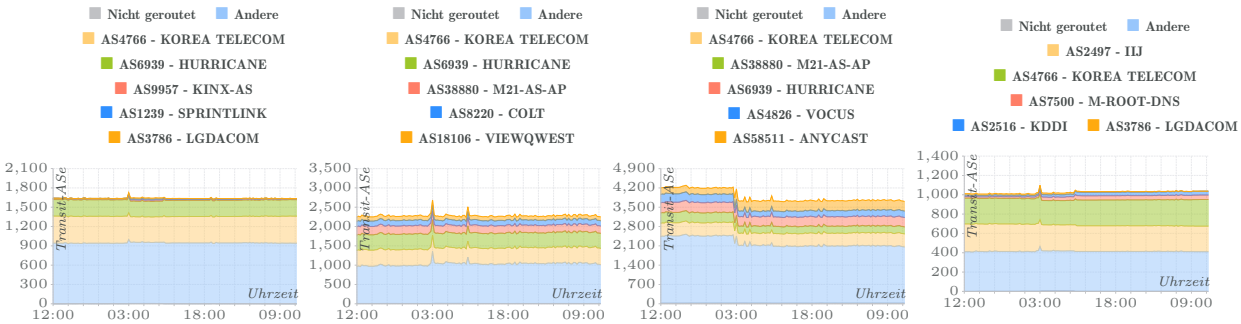


(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.36: [I3] **IP-Präfixe**, Transitanalyse (Control Plane)

Die Zahl der durch den Brand umgeleiteten IP-Präfixe bewegt sich zwischen 3,5% (LW-DTAG) und 0,3% (RV-WIDE), für letzteren weitere 14,3% der Transit-IP-Präfixe kurze Zeit vor Vorfallsbeginn. Die Menge der insgesamt betroffenen IP-Adressen liegt in der Größenordnung eines /15- bis etwas weniger als einem /17-Netzwerk.

Änderungsanalyse Um die Konsequenzen der beobachteten Routing-Änderungen zu quantifizieren, werden im Folgenden weiterführende Analysen aller Transitpfade und Topologieänderungen für die vom Kabelbrand betroffenen Netzbereiche vorgenommen. Zunächst lässt sich hierzu die Zusammensetzung der an der Weiterleitung auf Transitpfaden beteiligten Autonomen Systeme näher betrachten (Abb. 2.37).

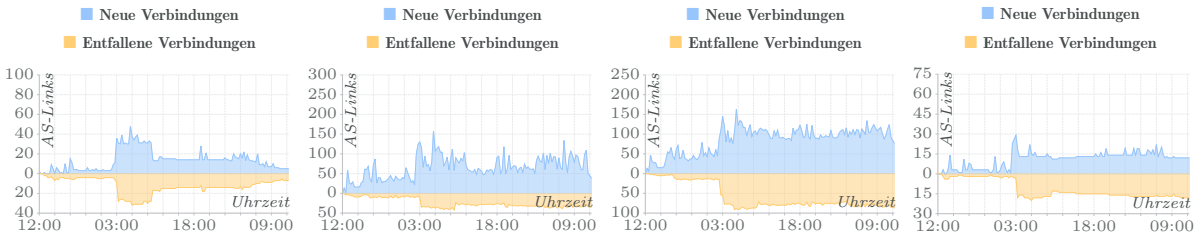


(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.37: [I3] **Transitverlauf**, Transit-ASe nach Ziel-ASen (Control Plane)

Je nach gewähltem BGP-Standort ergeben sich deutlich unterschiedliche Transitverläufe. Aus Sicht der Deutschen Telekom ändert sich das Verhältnis der wichtigsten beteiligten Transit-ASe (Hurricane und Korea Telecom) zunächst nicht, lediglich in den ersten Stunden des Brandes werden kleinere Teile der betroffenen Netzbereiche über SprintLink, LG UPlus und den koreanischen Exchange Point KINX geleitet. Vom RouteViews-Standort Singapore aus werden die Ausfälle im Netz der Korea Telecom über zahlreiche unabhängige Autonome Systeme kompensiert, so dass sich die Zusammensetzung der wichtigsten Transit-ASe ebenfalls nur unwesentlich ändert. Ausfallzeitpunkt und Gegenmaßnahmen sind durch einzelne Spitzen, die die Pfadänderungen und deren Konvergenz in BGP repräsentieren, klar zu erkennen.

Aus Sicht von Sydney verschiebt sich das Transitverhältnis zugunsten des Anbieters Anycast Networks, während weniger Verkehr über die Netzbetreiber Vocus und M21 abgewickelt wird. Eine Rückkehr zum ursprünglichen Routing nach Vorfallsende ist nicht zu erkennen. Über den Kollektor RV-WIDE in Japan ist eine Verschiebung von Transit-Routen hin zu KDDI und dem WIDE-Projekt selbst zu beobachten, weniger Routen sind ab dem Brandzeitpunkt dagegen über die Internet Initiative Japan (IIJ) sichtbar. Diese kurzfristig realisierten Mitigationsmaßnahmen werden im weiteren Verlauf stabilisiert und noch ausgebaut, eine Rückkehr zum ursprünglichen Routing ist auch hier nicht zu verzeichnen. Dieses Verhalten lässt sich auch am Topologieverlauf ablesen (Abb. 2.38). *Hinweis:* Da sich alle Änderungsanalysen auf das Routing zu direkt betroffenen Netzbereichen der Korea Telecom beschränken, sind die für RV-WIDE vorangehend beschriebenen Transit-Auffälligkeiten im Folgenden nicht ersichtlich.



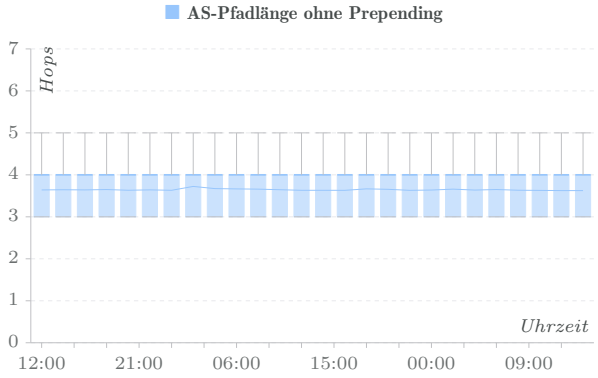
(a) LW-DTAG (b) RV-SG (c) RV-SYDNEY (d) RV-WIDE

Abbildung 2.38: [I3] **Topologieverlauf**, AS-Links (Control Plane)

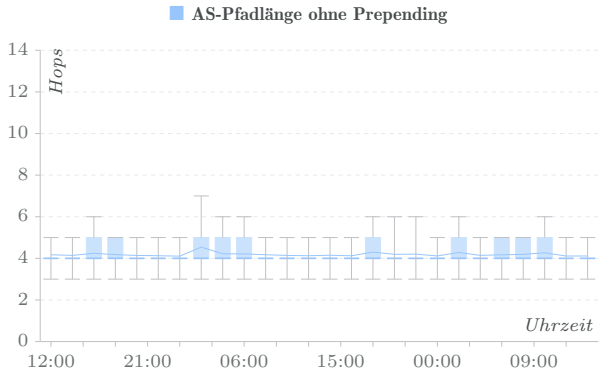
Aus Sicht der Deutschen Telekom werden während der ersten 7 Stunden des Vorfalls temporäre AS-Verbindungen für die Überbrückung ausgefallener AS-Links etabliert, die mit Voranschreiten der Reparaturarbeiten allmählich zurückgebaut werden. Die Routing-Tabellen der Standorte RV-SG und RV-SYDNEY beinhalten ebenfalls kurzlebige neue Verbindungen, zum größeren Teil bleiben neue Verbindungen aber auch nach der Störungsbehebung bestehen und werden weiter ausgebaut. Für den Standort Japan (RV-WIDE) bleibt die Zahl neuer AS-Links dagegen während und nach dem Vorfall konstant.

Pfadanalyse Im Folgenden werden die beschriebenen Transit- und Topologieänderungen hinsichtlich ihrer Auswirkungen auf zugehörige AS-Pfadlängen untersucht, um so mögliche Qualitätseinbußen durch längere Pfade abschätzen zu können (Abb. 2.39).

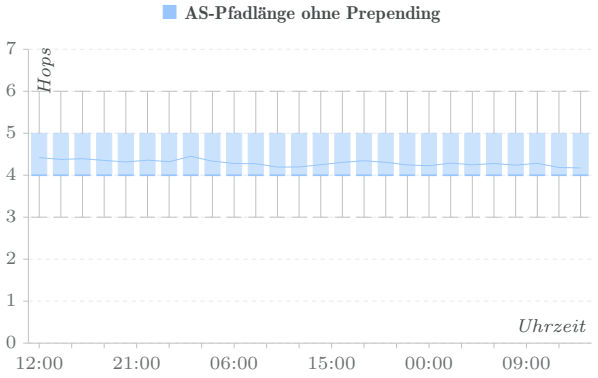
Für die Standorte LW-DTAG und RV-SYDNEY ändern sich die AS-Pfadlängen während des Vorfalls nur unwesentlich, so dass hier nicht auf eine Verschlechterung der Verbindungsqualität geschlossen werden kann. Im Falle von RV-WIDE sind dagegen Pfadverlängerungen unmittelbar zum Zeitpunkt des Brandes erkennbar. Diese betreffen jedoch nur das 95%-Quantil, d.h. nur 5% aller beobachtbaren AS-Pfade zum Netz der Korea Telecom, und kehren nach kurzer Zeit wieder zur Ausgangssituation zurück. Auch hier kann demnach nur von minimalen Störungen ausgegangen werden. Am Standort Singapore treten mehrmals deutliche Änderungen der Pfadlängen auf, jedoch sind diese Änderungen über den gesamten Betrachtungszeitrum verteilt und stehen daher vermutlich nicht in unmittelbarem Zusammenhang zum vorliegenden Vorfall. Einzig im Zeitpunkt des Brandes ist analog zu RV-WIDE eine größere Abweichung der Pfadlängen im 95%-Quantil zu erkennen. Zusammenfassend können demnach keine nennenswerten Pfadverlängerungen für das globale Routing zu den betroffenen Netzbereichen der Korea Telecom nachgewiesen werden. Netzinterne Qualitätseinbußen bleiben allerdings möglich und auch zu erwarten.



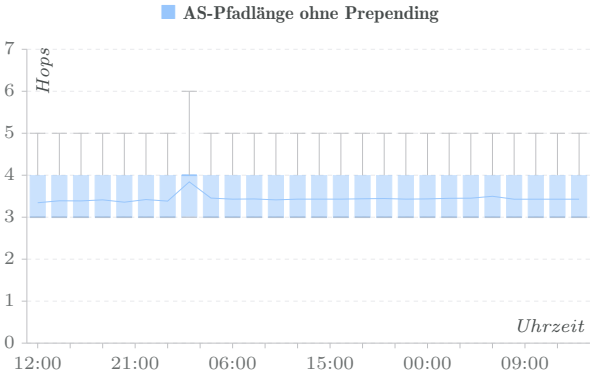
(a) LW-DTAG



(b) RV-SG



(c) RV-SYDNEY



(d) RV-WIDE

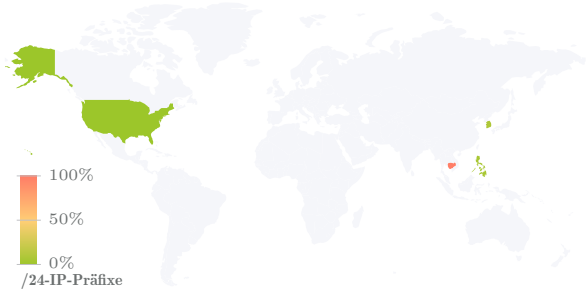
Abbildung 2.39: [I3] **Pfadanalyse**, ohne Prepending (Control Plane)

Betroffene Länder Die vorangehend diskutierten Topologieänderungen geben Einblicke in direkt betroffene Netze, lassen aber keine Rückschlüsse auf kollaterale Effekte zu. Inbesondere können Pfadänderungen auch unbeteiligte, über Korea Telcom an das Internet angebundene Netzbereiche betreffen. Im Folgenden werden daher die von der Korea Telecom weggeleiteten IP-Bereiche nach betroffenen Ländern dargestellt (Abb. 2.40).

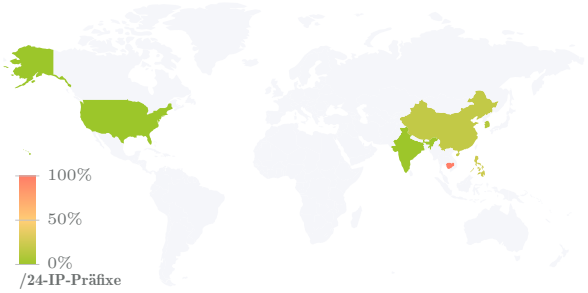
Aus Sicht der Deutschen Telekom wird das Äquivalent von 149 /24-Netzwerken nicht mehr über Korea Telecom geroutet, davon befinden sich 138 Netzwerke in Süd Korea. Bei den weiteren Standorten führt der Ausfall zu größeren Umleitungen in Asien, insbesondere müssen zahlreiche, bisher über Korea Telecom erreichbare chinesische Netzbereiche über andere Transitanbieter umgeleitet werden. Im Fall von RV-SYDNEY betrifft dies 1,1% aller chinesischen IP-Präfixe bzw. IP-Adressen in der Größenordnung eines /11-Netzwerks.

2.2.3.3 Analyse der Data Plane

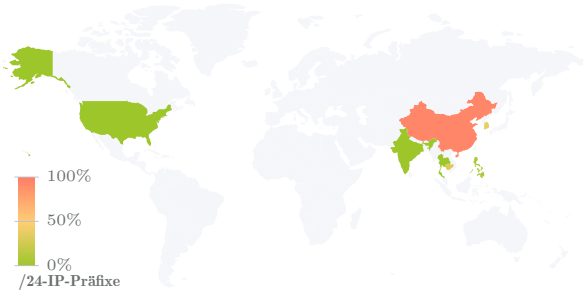
Über die RIPE ATLAS Messinfrastruktur wurden im Betrachtungszeitraum insgesamt 76.147.825 IP-Pfadmessungen und 224.755.542 Ping-Messungen durchgeführt. Daraus konnten 79.202 bzw. 118.828 Messungen mit direktem Bezug zu Süd Korea identifiziert werden. Keine dieser Messungen führte allerdings in das Land bzw. das Netz der Korea Telecom, es sind ausschließlich ausgehende Messungen (durch dort betriebene ATLAS-Messknoten) verfügbar. IPv6-Messungen wurden nur in vernachlässigbarem Maße durchgeführt. Alle folgenden Analysen beschränken sich auf diese Datenlage.



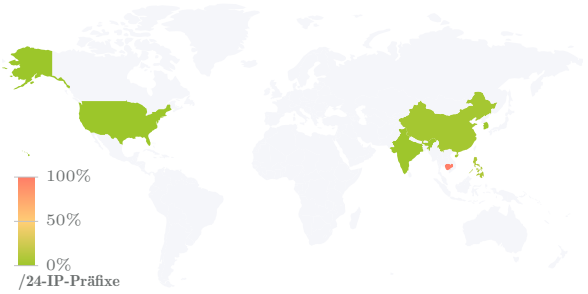
(a) LW-DTAG



(b) RV-SG



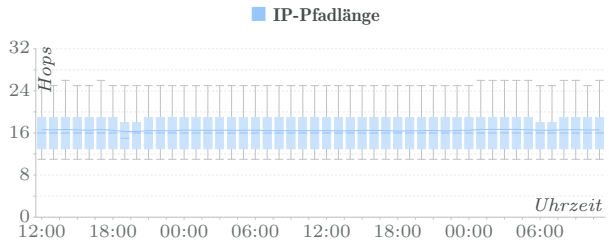
(c) RV-SYDNEY



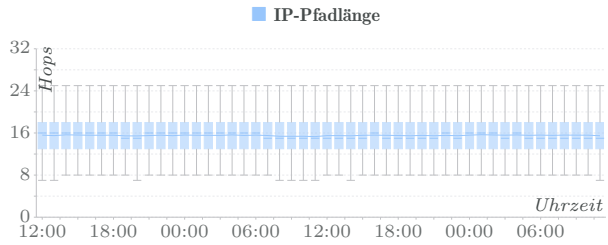
(d) RV-WIDE

Abbildung 2.40: [I3] **Betroffene Länder**, Routing-Änderungen (Control Plane)

Pfadanalyse Ein Maß für mögliche Beeinträchtigungen der Data Plane stellen Änderungen von IP-Pfadlängen und Umlaufzeiten dar. Im Folgenden werden daher Pfadlängen aller ausgehenden IP-Messungen dargestellt (Abb. 2.41). Es zeigen sich keinerlei Auffälligkeiten während des Brandzeitraumes, weder für ATLAS-Messknoten in Süd Korea noch für Messknoten im Netz der Korea Telecom. Auch eine Betrachtung entsprechender Ping-Messungen liefert keine Hinweise auf überregionale Qualitätseinbußen. (Abb. 2.42).

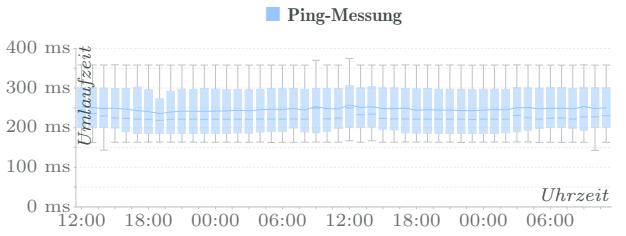


(a) Korea Telecom

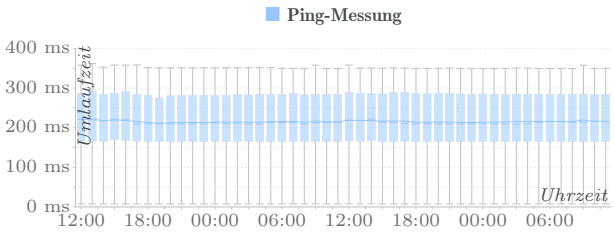


(b) Süd Korea

Abbildung 2.41: [I3] **Pfadlängen**, Messquellen (Data Plane)



(a) Korea Telecom

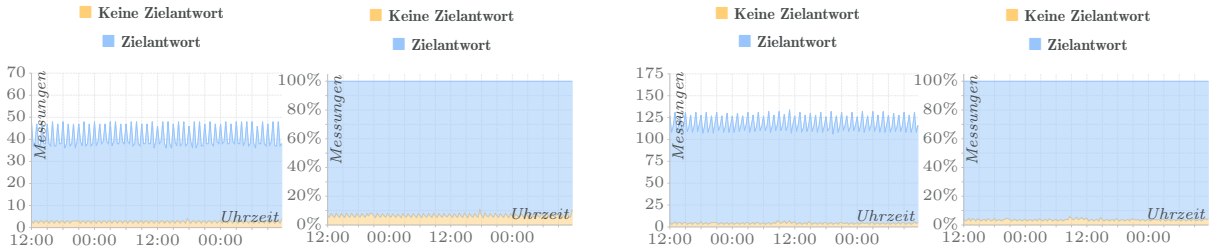


(b) Süd Korea

Abbildung 2.42: [I3] **Ping-Messungen**, Messquellen (Data Plane)

Die Auswertungen zeigen keinen Latenzanstieg, der in Zusammenhang mit brandbedingten Netzausfällen gebracht werden könnte, da sich sichtbare Schwankungen über den gesamten Betrachtungszeitraum erstrecken. Ausbleibende Effekte des Brandes auf die IP-Messungen können einerseits durch die geringe Anzahl an relevanten Messungen und insbesondere durch eine willkürliche Verteilung der RIPE ATLAS Messknoten erklärt werden. Andererseits legen die Ergebnisse aber auch nahe, dass die Brandschäden in Seoul lediglich zu lokalen Ausfällen und regionalen Beeinträchtigungen führten.

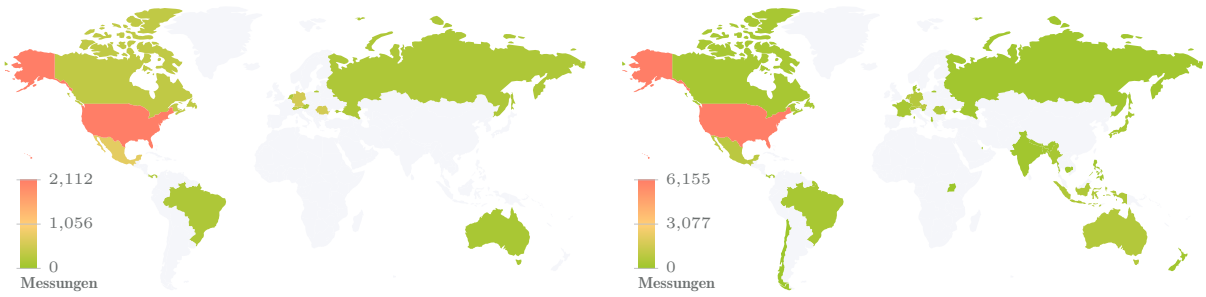
Messanalyse Neben den betrachteten Pfadeigenschaften können auch Anzahl und Erfolgsrate der durchgeführten Messungen analysiert werden (Abb. 2.43). Hier zeigt sich erwartungsgemäß sowohl für Messungen aus dem Netz der Korea Telecom als auch für ganz Süd Korea, dass die Anzahl durchgeführter wie auch der Anteil erfolgreicher Messungen keinen Änderungen unterliegen, die sich auf den Brand zurückführen ließen. Sichtbare regelmäßige Schwankungen spiegeln lediglich die Natur der periodischen ATLAS-Messungen wider und stehen nicht in Zusammenhang mit dem Vorfall. Auch diese Analyse verdeutlicht den lokal begrenzten Charakter des Brandes.



(a) Korea Telecom (b) Süd Korea

Abbildung 2.43: [I3] **Messanalyse**, Messquellen, absolut/relativ (Data Plane)

Betroffene Länder Zuletzt wird die geographische Verteilung der vermessenen IP-Ziele untersucht (Abb. 2.44). Dabei zeigt sich, dass vorrangig nordamerikanische und europäische Ziele vermessen wurden. Aus dem Netz der Korea Telecom sind insbesondere keine asiatischen Ziele zu verzeichnen, auch aus Süd Korea ist nur eine geringe Zahl vorhanden. Auffällig ist zudem, dass in beiden Fällen keine chinesischen Ziele vermessen wurden. In der Analyse der Control Plane wurde dagegen deutlich, dass sich vorfallsbedingte Routing-Änderungen überwiegend auf Süd Korea selbst sowie auf Transit-Routen nach China beschränken. Für einen Nachweis von regional begrenzten Dienststörungen ist die Datenlage der RIPE ATLAS Messinfrastruktur daher unzureichend.



(a) Korea Telecom (b) Süd Korea

Abbildung 2.44: [I3] **Zielländer**, Messquellen (Data Plane)

2.2.3.4 Bewertung und Folgen

Basierend auf den vorangehenden Analysen und Recherchen lassen sich folgende zentralen Ergebnisse für den betrachteten Vorfall festhalten.

Charakteristische Besonderheiten Der Ausfall wurde durch eine regulatorische Fehleinstufung ermöglicht, wodurch gesetzlich vorgeschriebene Schutzmaßnahmen für kritische Infrastruktur in der betroffenen Einrichtung nicht umgesetzt wurden und sich ein unterirdischer Brand unbemerkt entwickeln konnte. Die Analyse der Control Plane zeigt, wie durch zielgerichtete Mitigation seitens der Korea Telecom langanhaltende Internet-Störungen mit Hilfe von eilig aufgebauten Ausweichverbindungen noch während des Brandes vermieden werden konnten. Eine vollumfängliche Bewertung von Dienstausfällen in der Data Plane ist aufgrund der unzureichenden Datenlage schwierig, was unter anderem im geringen Messaufkommen der RIPE ATLAS Messinfrastruktur in Süd Korea und den lokal begrenzten Auswirkungen des Vorfalls begründet liegt.

Konsequenzen und Auswirkungen Laut Medienberichten und späteren Untersuchungen führte der Brand zum Ausfall von Mobilfunk, Festnetz und Internet in über 210.000 Haushalten. In einigen Bereichen von Seoul waren Notrufe und Kreditkartenzahlungen nicht mehr möglich und öffentliche Einrichtungen in ihrer Funktion gestört (darunter auch 28 militärische Kommunikationspfade). Es entstand Sachschaden in geschätzter Höhe von $7 Millionen, zudem wurde die Korea Telecom zu $27,5 Millionen Schadensersatz verpflichtet. Die Analyse der Control Plane offenbart weitere Auswirkungen auf Transit-Routen durch Süd Korea, die zum Teil auch nach den Bränden fortbestehen.

Schutz- und Gegenmaßnahmen In der Folge des brandbedingten Ausfalls fand eine landesweite Neueinstufung kritischer Telekommunikationsinfrastruktur durch die südkoreanische Regierung statt. Dadurch wurden mehrere ISPs verpflichtet, deren Einrichtungen mit Überwachungs- und Löschsystemen auszurüsten. Zudem sind für wichtige Kommunikationsleitungen redundante Systeme vorzuhalten, um Ausfallzeiten zukünftig zu verkürzen. Die Korea Telecom kündigte Investitionen in Höhe von $426,6 Millionen an.

Wesentliche Erkenntnisse Der Betreiber begann bereits während der Löscharbeiten mit einer Netzmigration und konnte damit wenige Stunden nach dem Brand alle betroffenen Netzbereiche wiederherstellen. Dennoch kam es standortabhängig zu längerfristigen Dienstausfällen und ferner auch zu Transitänderungen im globalen Internet-Routing, deren Ursachen sich trotz der zeitlichen Nähe zum Brand nicht unmittelbar darauf zurückführen lassen. Die unzureichende Datenlage im Hinblick auf aktive Messungen legt den zukünftigen Aufbau von Messstandorten auch für entlegene Regionen nahe.

Einschätzung: Ähnlich gelagerte Fälle treten durchaus auch in Deutschland auf [10,11] *und führen immer wieder zu tausenden betroffener Kunden. Analog zu Süd Korea existieren zwar Gesetze*[12] *und Verordnungen*[13] *zum Schutz kritischer Infrastruktur, jedoch wird darin keine kontinuierliche Überwachung von Betreibern und Einrichtungen veranlasst. Daher muss auch in Deutschland mit Fällen größeren Ausmaßes gerechnet werden.*

[10] https://www.teltarif.de/brand-telekom-telefon-internet-ausfall-jena/news/52257.html

[11] https://www.sueddeutsche.de/muenchen/benzin-ueber-kabel-geschuettet-erneut-brandanschlag-auf-datenleitungen-1.4730864

[12] https://www.gesetze-im-internet.de/bsig_2009/__8a.html

[13] https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf

2.2.4 Fallstudie: Schweizer Route Leak über China Telecom

2.2.4.1 Übersicht und Einordnung

Am 6. Juni 2019 kommt es zu zahlreichen Störungen bei unabhängigen Online-Diensten. Ausgelöst wurde der Vorfall durch ein Route Leak der Firma Safe Host SA, das sich über die China Telecom weltweit ausbreiten konnte. Ungewöhnlich an diesem Vorfall ist die lange Dauer der Störungen, die über zwei Stunden anhielten.

Vorfallshergang [I59] Am 6. Juni 2019 um 09:43 Uhr UTC beginnt der Schweizer Rechenzentrumsbetreiber Safe Host laut Medienberichten[14] damit, bis zu 70.000 BGP-Routen versehentlich an den Transit-Provider China Telecom zu annoncieren. Aufgrund fehlender Schutzmechanismen aufseiten der China Telecom werden die Routen übernommen und verbreiten sich über deren BGP-Verbindungen weltweit. Viele der Routen von Safe Host werden von weiten Teilen des Internets bevorzugt, darunter auch zu IP-Präfixen des Messenger-Dienstes WhatsApp (Abb. 2.45). Das durch die Umleitung hervorgerufene stark erhöhte Verkehrsaufkommen bei Safe Host und der China Telecom führt zu Router-Überlastungen, Qualitätseinbußen und schließlich zu Ausfällen für die betroffenen Netzbereiche. Um 10:30 Uhr UTC normalisiert sich die Lage, jedoch tritt von 12:10 Uhr UTC bis 13:13 Uhr UTC ein weiteres Route Leak auf, das erneut zu Ausfällen führt[15]. Laut Safe Host wurde vor den Route Leaks keine Konfigurationsänderung an eigenen BGP-Routern vorgenommen. Allerdings wurde eine Unregelmäßigkeit in deren Forwarding Information Base festgestellt, die die eingesetzten Routen-Filter auf Basis von IP-Präfix-Listen beeinflusst haben könnte[16]. Seitens der China Telecom sind keine Stellungnahmen bekannt.

Abbildung 2.45: **Topologie des Route Leaks**[15]

Direkte Folgen Während des Route Leaks waren viele Web-Dienste für längere Zeit nicht oder nur eingeschränkt erreichbar, da Datenpakete von betroffenen Kunden zu diesen Diensten über das Netz des Verursachers geleitet wurden, das auf eine derart hohe Zunahme der Verkehrslast naturgemäß nicht ausgelegt war. Medienberichten zufolge wirkten sich die Störungen dabei überwiegend auf mobiles Internet im europäischen Raum aus. Durch die Verwicklung der China Telecom und insbesondere aufgrund der Schwere der

[14] https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom

[15] https://blog.thousandeyes.com/whatsapp-disruption-just-one-symptom-of-broader-route-leak/

[16] https://twitter.com/swisscolo/status/1138418158698663937

Ausfälle zog der Vorfall zwar eine große mediale Aufmerksamkeit nach sich. Auch wurde die China Telecom als international agierender Transit-ISP für den fehlenden Einsatz von BGP-Filtern und eine unverhältnismäßig lange Reaktionszeit öffentlich kritisiert [17]. Darüber hinausgehende Konsequenzen für die Beteiligten sind allerdings nicht bekannt.

Verwandte Vorfälle Der vorliegende Fall gleicht in seiner Reichweite und Auswirkung anderen Route Leaks, liegt aufgrund einer mittleren Dauer jedoch über dem Durchschnitt der meist kurz anhaltenden Vorfälle (siehe Abschnitt 2.1.2.6). Nur wenige Tage nach dem betrachteten Vorfall wurden am 24. Juni 2019 erneut zahlreiche Dienste durch einen Routing-Fehler gestört. Der Vorfall wurde ausgelöst, als der Metallverarbeiter Allegheny Technologies BGP-Routen seines Transit-Providers DQE an Verizon weiterleitete [I58]. Auch in diesem Fall wurden die Routen aufgrund fehlender Filtermaßnahmen weltweit verbreitet und betrafen populäre Dienste wie Amazon und Cloudflare. Durch die ausbleibende Reaktion seitens Verizon dauerte der Vorfall ebenfalls ungewöhnlich lange an und konnte letztlich erst in Zusammenarbeit mit dem Verursacher DQE behoben werden.

Wissenschaftliche Arbeiten Aufgrund des regelmäßigen Vorkommens von Route Leaks und dem damit verbundenen großen Schadenspotential für die Internet-Infrastruktur finden in diesem Umfeld nach wie vor zahlreiche Forschungsarbeiten statt. In mehreren Studien werden häufige Ursachen von Route Leaks aufgearbeitet oder eine Klassifikation verschiedenartiger Vorfälle vorgenommen [23, 24]. Ein größerer Teil der Forschung befasst sich mit der Konzeption von automatisierten Systemen, die Routing-Anomalien frühzeitig erkennen sollen [25, 26, 27], um herkömmliche (meist manuelle) Reaktionsmechanismen zu ergänzen. Darüber hinaus wurden auch verschiedene Präventionsmaßnahmen vorgestellt [28, 29, 30]. Es sind allerdings keine quantitativen Studien bekannt, die die durch Route Leaks entstandenen wirtschaftlichen Schäden näher beziffern.

2.2.4.2 Analyse der Control Plane

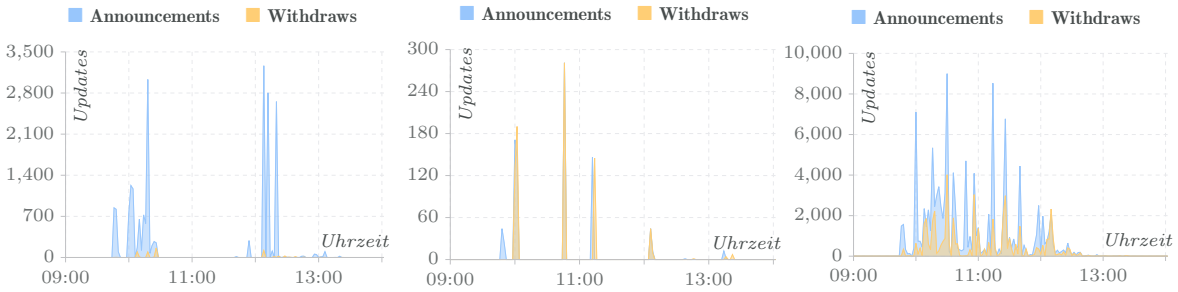
Da Route Leaks generell auf fehlerhaft angewandten BGP-Mechanismen beruhen, sollte sich der vorliegende Fall lückenlos mit Analysen der Control Plane nachvollziehen lassen. Durch eine Auswertung von mehreren BGP-Kollektoren können explizite Auswirkungen auf unterschiedliche ISPs sowie deren netzlokale Filtermaßnahmen verglichen werden. Daraus ergeben sich auch Aussagen über die Reichweite des Vorfalls, d.h. der Internet-weite Anteil betroffener Endanwender wird abschätzbar. Den nachfolgenden Analysen liegen BGP-Tabellen von AS3320 (LW-DTAG) und AS174 (LW-COGENT) als Vertreter internationaler Tier1-Provider sowie eines öffentlichen RouteViews-Kollektors (RV-OREGON4) mit einer aggregierten Routing-Sicht zahlreicher kleinerer ISPs zugrunde.

Für alle Auswertungen wird stets ein Zeitraum am 06. Juni 2019 von 09:00 Uhr UTC bis 14:00 Uhr UTC zugrunde gelegt. Es werden ausschließlich Routen zu Netzbereichen untersucht, die im Betrachtungszeitraum von dem Route Leak betroffen waren, d.h. für zeitweise über Safe Host (AS21217) geroutet wurden. Da im Route Leak keine IPv6-Routen annonciert wurden, beschränken sich die folgenden Betrachtungen auf IPv4. Die vollständigen Ergebnisse lassen sich auf der interaktiven Projekt-Webseite abrufen.

[17] https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/

Zielanalyse Im vorliegenden Fall tritt Safe Host als Verursacher des Route Leaks hervor. Durch fälschliche Routen-Annoncierungen werden weltweite Verkehre zu dessen Netzbereiche umgeleitet, wo eine Weiterleitung zu den jeweiligen Verkehrszielen aufgrund schnell wachsender Überlast nicht mehr sichergestellt werden kann. Die Netzbereiche von Safe Host selbst sind von diesen Routing-Änderungen allerdings nicht unmittelbar betroffen und im Hinblick auf das Route Leak nicht weiter von Bedeutung. Eine explizite Zielanalyse für Safe Host verspricht daher keine Erkenntnisse über den Ablauf des Vorfalls. Stattdessen wird der Analysefokus auf Änderungen am Weiterleitungsverhalten und insbesondere die hiervon betroffenen Drittnetze im weltweiten Internet-Routing gelegt.

Transitanalyse Mit Hilfe einer Analyse der Transitänderungen von Safe Host lassen sich explizite Auswirkungen sowie die Reichweite der fehlerhaften BGP-Announcements in der globalen Routing-Tabelle untersuchen. Hierzu kann zunächst die BGP-Aktivität von AS21217 in Bezug auf Transit-Routen näher betrachtet werden (Abb. 2.46).

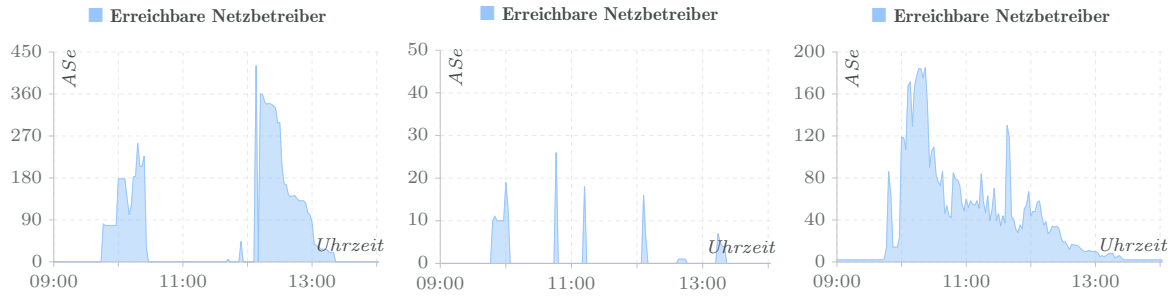


(a) LW-COGENT (b) LW-DTAG (c) RV-OREGON4

Abbildung 2.46: [I59] **BGP-Aktivität**, Transitanalyse (Control Plane)

Als reiner Rechenzentrumsbetreiber sind über das Autonome System von Safe Host keine Transit-Routen zu erwarten, was durch fehlende BGP-Aktivität vor und nach dem Vorfall bestätigt wird. Hingegen ist ein starker Anstieg der Transitaktivität im Vorfallszeitraum über alle untersuchten Standorte hinweg mit einer Gesamtdauer von etwa 2 Stunden zu erkennen. Von LW-COGENT aus betrachtet lassen sich zwei separate Spitzen unterscheiden (gegen 10:00 Uhr und 12:00 Uhr), was im Einklang zu Medienberichten bzgl. zweier aufeinanderfolgender Route Leaks steht. Verglichen mit LW-DTAG ist eine deutlich höhere Zahl an empfangenen Announcement-Nachrichten (etwa um Faktor 10) bei gleichzeitig geringerer Zahl an Withdraw-Nachrichten hervorzuheben. Daraus lässt sich schließen, dass im Netzbetrieb der Deutschen Telekom weit effektivere Routen-Filter zum Einsatz kommen und deren eigenes Netz – wie auch deren Transitkunden – in deutlich geringerem Maße von Route Leaks betroffen sind. Die hohe Anzahl und gleichmäßigere Verteilung von BGP-Updates am Standort RV-OREGON4 lässt sich einerseits durch eine große Zahl von Peers erklären, die entsprechende Nachrichten in unterschiedlichen Zeitabständen an den Kollektor weitergeben. Andererseits verdeutlicht diese Analyse aber auch eine globale Ausbreitung des Vorfalls. Neben der BGP-Aktivität ist die Anzahl der über AS21217 erreichbaren Autonomen Systeme ein maßgeblicher Indikator für Reichweite und Auswirkungen des Route Leaks auf das globale Internet-Routing (Abb. 2.47).

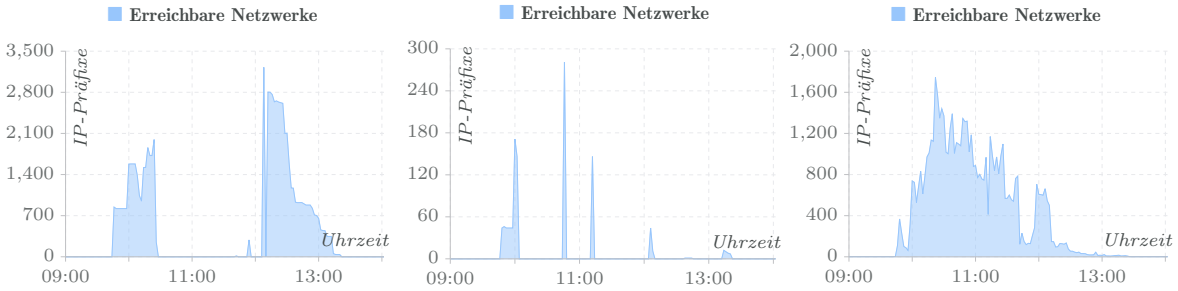
Auch hier zeigt sich für alle betrachteten Standorte ein starker Anstieg der über Safe Host erreichbaren Netzbetreiber. Während vor und nach dem Vorfall keinerlei Transit-Routen über AS21217 zu anderen Autonomen Systeme vorhanden sind, steigt diese Zahl im Verlauf des Route Leaks auf bis zu 420 zeitgleich betroffene Autonome Systeme an.



(a) LW-COGENT (b) LW-DTAG (c) RV-OREGON4

Abbildung 2.47: [I59] **Autonome Systeme**, Transitanalyse (Control Plane)

Aufgrund des fehlenden Transitgeschäfts ist jedoch keine ausreichend dimensionierte Infrastruktur zu erwarten, die den unerwarteten Anstieg des Transitverkehrs im Netz von Safe Host bewältigen könnte. Erneut sind die Auswirkungen des Route Leaks für LW-COGENT am größten, hier kann von einer ungefilterten Sicht auf das Route Leak – und mit über 6.000 direkten Transitkunden von einer enormen Reichweite – ausgegangen werden. Bei LW-DTAG dagegen zeigen sich nur wenige Autonome Systeme vom Route Leak betroffen, der erfolgreiche Einsatz von Filtermaßnahmen der Deutschen Telekom verhindern zum überwiegenden Teil eine Ausbreitung illegitimer Routen-Änderungen. Die aggregierte Sicht mehrerer ISPs bei RV-OREGON4 reicht auch im Maximum nicht an die bei LW-COGENT beobachteten Autonomen Systeme heran. Daraus lässt sich schließen, dass viele dieser ISPs abhängig von deren individueller Wahl an Transitanbietern nur teilweise von dem Route Leak betroffen sind. Gleichzeitig ist aber anzumerken, dass nicht zwangsläufig vollständige Routing-Tabellen an den RouteViews-Kollektor exportiert werden, in der Praxis erfolgt oft eine Beschränkung auf die Untermenge der Kunden-Routen. Ein nahezu identisches Bild ergibt sich für die Zahl der erreichbaren IP-Präfixe (Abb. 2.48).

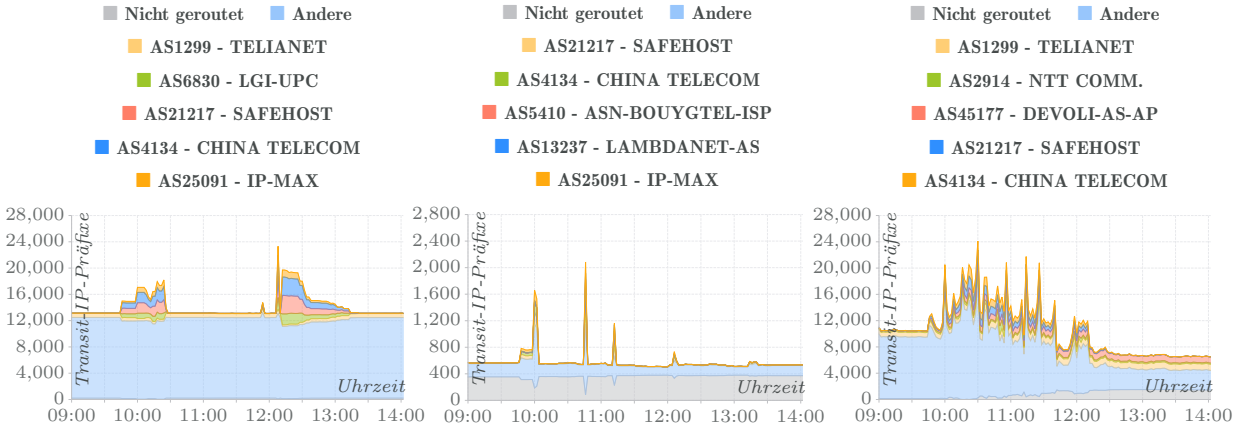


(a) LW-COGENT (b) LW-DTAG (c) RV-OREGON4

Abbildung 2.48: [I59] **IP-Präfixe**, Transitanalyse (Control Plane)

Bei LW-COGENT sind zeitweise bis zu 3.200 IP-Präfixe über Safe Host erreichbar, was in Summe einem IP-Äquivalent von 90.000 /24-Netzwerken bzw. mehr als einem /8-Netzwerk entspricht. Medienberichte von bis zu 70.000 betroffenen IP-Präfixen können anhand der verfügbaren Datenlage jedoch nicht bestätigt werden. Entweder wurde auch hier eine /24-Zählweise zugrunde gelegt, oder durch eine direkte BGP-Verbindung mit der China Telecom weitere Routen beobachtet, die sich aufgrund eines Filtereinsatzes bei dessen Peers nicht weltweit ausbreiten konnten. Da Cogent allerdings eine eigene BGP-Verbindung zur China Telecom unterhält und darüber hinaus ein direkter Vergleich mit LW-DTAG keinen Filtereinsatz nahe legt, erscheint dies weniger wahrscheinlich.

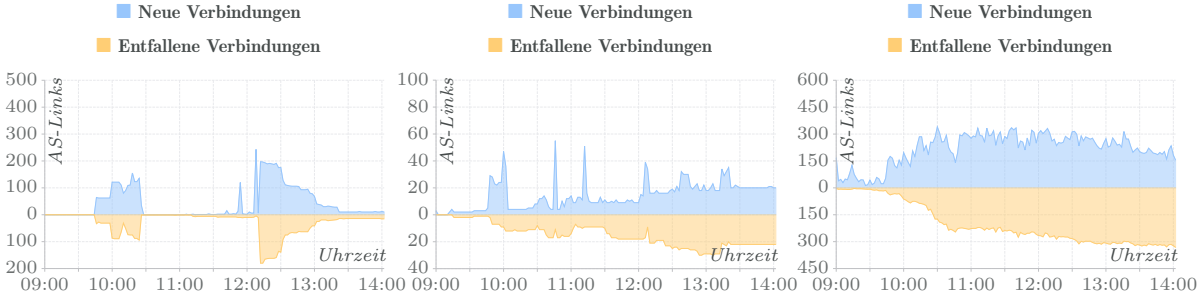
Änderungsanalyse Um Ablauf und Auswirkungen des Route Leaks besser einordnen zu können, werden im Folgenden Transit- und Topologie-bezogene Änderungen während des Vorfalls näher untersucht. Dazu erfolgt zunächst eine Betrachtung der an der Weiterleitung zu den betroffenen IP-Präfixen beteiligten Autonomen Systeme (Abb. 2.49).



(a) LW-COGENT (b) LW-DTAG (c) RV-OREGON4

Abbildung 2.49: [I59] **Transitverlauf**, Transit-ASe nach IP-Präfixen (Control Plane)

Wie zu erwarten ist für Safe Host und die China Telecom ein signifikanter Anstieg an Transit-Routen zu verzeichnen. Ein kleinerer Teil dieser Routen propagiert dabei nicht bzw. nicht nur über China Telecom, in geringem Maße sind auch der Tier1-ISP Telia (AS1299) und der Schweizer ISP IP-MAX (AS25091) sowie weitere kleine Netzbetreiber beteiligt. Zudem sind mehrere Hundert IP-Präfixe mit der Gesamtgröße eines /11-Netzwerks von dem Route Leak betroffen, die vor bzw. nach dem Vorfall nicht in der globalen Routing-Tabelle sichtbar sind und somit erst durch das Route Leak im Internet geroutet werden. Insbesondere für LW-DTAG bezieht sich ein Großteil aller Routen-Änderungen auf diese IP-Präfixe, was darauf hindeutet, dass die Filter der Deutschen Telekom für ungeroutete Netzbereiche weniger effektiven Schutz bieten. Gleichzeitig ist durch das Route Leak für diese IP-Präfixe jedoch kaum mit Störungen zu rechnen, da sie auch bei regulärem Routing nicht erreichbar sind. Interessanterweise nimmt bei RV-OREGON4 die Zahl der nicht erreichbaren IP-Präfixe mit Abklingen des Route Leaks bis zur Größenordnung eines /8-Netzwerkes zu, auch sind dort dauerhafte Änderungen an der Zusammensetzung der Transitanbieter zu verzeichnen. Beide Sachverhalte lassen auf manuelle, weniger zielgerichtete Routing-Eingriffe einzelner Peers zur Mitigation schließen. Eine Betrachtung von Topologieänderungen vervollständigt dieses Bild (Abb. 2.50).

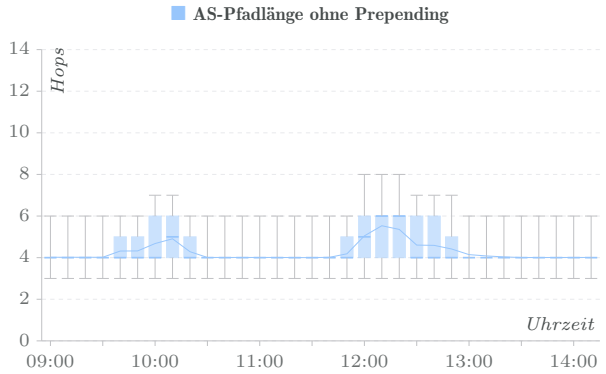


(a) LW-COGENT (b) LW-DTAG (c) RV-OREGON4

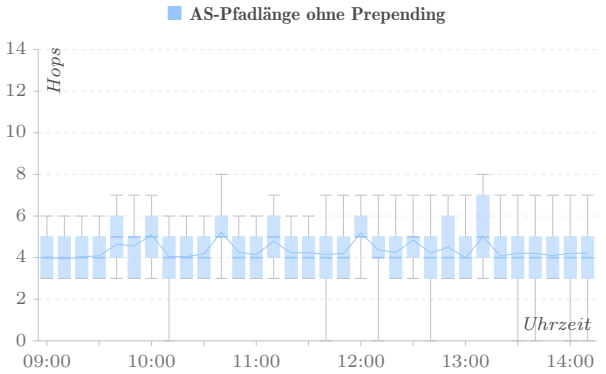
Abbildung 2.50: [I59] **Topologieverlauf**, AS-Links (Control Plane)

An allen Standorten sind während des Vorfalls deutliche Änderungen in der BGP-Topologie erkennbar. Aus Sicht von LW-COGENT beteiligen sich im Maximum knapp 250 neue AS-Verbindungen am Routing zu den betroffenen Präfixen, die nach Vorfallsende jedoch weitestgehend zurückgebildet werden. Dies steht im Einklang zum vorangehend betrachteten Transitverlauf. Im Gegensatz dazu sind bei LW-DTAG nur wenige, dafür aber anhaltende Änderungen sichtbar. Auf Grund der geringen Menge kommen hier jedoch auch reguläre Routing-Änderungen für die betroffenen IP-Präfixe in Frage. Bei RV-OREGON4 sind ebenfalls dauerhafte Änderungen im Topologieverlauf ersichtlich, die sich allerdings auch in obiger Analyse der häufigsten beteiligten Transit-ASe widerspiegeln. Hier ist demnach von vorfallsbezogenen Änderungen auszugehen.

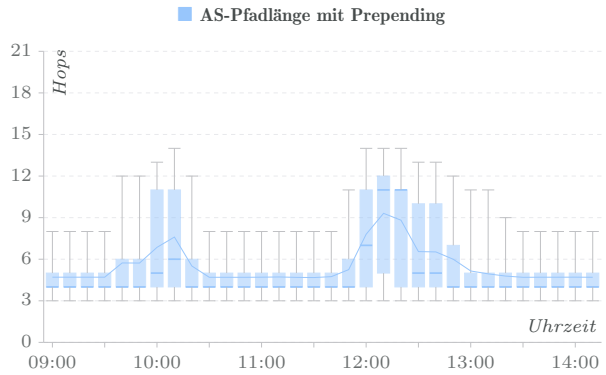
Pfadanalyse Im Folgenden werden weitere Umleitungseffekte des Route Leaks anhand von Änderungen der Pfadlängen für betroffene IP-Präfixe nachvollzogen (Abb. 2.51).



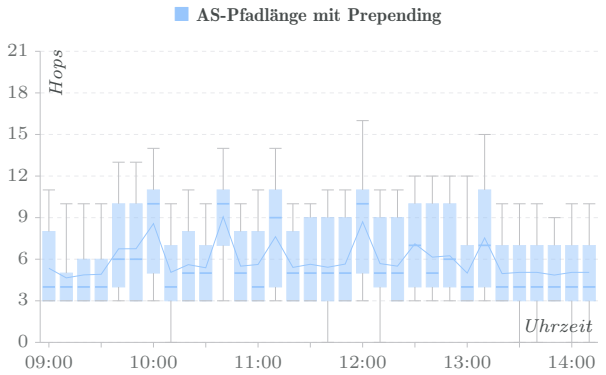
(a) LW-COGENT (ohne Prepending)



(b) LW-DTAG (ohne Prepending)



(c) LW-COGENT (mit Prepending)



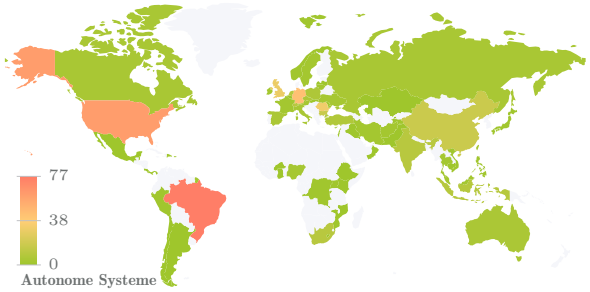
(d) LW-DTAG (mit Prepending)

Abbildung 2.51: [I59] **Pfadanalyse** (Control Plane)

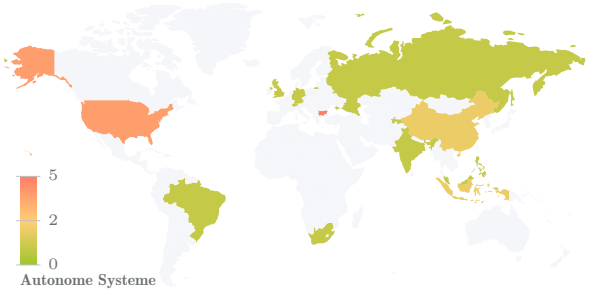
Am Standort LW-COGENT zeigt sich ein signifikanter Anstieg der Pfadlängen, was unmittelbar die über Safe Host und die China Telecom verlängerten Routen widerspiegelt. Unter Berücksichtigung von AS Path Prepending ergeben sich im Median um sieben Hops verlängerte AS-Pfade, da die von Safe Host annoncierten Routen dessen AS sechsfach beinhalten. Dies lässt auf einen fehlerhaften Einsatz von Traffic Shaping schließen, über das Einfluss auf die netzlokale Wegewahl genommen werden kann. Da sich die illegitimen Änderungen allerdings über das gesamte Internet ausbreiten konnten, in BGP aber kürzeste Routen bevorzugt werden, muss im vorliegenden Fall von More Specific IP-Präfixen ausgegangen werden, die sich in der Best Path Selection von BGP auch gegenüber kürzeren

AS-Pfaden durchsetzen. Dieser Umstand weist ebenfalls auf missglücktes Traffic Shaping aufseiten von Safe Host hin. Für LW-DTAG fallen die Änderungen weniger deutlich aus und kehren mit Ende des Route Leaks auch nicht vollständig zum Ausgangszustand zurück, was erneut auf vorfallsunabhängige Routing-Änderungen hindeutet.

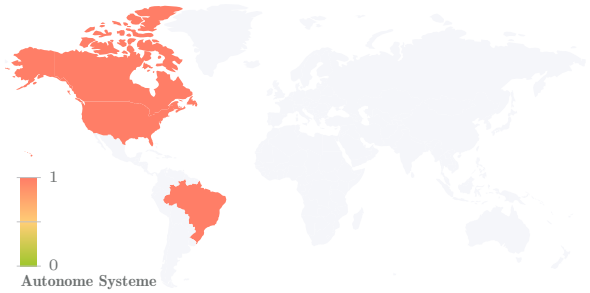
Betroffene Länder Die bisherigen Analysen lassen qualitative Rückschlüsse auf die Reichweite und Auswirkungen des Route Leaks zu. Für eine quantitative Beurteilung ist darüber hinaus eine geographische Betrachtung der betroffenen Netzbetreiber hilfreich. Dazu werden im Folgenden die Ursprungsländer von Autonomen Systemen mit umgeleiteten bzw. neu gerouteten IP-Präfixen über alle Standorte hinweg dargestellt (Abb. 2.52).



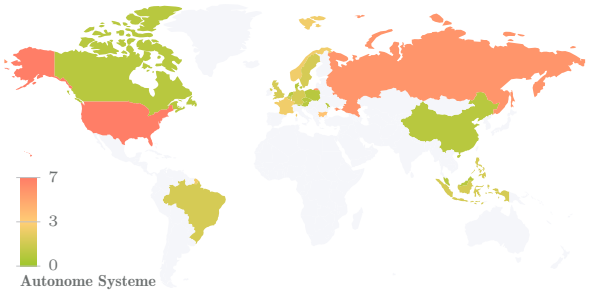
(a) LW-COGENT (hingeleitet)



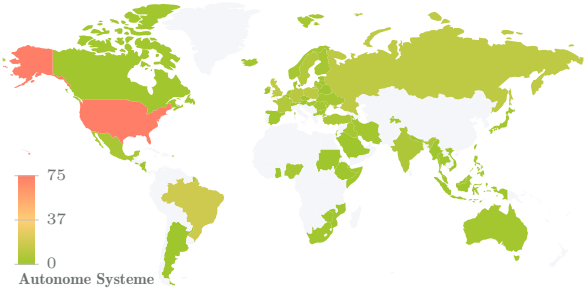
(b) LW-COGENT (neu geroutet)



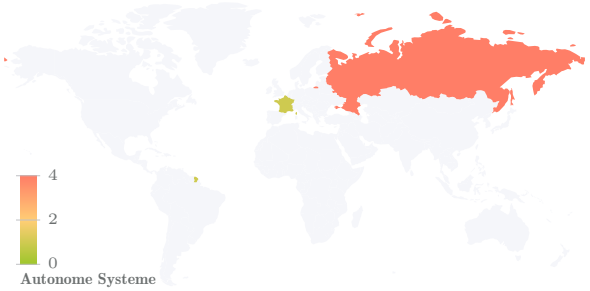
(c) LW-DTAG (hingeleitet)



(d) LW-DTAG (neu geroutet)



(e) RV-OREGON4 (hingeleitet)



(f) RV-OREGON4 (neu geroutet)

Abbildung 2.52: [I59] **Betroffene Länder**, Routing-Änderungen (Control Plane)

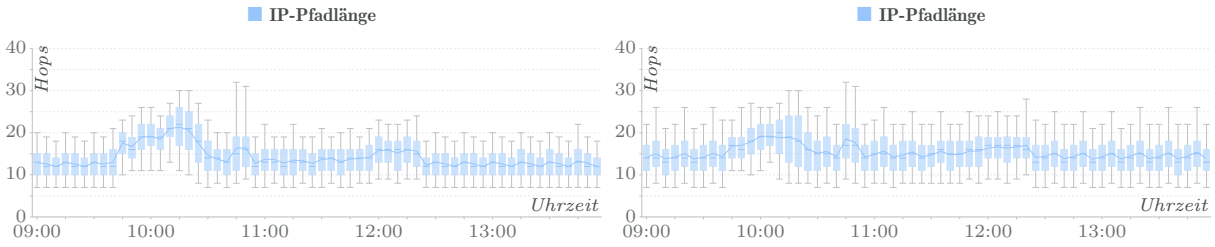
Die vorangehend gewonnene Erkenntnis, dass LW-COGENT und zum Teil auch RV-OREGON4 sehr stark vom Route Leak betroffen sind, zeigt sich auch in der weltweiten Verteilung der zu Safe Host hingeleiteten Autonomen Systeme. Die Verteilungen ähneln sich bis auf wenige Ausnahmen für beide Standorte, wohingegen aus Sicht von LW-DTAG nur drei Netzbetreiber überhaupt den Effekten des Route Leaks unterliegen. Autonome

Systeme mit bisher unerreichbaren, d.h. neu über Safe Host gerouteten IP-Präfixen, lassen sich überwiegend Asien und den USA zuordnen. Hier sind für die verschiedenen Standorte jedoch deutliche Diskrepanzen – allerdings im niedrigen einstelligen Bereich – festzustellen, die auf unterschiedliche Filterstrategien im Umgang mit nicht gerouteten Netzbereichen hindeuten. In den Diagrammen nicht ersichtlich ist die geographische Verteilung der tatsächlich umgeleiteten IP-Adressen. Interessanterweise ergeben sich die größten Auswirkungen (bei LW-COGENT) für australische IP-Präfixe mit einem IP-Äquivalent in der Größenordnung eines /9-Netzwerks, was 26,4% aller landesweit vorhandenen Netzbereiche entspricht. Die größte Zahl an neu gerouteten IP-Adressen ist für die Schweiz und China mit dem IP-Äquivalent eines /11- bzw. /13-Netzwerks zu verzeichnen. Dies entspricht 17,4% aller Schweizer bzw. 0,2% aller chinesischen IP-Präfixe. Die vollständigen Ergebnisse können über die interaktive Projekt-Webseite abgerufen werden.

2.2.4.3 Analyse der Data Plane

Um besser nachzuvollziehen, wie sich die in der Control Plane festgestellten Routing-Änderungen auf die Dienstqualität auswirken, werden im Folgenden aktive IP-Messungen hinsichtlich verschiedener Metriken ausgewertet. Über die RIPE ATLAS Messinfrastruktur wurden im Betrachtungszeitraum insgesamt 12.359.925 IP-Pfadmessungen durchgeführt. Davon konnten 7.212 Messungen mit direktem Bezug zum vorliegenden Route Leak identifiziert werden. Dies umfasst all diejenigen Messungen, für die das vermessene Zielsystem über einen Router von Safe Host oder der China Telecom erreicht wurden. Die resultierenden Pfade über die China Telecom stellen dabei eine Obermenge der Messungen über Safe Host dar. Ping-Messungen wurden aufgrund fehlender Pfadinformationen zur Überprüfung von Verkehrsumleitungen für die folgenden Analysen nicht herangezogen.

Pfadanalyse Eine erste Einschätzung zu den Auswirkungen des Route Leaks auf die Data Plane ist über Pfadanalysen möglich. Dazu werden die mit RIPE ATLAS vermessenen IP-Pfade – sofern deren jeweiliges Messziel erreicht wurde – hinsichtlich Dienstgüte-bezogener Gesichtspunkte ausgewertet, um Beeinträchtigungen für Endanwender zu quantifizieren. Zunächst erfolgt eine Analyse der zugehörigen Pfadlängen (Abb. 2.53).

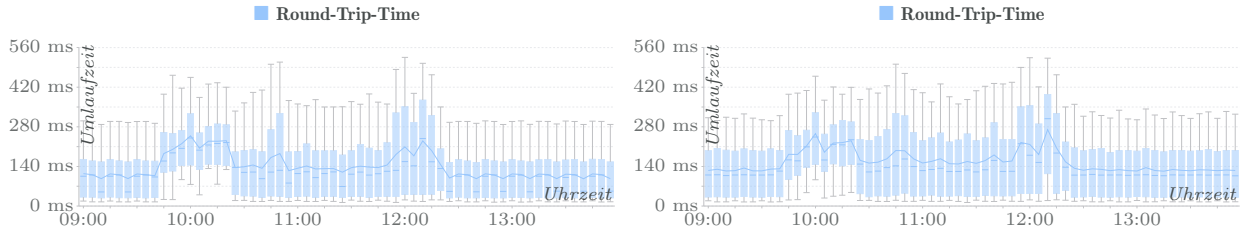


(a) Safe Host (b) China Telecom

Abbildung 2.53: [I59] **Pfadlängen**, Transit-Router (Data Plane)

Die Auswertung zeigt, dass alle vom Route Leak betroffenen Messungen einen signifikanten Anstieg der Pfadlänge verzeichnen. Zeitgleich zum ersten in der Control Plane sichtbaren Route Leak beträgt der Anstieg im 50%-Quantil bis zu 10 Hops über Safe Host bzw. 7 Hops über China Telecom. Pfadverlängerungen während der zweiten BGP-Aktivitätsspitze fallen mit bis zu 4 Hops im Median deutlich geringer aus. Dies lässt

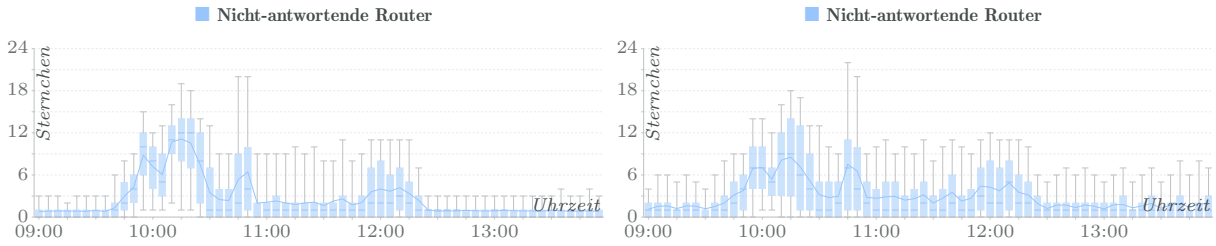
auf aktive Gegenmaßnahmen seitens der an der Weiterleitung beteiligten Netzbetreiber schließen, die bereits mit der ersten Phase des Route Leaks umgesetzt wurden. Nach Vorfallsende fallen die Pfadlängen wieder auf ein normales Maß zurück. Allerdings ist anzumerken, dass auch zwischen den in BGP sichtbaren Spitzen vereinzelt längere IP-Pfade beobachtet werden, was auf höhere Konvergenzzeiten in der Control Plane insbesondere für entlegenere Messstandorte hindeutet. Die erhöhte Anzahl der zu durchquerenden Router weist für sich allein bereits auf eine verminderte Dienstqualität hin. Dies spiegelt sich auch in der folgenden Analyse der gemessenen Umlaufzeiten wider (Abb. 2.54).



(a) Safe Host (b) China Telecom

Abbildung 2.54: [I59] **Pfadlatenzen**, Transit-Router (Data Plane)

Alle über Safe Host umgeleiteten Messungen zeigen einen drastischen Zuwachs der Umlaufzeit um bis zu 100 ms über alle Quantile hinweg, mit einzelnen Spitzen von 500 ms Zuwachs. Auch zwischen den beiden Phasen des Route Leaks sind erhöhte Messwerte im 75%- und 95%-Quantil festzustellen. Erst nach Ende des Route Leaks fallen die Umlaufzeiten wieder auf das Ausgangsniveau zurück. Die Messungen über China Telecom zeigen ein identisches Bild und lassen keine Abweichungen erkennen. Um festzustellen, ob die erhöhten Umlaufzeiten ausschließlich aus der veränderten Topologie oder aus der Überlastung von Transit-Routern entlang des Pfades resultieren, können mit Hilfe einer weiteren Analyse auch Ausfälle auf den Pfaden selbst betrachtet werden (Abb. 2.55).

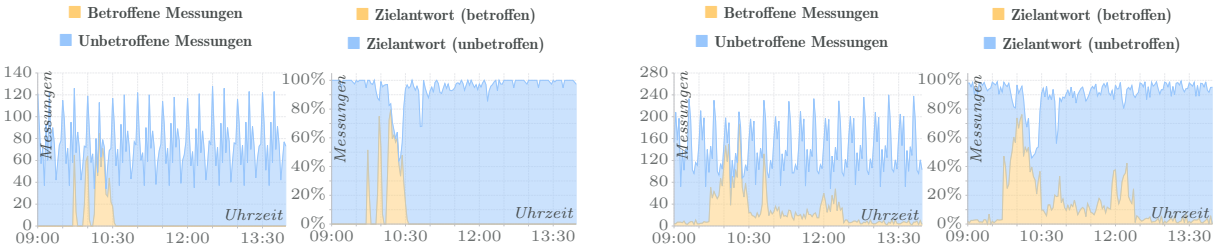


(a) Safe Host (b) China Telecom

Abbildung 2.55: [I59] **Pfadausfälle**, Transit-Router (Data Plane)

Die überaus hohe Zahl an nicht-responsiven Routern über alle vermessenen IP-Pfaden hinweg – in interaktiven Werkzeugen oft mittels Sternchen dargestellt – weist gerade im Vergleich mit der unauffälligen Normalsituation vor und nach dem Route Leak zweifelsfrei auf eine Vielzahl überlasteter Systeme hin. In Relation zu den jeweiligen Pfadlängen ergeben sich bis zu 50% an ausbleibenden Antwortpaketen der durchquerten Transit-Router. Dieses Verhalten lässt sich sowohl für IP-Messungen über Safe Host als auch über China Telecom feststellen, für letztere im Median etwas geringer ausgeprägt. Zusammenfassend ergibt sich aus der Pfadanalyse, dass die durch das Route Leak hervorgerufenen Umleitungen in der Control Plane zu gravierenden Störungen in der Data Plane führten.

Messanalyse Anhand von Pfadanalysen wurden negative Effekte des Route Leaks auf die Verbindungsqualität in der Data Plane nachgewiesen. Dabei blieben Verbindungsausfälle, d.h. Messungen mit ausbleibenden Antworten des Messziels, naturgemäß außer Betracht. Zur Beurteilung von Totalausfällen kann stattdessen die Erfolgsrate aller RIPE ATLAS Messungen mit Bezug zum vorliegenden Fall analysiert werden (Abb. 2.56).

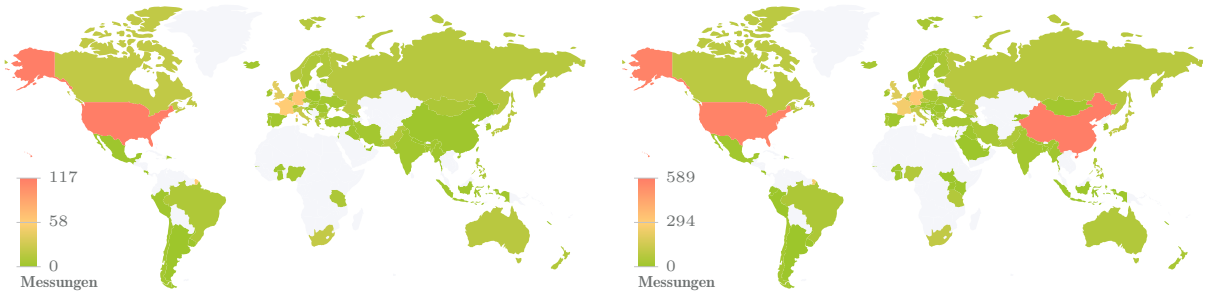


(a) Safe Host (b) China Telecom

Abbildung 2.56: [I59] **Messanalyse**, absolut/relativ, Transit-Router (Data Plane)

Weder bei Safe Host noch bei der China Telecom sind Änderungen in der Anzahl der periodisch durchgeführten Messungen erkennbar, d.h. die betrachteten RIPE ATLAS Messknoten selbst sind (erwartungsgemäß) nicht von den Störungen betroffen. Im Falle der China Telecom zeigen sich über den gesamten Betrachtungszeitraum durchgehend etwa 5-10% an Messungen über deren Netz, wobei es sich um reguläre Messungen der RIPE ATLAS Infrastruktur ohne Bezug zum vorliegenden Fall handelt. Mit Beginn des Route Leaks verzwanzigfacht sich diese Menge. Die Erfolgsrate, d.h. der Anteil an Messungen mit empfangener Zielantwort, bricht auf dem Höhepunkt der ersten Phase dabei um über 50% ein. Dies zeigt eindringlich, dass nicht nur Dienstgüten aufgrund größerer Pfadlängen und höherer Umlaufzeiten beeinträchtigt, sondern betroffene Netzbereiche in großem Umfang unerreichbar wurden. Die etwas niedrigeren Ausfallraten mit Voranschreiten des Route Leaks lassen sich einerseits auf mögliche Einzelmaßnahmen in Transitnetzen zurückführen, andererseits zeigen zu diesem Zeitpunkt auch BGP-Eingriffe der an der Verbreitung des Route Leaks beteiligten ISPs erste Effekte. Insbesondere ist ersichtlich, dass in der zweiten Phase des Route Leaks kein Messverkehr mehr über das Netz von Safe Host geleitet wird, während Umleitungen über die China Telecom nach wie vor stattfinden. Totalausfälle sind in dieser Phase allerdings kaum mehr zu verzeichnen.

Betroffene Länder Um die tatsächliche geographische Reichweite der Störungen in Bezug auf Endanwender zu bewerten, kann stellvertretend eine Länderverteilung der IP-Pfade nach deren RIPE ATLAS Messquellen betrachtet werden (Abb. 2.57).



(a) Safe Host (b) China Telecom

Abbildung 2.57: [I59] **Transitländer**, Messquellen (Data Plane)

Es ist ersichtlich, dass sich das Route Leak in der Tat weltweit ausbreiten konnte, was die Ergebnisse in der Control Plane bestätigt. Häufungen in Europa und Nordamerika spiegeln zwar nicht zwangsläufig ein größeres Maß an Betroffenheit wider, vielmehr ist dort von einer höheren Dichte an RIPE ATLAS Messknoten auszugehen. Gleichzeitig wurde aber bereits in der Control Plane gezeigt, dass Endanwender nur in Einzelfällen durch konsequent filternde Internet-Anbieter geschützt werden konnten.

2.2.4.4 Bewertung und Folgen

Basierend auf den vorangehenden Analysen und Recherchen lassen sich folgende zentralen Ergebnisse für den betrachteten Vorfall festhalten.

Charakteristische Besonderheiten Das Route Leak eines Schweizer Rechenzentrumsbetreibers kann sich durch unzureichende Schutzmaßnahmen über die China Telecom weltweit ausbreiten und führt zu zweistündigen Störungen und Ausfällen zahlreicher populärer Dienste für einen Großteil der Endanwender. Bei genauerer Betrachtung zerfällt der Vorfall in zwei unabhängige Phasen im Abstand von einer Stunde, was auf gravierende Fehler in der Umsetzung erster Mitigationsmaßnahmen hindeutet.

Konsequenzen und Auswirkungen Durch Verkehrsumleitungen über das Netz des Verursachers wird die Verbindungsqualität einer Vielzahl von Diensten, darunter der Messenger-Dienst WhatsApp, massiv beeinträchtigt. Auf dem Höhepunkt des Route Leaks wird jeder zweite Kommunikationsfluss zu betroffenen Netzbereichen unterbrochen. Zum Teil bleiben Topologieänderungen im Internet-Routing auch über den Vorfall hinaus bestehen. Rechtliche oder wirtschaftliche Konsequenzen für die Beteiligten sind nicht bekannt, lediglich Kritik an der China Telecom über unzureichenden Filtereinsatz wurde geäußert.

Schutz- und Gegenmaßnahmen Gegen Route Leaks ist eine Vielzahl von einfachsten Schutzmaßnahmen bekannt. Diese umfassen manuell gepflegte Filterlisten und Routen-Limits sowie automatische Filter basierend auf Einträgen in Internet Routing Registry Datenbanken. Auch wenn derartige Techniken aufgrund einer unvollständigen und sich schnell ändernden Datenlage generell fehleranfällig sind, können Risiko und Tragweite von Route Leaks damit deutlich begrenzt werden. Im vorliegenden Fall wurde laut Verursacher Safe Host zwar eine Filterliste eingesetzt, diese durch einen nicht näher definierten Fehler jedoch deaktiviert. Seitens der China Telecom hätte bereits ein einfaches Routen-Limit das Route Leak vermieden. Selbst bei weit vom Ursprung des Route Leaks entfernten Netzbetreibern machen sich Routing-Filter positiv bemerkbar – so ergab sich für Kunden der Deutschen Telekom im vorliegenden Fall nahezu keine Beeinträchtigung.

Wesentliche Erkenntnisse Ein netzlokaler Fehler kann innerhalb kürzester Zeit zu massiven weltweiten Störungen für unbeteiligte Endanwender und Dienstbetreiber führen. Der Vorfall verdeutlicht die Wichtigkeit selbst einfachster Schutzmaßnahmen, die aufgrund der Fragilität des Internet-Routings und jederzeit möglichen Route Leaks notwendig sind.

Einschätzung: Route Leaks stellen eine stete Gefahr für die Internet-Infrastruktur dar. Fehlende Konsequenzen für Beteiligte im vorliegenden Fall bestätigen jedoch, dass Route Leaks trotz ihres Gefährdungspotentials als alltäglich wahrgenommen und in aller Regel nicht sanktioniert werden. Nicht zuletzt deshalb ergibt sich durch besonders strikten Einsatz von Routing-Filtern bei der Deutschen Telekom ein Standortvorteil für Deutschland.

2.2.5 Fallstudie: Cloudflare-Ausfall durch Fehlkonfiguration

2.2.5.1 Übersicht und Einordnung

Am 2. Juli 2019 sind viele der weltweit populärsten Webseiten für eine halbe Stunde nicht mehr erreichbar. Ausgelöst wurde der Ausfall durch fehlerhafte Konfiguration einer programmierbaren Web Application Firewall (WAF) von Cloudflare, die sowohl Kunden des Content Delivery Networks (CDN) als auch Endanwender vor Angriffen schützen soll.

Vorfallshergang [I13] Am 2. Juli 2019 um 13:42 Uhr UTC aktiviert ein Cloudflare-Entwickler eine neue WAF-Regel, die schädlichen Code in Kunden-Webseiten erkennen soll. Durch ineffiziente Umsetzung führt die Regel zu voll ausgelasteten Prozessoren auf allen für HTTP/HTTPS-Anwendungen zuständigen Cloudflare-Servern (Abb. 2.58). Dadurch kann ein Großteil der Anfragen an Webseiten, die über das CDN ausgeliefert werden, nicht mehr beantwortet werden. Das Verkehrsaufkommen bei Cloudflare bricht zeitweise um 80% ein, bis der Fehler um 14:09 Uhr durch Deaktivieren der WAF mitigiert wird.

Abbildung 2.58: [I13] **CPU-Auslastung auf WAF-System**, Quelle: Cloudflare [18]

Der tatsächliche Grund für die Überlastung der Web-Server lag in einem fehlerhaften regulären Ausdruck. Ein regulärer Ausdruck beschreibt eine beliebige Menge von Zeichenketten und wird häufig verwendet, um Übereinstimmungen in Texten und Daten zu suchen. Im vorliegenden Fall führte dieser reguläre Ausdruck jedoch zu einem unvorhergesehen hohen Ressourcenverbrauch. Dass dieser isolierte Fehler zu einem faktischen Totalausfall führen konnte, hat mehrere Gründe. Zum Einen wurde die WAF kurze Zeit zuvor überarbeitet, um Anfragen effizienter bearbeiten zu können. Dabei wurde ein Schutzmechanismus entfernt, der CPU-Überlastungen hätte verhindern können. Des Weiteren wurde die neu eingesetzte Firewall-Regel vorab nicht auf deren Ressourcenverbrauch hin überprüft und innerhalb von Sekunden weltweit auf Produktivsystemen eingesetzt.

Obwohl die WAF durch Einsatz von Überwachungssystemen um 14:00 Uhr als Fehlerquelle identifiziert werden konnte, war eine globale Deaktivierung des überlasteten Systems erst um 14:07 Uhr möglich, da Cloudflare-Mitarbeiter aufgrund der Server-Überlast auch auf die eigene Management-Infrastruktur nicht mehr zugreifen konnten. Ab 14:09 Uhr wurden Web-Anfragen wieder normal beantwortet, bis 14:52 Uhr wurde die fehlerhafte WAF-Regel entfernt und die Firewall global wieder in Betrieb genommen.

[18] `https://blog.cloudflare.com/details-of-the-cloudflare-outage-on-july-2-2019/`

Direkte Folgen Trotz der weitreichenden Ausfälle vieler populärer Webseiten sind keine Schadensersatzforderungen o.ä. bekannt. Um Störungen dieser Art in Zukunft zu vermeiden, kündigte Cloudflare mehrere Maßnahmen an. Dazu zählen bessere Tests auf hohe CPU-Auslastung, schrittweises Ausrollen von Regelaktualisierungen, Laufzeitbeschränkungen für die Regelauswertung innerhalb der WAF sowie eine manuelle Überprüfung aller existierenden Firewall-Regeln. Zusätzlich soll im Hinblick auf zukünftige Ausfälle eine separate Infrastruktur für den Zugriff auf Steuerungssysteme aufgebaut werden, um die Reaktionsgeschwindigkeit von Störfällen zu entkoppeln und somit weiter zu erhöhen.

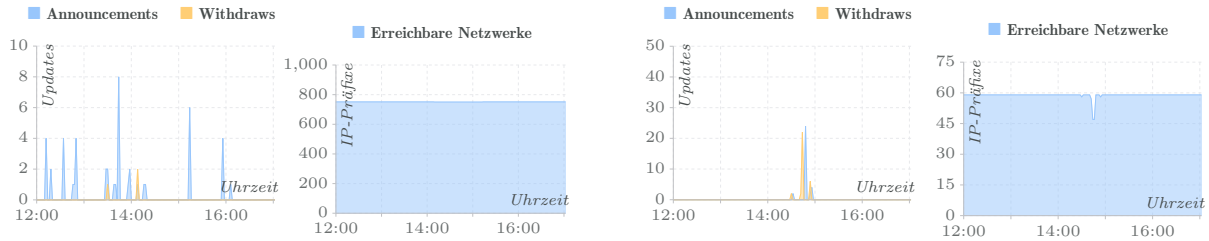
Verwandte Vorfälle Aufgrund der vergleichsweise raschen Behebung der Störung liegt die Vorfallsdauer unter dem Durchschnitt aller Ausfälle durch menschliche Fehler (siehe Abschnitt 2.1.2.2). Gleichzeitig ist eine überdurchschnittlich hohe Reichweite zu verzeichnen, während die hohen Auswirkungen des Fehlers denen vergleichbarer Vorfälle entsprechen. Bereits am 31. Mai 2018 führte eine Fehlkonfiguration seitens Cloudflare zu einem weltweiten Dienstausfall [I15]. In diesem Fall war allerdings nur ein öffentlicher DNS-Resolver von Cloudflare unmittelbar betroffen, das Content-Delivery-Network selbst blieb einsatzbereit. Demnach kam es auch nicht zu Ausfällen von Kunden-Webseiten, zudem konnte der Fehler schnell behoben werden. Ein in Auswirkung und Reichweite vergleichbarer Konfigurationsfehler trat im Jahr 2016 beim Tier1-ISP Telia auf [I19].

Wissenschaftliche Arbeiten Aufgrund des spezifischen Vorfallsverlaufs und der Besonderheiten der Cloudflare-Infrastruktur existiert nur wenig Forschung, die die konkrete Problemstellung abdeckt. So beschäftigen sich zwar Arbeiten mit dem Einsatz mehrerer CDN-Dienste [31, 32, 33], allerdings liegt deren Schwerpunkt auf einer Verbesserung der Leistung und nicht auf Ausfallsicherheit. Daneben werden auch Leistungssteigerungen mit direktem Bezug zu Cloudflare [34] untersucht. Andere Studien konzentrieren sich auf Sicherheitsaspekte beim Einsatz einer Web Application Firewall [35, 36].

2.2.5.2 Analyse der Control Plane

Eine Analyse der Control Plane lässt wenig Erkenntnisse in Bezug auf den Ausfall erwarten, da die Störungen nicht im Netzwerk, sondern der Anwendungsschicht auftraten. Dennoch ist ein Blick auf das Routing sinnvoll, um unter Umständen Mitigationsmaßnahmen oder BGP-Umleitungen des Betreibers nachzuvollziehen. Alle folgenden Auswertungen beziehen sich auf die beiden Standorte LW-DTAG und LW-DECIX, wodurch eine deutsche Sicht auf das weltweite Content Delivery Network von Cloudflare gewonnen und so ggf. auch regional relevante Konsequenzen besser identifiziert werden können.

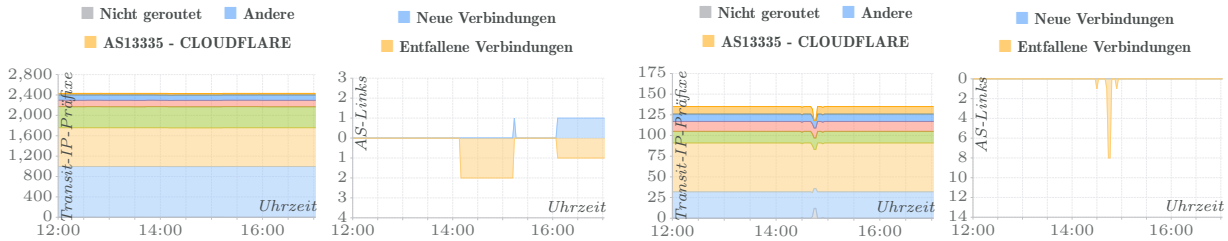
Zielanalyse Im Folgenden werden alle BGP-Routen betrachtet, die zu den Netzbereichen von Cloudflare führen. Eine Analyse von Transit-Routen erfolgt nicht, da Cloudflare im Internet-Routing nicht als Transitanbieter auftritt. Zudem betreibt Cloudflare mit AS13335 nur ein einzelnes Autonomes System, Zielanalysen beschränken sich daher auf dessen BGP-Aktivität und annoncierte IP-Präfixe (Abb. 2.59). Im Vorfallszeitraum zeigen sich kaum signifikante BGP-Aktivitäten oder Änderungen in den erreichbaren Netzbereichen, die über das übliche Maß im Internet-Routing hinausgehen. Bei LW-DECIX kommt es zwar zwischen 14:44 Uhr und 14:46 Uhr zum Wegfall von 12 IP-Präfixen in der Größe eines /20-Netzwerkes, ein Zusammenhang zum Vorfall ist aber jedoch nicht ersichtlich.



(a) LW-DTAG (b) LW-DECIX

Abbildung 2.59: [I13] **Zielanalyse**, BGP-Aktivität/IP-Präfixe (Control Plane)

Änderungsanalyse Um die vorangehend beobachteten Routing-Vorgänge von Cloudflare besser einschätzen zu können, werden zugehörige BGP-Routen im Folgenden anhand ihrer topologischen Charakteristiken analysiert. Dazu werden die an der Weiterleitung beteiligten Autonomen Systeme sowie Änderungen an den Verbindungen zwischen diesen Autonomen Systemen näher untersucht (Abb. 2.60).



(a) LW-DTAG (b) LW-DECIX

Abbildung 2.60: [I13] **Änderungsanalyse**, Transit-/Topologieverlauf (Control Plane)

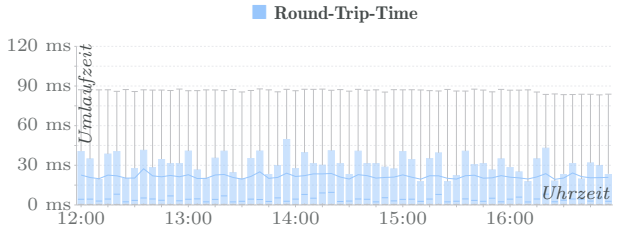
Bei LW-DTAG sind keine nennenswerten Änderungen im Transit- oder Topologieverlauf zu erkennen, für LW-DECIX kann erneut ein kurzfristiger Ausfall von 12 IP-Präfixen nachvollzogen werden. Davor waren 9 dieser IP-Präfixe über den indischen ISP Bharti Airtel (AS9498) erreichbar, so dass hier nicht von einer aktiven Aktion seitens Cloudflare auszugehen ist. Alle beobachteten Änderungen an Transit und Topologie kehren zudem nach kurzer Zeit in den Ursprungszustand zurück. Zusammenfassend können die in Erscheinung tretenden (marginalen) Routing-Änderungen kaum mit dem Ausfall in Verbindung gebracht werden, auch für IPv6 ergeben sich keine Auffälligkeiten. Wie zu erwarten liefert die Control Plane keine verwertbaren Hinweise auf Vorgänge in der Anwendungsschicht.

2.2.5.3 Analyse der Data Plane

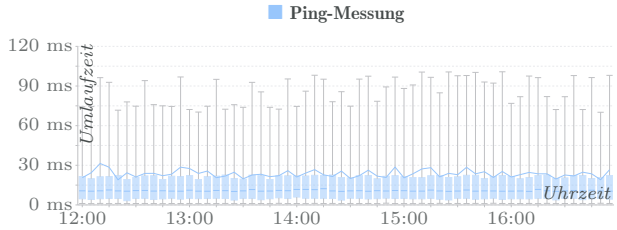
Mit Hilfe einer Analyse von IP-basierten Messungen ist es prinzipiell denkbar, eine Überlast auf den Systemen von Cloudflare festzustellen und somit weitere Erkenntnisse über den Ausfall zu gewinnen. Zu diesem Zweck werden alle über die RIPE ATLAS Messinfrastruktur verfügbaren IP-Pfadmessungen (12.785.405 Datensätze) und Ping-Messungen (40.769.146 Datensätze) im Betrachtungszeitraum für die betroffenen Netzbereiche ausgewertet. Die Verteilung von Messzielen wird durch die Infrastruktur der Messplattform selbst und in geringerem Maße auch von dessen Nutzern festgelegt und ist demnach prinzipiell nicht gleichverteilt. Aufgrund der Popularität des Cloudflare-CDNs sind jedoch überproportional viele Messungen dorthin vorhanden. Um weitere Netzbereiche zu erfas-

sen, die mit hoher Wahrscheinlichkeit Dienste der Cloudflare-Infrastruktur nutzen, werden zusätzlich auch Messungen zu allen IP-Adressen betrachtet, für die DNS-Namen in öffentlich zugänglichen Webseiten-Rankings (Amazon Alexa, Majestic Million und Cisco Umbrella) unter den Top-1000 Einträgen zu finden sind. Insgesamt ergeben sich daraus 106.837 IP-Pfadmessungen und 152.092 Ping-Messungen mit Bezug zum vorliegenden Ausfall. Alle nachfolgenden Ergebnisse beziehen sich zunächst nur auf IPv4, bei wesentlichen Abweichungen werden entsprechende Hinweise für IPv6-Messungen angegeben. Die vollständigen Ergebnisse lassen sich – über die nachfolgende Analyse hinaus auch weiter parametrisier- und filterbar – auf der interaktiven Projekt-Webseite abrufen.

Pfadanalyse Ein wesentliches Indiz für Überlast stellen erhöhte Umlaufzeiten dar. Daher werden im Folgenden Latenzwerte für alle vermessenen Ziele, sowohl über Pfad- als auch Ping-Messungen, im Vorfallszeitraum verglichen (Abb. 2.61 und Abb. 2.62).

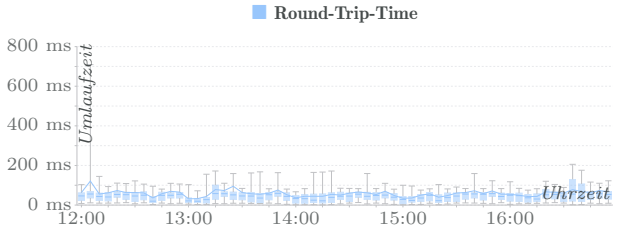


(a) Pfadlatenzen

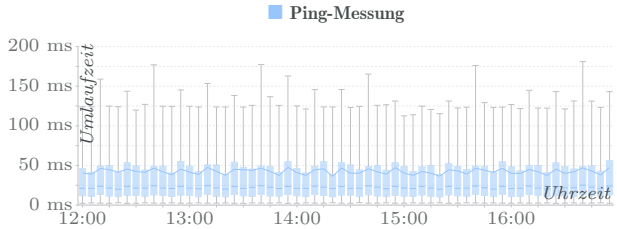


(b) Ping-Messungen

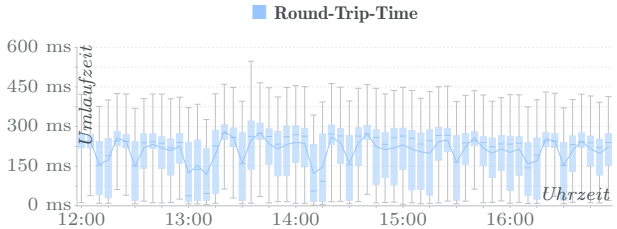
Abbildung 2.61: [I13] **Pfadanalyse**, Messziele in AS13335 (Data Plane)



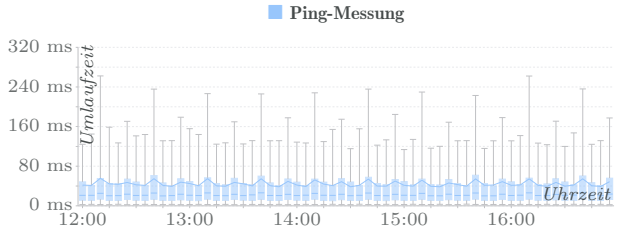
(a) Pfadlatenzen (Alexa Top-1000)



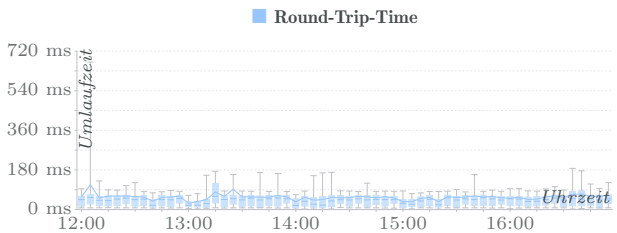
(b) Ping-Messungen (Alexa Top-1000)



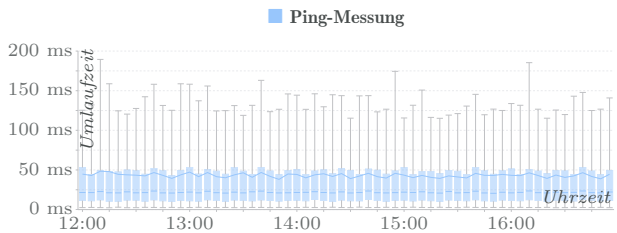
(c) Pfadlatenzen (Majestic Top-1000)



(d) Ping-Messungen (Majestic Top-1K)



(e) Pfadlatenzen (Umbrella Top-1K)

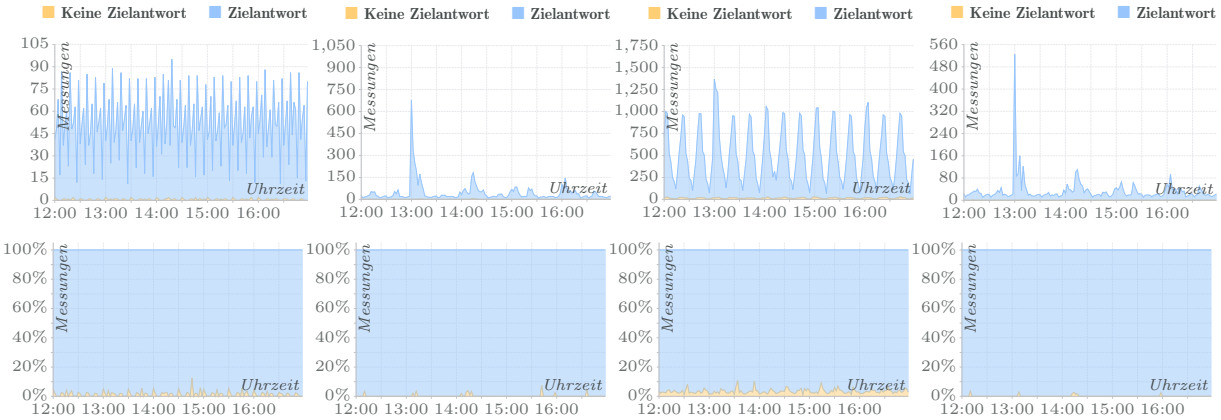


(f) Ping-Messungen (Umbrella Top-1K)

Abbildung 2.62: [I13] **Pfadanalyse**, Messziele in DNS-Toplisten (Data Plane)

Bei der Betrachtung der Umlaufzeiten für Messungen zu den Netzbereichen von Cloudflare (AS13335) sind keine über normale Schwankungen hinausgehenden Abweichungen erkennbar. Dies gilt sowohl für gemessene Pfadlatenzen als auch für die Umlaufzeiten der Ping-Messungen. Auch für die Top-1000 Messziele der Webseiten-Rankings ergeben sich keinerlei Auffälligkeiten in den Messwerten. Da die Datenlage durchaus als zureichend zu bewerten ist, weisen die Ergebnisse ausschließlich auf Störungen in den Web-Anwendungen hin, während die zugrunde liegenden Server-Systeme weiterhin erreichbar blieben.

Messanalyse Ein weiterer Blick auf mögliche Konsequenzen des Ausfalls ergibt sich aus einer Gegenüberstellung aller durchgeführten mit den tatsächlich erfolgreichen Messungen. Dazu wird im Folgenden die Zahl der Messungen im Betrachtungszeitraum nach Zielliste zusammen mit den zugehörigen anteiligen Erfolgsraten dargestellt (Abb. 2.63).



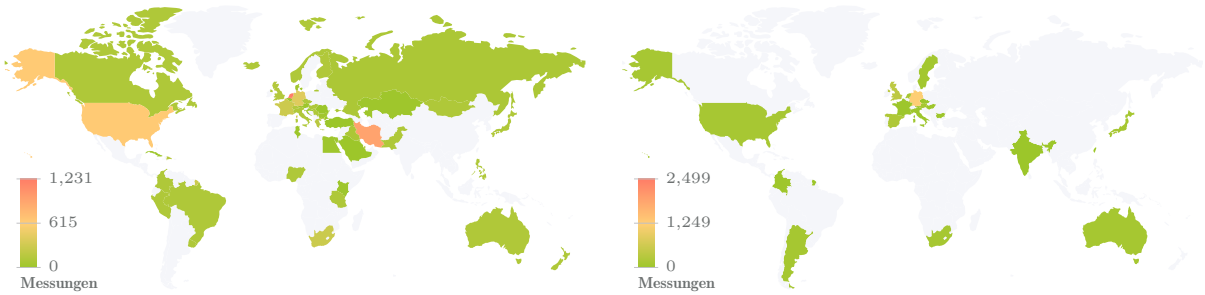
(a) AS13335 (b) Alexa Top-1K (c) Majestic Top-1K (d) Umbrella Top-1K

Abbildung 2.63: [I13] **Messanalyse**, absolut/relativ, Messziele (Data Plane)

Zum Zeitpunkt des Vorfalls lassen sich keinerlei ungewöhnliche Veränderungen der Datenlage festzustellen. Periodische Muster in der Messverteilung sowie ein deutlicher Anstieg der Zahl der Messungen um 13:00 Uhr können nicht in Verbindung mit der Cloudflare-Störung gebracht werden. Diese Beobachtungen resultieren vielmehr aus einer periodischen Messplanung bzw. aus nutzergestützten Messaufträgen in der RIPE ATLAS Infrastruktur. Auch die Erfolgsrate der Messungen zeigt keine besonderen Auffälligkeiten, die über das normale Maß hinausgehen. Diese Ergebnisse bestätigen erneut die Annahme, dass die von der Überlast betroffenen Systeme durchweg imstande waren, auf eingehende Pakete zu reagieren. Dies steht im Einklang mit Medienberichten, wonach Aufrufe der betroffenen Webseiten mit dem HTTP-Statuscode 502 (Bad Gateway) beantwortet wurden. Derartige Meldungen werden zurückgeliefert, wenn Anfragen eines Proxy-Servers vom bearbeitenden System nicht beantwortet werden. Zusammenfassend kann zweifelsfrei davon ausgegangen werden, dass Pfad- und Ping-Messungen auch während der Störung mit gültigen TCP/IP-Antworten der Web-Server quittiert wurden, weshalb der Ausfall generell nicht in der Data Plane nachverfolgbar ist. Eine Analyse von HTTP-Messungen der Anwendungsschicht war aufgrund fehlender historischer Daten nicht möglich.

Betroffene Länder Zuletzt wird zur Plausibilisierung der gewonnenen Erkenntnisse die geographische Verteilung aller Messquellen und Transit-Router betrachtet, über die Messziele in den Netzbereichen von Cloudflare (AS13335) vermessen wurden (Abb. 2.64).

Es zeigt sich eine weltweite Verteilung aller beteiligten Messquellen, wodurch auch Stö-



(a) Messquellen (b) Transit-Router

Abbildung 2.64: [I13] **Transitländer**, Messquellen/Transit-Router (Data Plane)

rungen in etwaigen regionalen Spiegelsystemen des CDNs zuverlässig beobachtbar wären. Häufungen der Messquellen in Nordamerika und Europa entsprechen dabei im Wesentlichen der Verteilung der RIPE ATLAS Messknoten. Auffällig ist allerdings ein hoher Anteil an Messungen aus dem Iran, was auf ein gesteigertes Interesse an der Cloudflare-Infrastruktur bzw. den darüber bereitgestellten Diensten hindeutet. Interessanterweise sind bei mehr als der Hälfte aller Messungen Transit-Router in Deutschland an der Weiterleitung zu Cloudflare beteiligt, was auf eine große Bedeutung des Internet Exchange Points DE-CIX für dessen Routing schließen lässt. Weitere konkrete Erkenntnisse über den Ausfall liefern diese Ergebnisse allerdings nicht.

2.2.5.4 Bewertung und Folgen

Basierend auf den vorangehenden Analysen und Recherchen lassen sich folgende zentralen Ergebnisse für den betrachteten Vorfall festhalten.

Charakteristische Besonderheiten Menschliches Versagen führt in Kombination mit unzureichenden Testprozeduren des Content Delivery Networks Cloudflare zu massiven weltweiten Ausfällen beliebter Webseiten. Eine fehlerhafte Firewall-Konfiguration wird trotz vorhandener Sicherheitsmaßnahmen global ausgerollt und legt sowohl Infrastruktur als auch alle darüber bereitgestellten Web-Dienste für eine halbe Stunde lahm.

Konsequenzen und Auswirkungen Die Fehlkonfiguration führt zur Überlastung der Web-Server von Cloudflare, wodurch alle Kunden des CDNs betroffen sind. Da in der Folge auch Dienste der eigenen Infrastruktur nicht mehr erreichbar sind, verzögert sich die Behebung des Problems. Cloudflare kündigte im Rahmen einer detaillierten Aufarbeitung des Vorfalls an, bestehende Sicherheitsmaßnahmen zu verbessern. Trotz des Ausfalls zahlreicher stark frequentierter Webseiten wurden keine Schadensersatzforderungen oder rechtlichen Konsequenzen für Cloudflare öffentlich bekannt.

Schutz- und Gegenmaßnahmen Die von Cloudflare eingesetzten Schutzmaßnahmen waren aus mehreren Gründen unzureichend für eine Vermeidung des Ausfalls. Zunächst wurde der von Konfigurationsänderungen hervorgerufene Ressourcenbedarf im Vorfeld einer Ausrollung nicht überprüft. Weiterhin fand die Verteilung von Updates nicht schrittweise statt, vielmehr wurden Aktualisierungen innerhalb weniger Sekunden in der gesamten Infrastruktur zum Einsatz gebracht. Schließlich waren Systeme zur Verwaltung des CDNs nicht von der Produktiv-Infrastruktur entkoppelt und dementsprechend ebenfalls

von den Störungen betroffen. Laut Aussage des Betreibers sollen zukünftig verbesserte Maßnahmen umgesetzt werden. Für Kunden von Cloudflare bzw. von CDNs im Allgemeinen sind kaum geeignete Schutz- oder Gegenmaßnahmen bekannt, um kurzfristig auf Ausfälle dieser Art reagieren zu können. Einzig eine Umstellung von DNS-Einträgen wäre denkbar, aufgrund des Verzögerungseffekts durch Caching erscheint das Abwarten auf Fehlerbehebung durch den Anbieter in vielen Fällen jedoch zweckmäßiger. Für die Zukunft könnten kritische Dienste mittels Hot-Standby-Systemen in Verbindung mit kurzlebigem DNS-Caching oder reaktiven Routing-Umleitungen zusätzlich abgesichert werden.

Wesentliche Erkenntnisse Der Fall zeigt eindringlich, wie eine weltweit verteilte, hochredundante Infrastruktur zum Schutz von Drittanbieterdiensten durch menschliches Versagen selbst zum Single-Point-of-Failure wurde. Ebenfalls wird deutlich, dass trotz des Einsatzes weithin akzeptierter Sicherheitsmaßnahmen gravierende Betriebsstörungen möglich sind. Ferner bleibt anzumerken, dass nicht jeder Ausfall im Internet durch Daten in der Control Plane oder Data Plane nachweisbar ist, was einen Bedarf an weiterführenden Beobachtungsmöglichkeiten für kritische Anwendungen und Dienste nahelegt.

Einschätzung: Durch wachsende Anforderungen an die Verfügbarkeit von Netzdiensten und aufgrund steigender Gefahren von Angriffen werden Content Delivery Networks immer häufiger eingesetzt. So wird mittlerweile ein signifikanter Anteil beliebter Webseiten über CDN-Anbieter wie Cloudflare ausgeliefert, um deren Leistungsfähigkeit und Ausfallsicherheit selbst für größte Nutzerzahlen zu garantieren[19]*. Damit sind auch deutsche Endanwender und Dienstbetreiber in zunehmendem Maße von potentiellen Infrastrukturausfällen bei CDN-Anbietern betroffen. Eine echte Unabhängigkeit der nationalen Internet-Landschaft von internationalen Anbietern ließe sich nur durch Aufbau eigener Redundanz in Deutschland herstellen, was den aktuellen Trends jedoch entgegenläuft.*

2.2.6 Fallstudie: Peering-Streit zwischen Netflix und Verizon

2.2.6.1 Übersicht und Einordnung

Mitte des Jahres 2014 kommt es zu einem öffentlich ausgetragenen Streit zwischen dem Streaming-Dienstleister Netflix und den Internet-Anbietern Verizon und Level3. Streitpunkt dabei ist eine verringerte Videoqualität für Kunden mit einem Internet-Anschluss bei Verizon, was in der Folge zu gegenseitigen und öffentlich vorgetragenen Schuldzuweisungen der beteiligten Anbieter eskaliert. Netflix wirft den ISPs insbesondere ein Ausnutzen ihrer Marktmacht vor, um kostenpflichtige Peering-Verträge zu erzwingen.

Vorfallshergang Am 29. April 2014 einigen sich Verizon und Netflix nach langen Verhandlungen auf ein Paid-Peering, also einen direkten, für Netflix kostenpflichtigen Datenaustausch, um die Dienstqualität für Kunden beider Firmen zu verbessern[20] [I49]. Bereits im Vorfeld hatte Netflix unter ähnlichen Umständen Verträge mit Comcast abgeschlossen. Zwischen Netflix und Comcast wurde der Ausbau bereits während den Vertragsverhandlungen vorangetrieben, wodurch zum Zeitpunkt der Einigung die neue Verbindung ohne größere Verzögerungen genutzt werden konnte und sofort eine Verbesserung eintrat. Ve-

[19] https://www.keycdn.com/blog/why-use-a-cdn

[20] https://arstechnica.com/tech-policy/2014/04/netflix-and-verizon-reach-interconnection-deal-to-speed-up-video/

Abbildung 2.65: **Hinweis auf Überlast**, Quelle: Netflix [22]

rizon hingegen beginnt mit dem Ausbau nach Abschluss der Vertragsverhandlungen, so dass eine Besserung erst nach mehreren Monaten eintritt. Der Datenaustausch zwischen Netflix und Verizon findet bis dahin weiter über den Tier1-Provider Level3 statt [21]. Als Reaktion auf die noch immer überlastete Verbindung und steigende Unzufriedenheit bei den eigenen Kunden blendet Netflix in der Zwischenzeit Hinweismeldungen ein, die Verizon als Ursache für die verminderte Dienstqualität verantwortlich machen (Abb. 2.65).

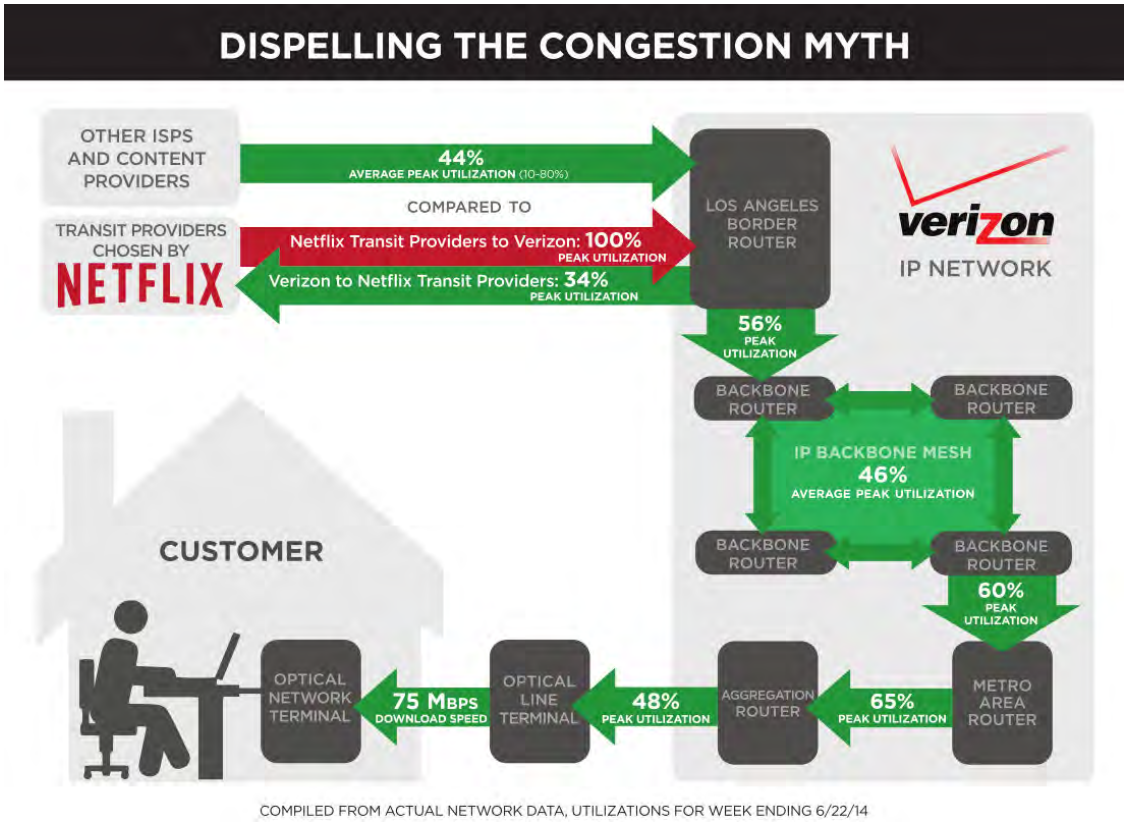


Abbildung 2.66: **Öffentliche Stellungnahme**, Quelle: Verizon [I49]

[21] https://arstechnica.com/information-technology/2014/06/why-verizon-wont-solve-its-netflix-problem-as-soon-as-comcast/

[22] https://www.techdirt.com/articles/20140605/12291627480/verizon-sends-netflix-cease-desist-saying-it-cant-blame-verizon-clogged-networks.shtml

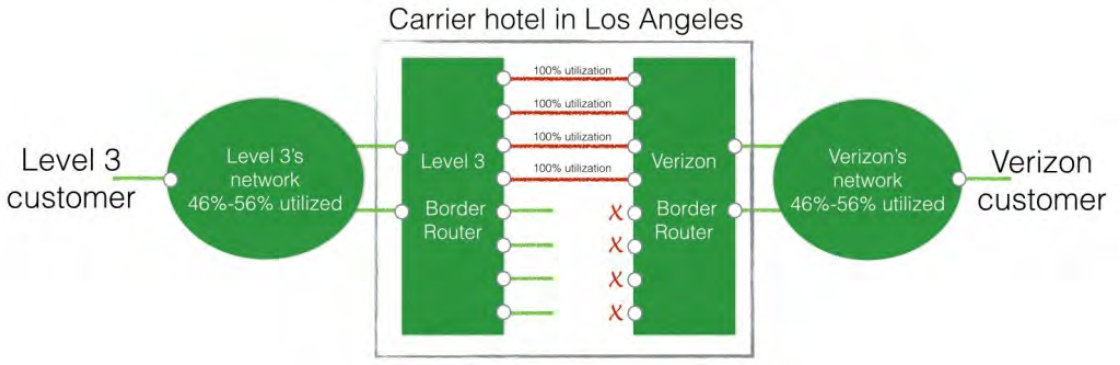


Abbildung 2.67: **Öffentliche Gegendarstellung**, Quelle: Level3 [23]

Daraufhin entwickelt sich ein öffentlich ausgetragener Konflikt, in dessen Rahmen Verizon Netflix auch per Unterlassungserklärung auffordert, die Hinweismeldung nicht länger anzuzeigen. Im Zuge der folgenden medialen Aufmerksamkeit veröffentlicht Verizon zur weiteren Schadensbegrenzung eine technische Gegendarstellung (Abb. 2.66). In dieser öffentlichen Stellungnahme wird dargelegt, dass der Engpass nicht im Netz von Verizon, sondern ausschließlich bei Transitanbietern von Netflix zu finden sei, die deren Verbindung zu Verizon zu 100% auslasten. Level3 – implizit an der Überlast mitbeschuldigt – reagiert daraufhin ebenfalls öffentlich (Abb. 2.67) und stellt klar, dass Verizon sich bereits seit längerer Zeit einer Kapazitätserweiterung verschließt. Dieser Schlagabtausch ist insbesondere auch deshalb bemerkenswert, da zu diesem Zeitpunkt längst eine Einigung mit Netflix erzielt wurde, Verizon aber nach wie vor nicht zu einer (kurzfristigen) Verbesserung der Situationen im Sinne der gemeinsamen Kunden bereit ist. Es ist anzunehmen, dass vorzeitige Verbesserungen schlicht nicht vertraglich vereinbart wurden.

Direkte Folgen Das vereinbarte Paid-Peering zwischen Netflix und Verizon wird ab August 2014 in Betrieb genommen. Die Situation verbessert sich bis September zunehmend, in der Folge leiden Kunden beider Anbieter schließlich nicht mehr unter Qualitätseinbußen. Netflix übt jedoch öffentliche Kritik an der Regulierungsbehörde Federal Communications Commission (FCC), da Paid-Peering laut FCC nicht als Aspekt der Netzneutralität zu werten ist und somit nicht reguliert werden muss. Neben Comcast und Verizon streben auch weitere Provider wie AT&T Paid-Peerings an. Netflix treibt unterdessen den Ausbau seines eigenen Content Delivery Networks voran [24], um unabhängiger von Internet-Anbietern und deren Marktmacht zu werden. Anfang 2015 entschließt sich die FCC unter steigendem medialen Druck, Paid-Peering-Veträge zukünftig zu überwachen, um die Interessen der Endverbraucher zu schützen [25].

Verwandte Vorfälle Sowohl die hohe Dauer als auch die mittleren Auswirkungen des Vorfalls gleichen dem Durchschnitt aller betrachteten Peering-Streitigkeiten (siehe Abschnitt 2.1.2.5). Die Reichweite fällt aufgrund der Beschränkung auf einen einzelnen Streaming-Dienst jedoch unterdurchschnittlich aus. Bereits 2010 kam es aufgrund des hohen Verkehrsaufkommens von Netflix zu einem öffentlich ausgetragenen Konflikt [I53]. In diesem Fall versorgte Level3 sowohl Comcast als auch Netflix kostenpflichtig mit Transit. Aufgrund der großen Datenmengen seitens Netflix forderte Comcast schließlich eine

[23] https://www.techdirt.com/articles/20140605/12291627480/verizon-sends-netflix-cease-desist-saying-it-cant-blame-verizon-clogged-networks.shtml

[24] https://blog.apnic.net/2018/06/20/netflix-content-distribution-through-open-connect/

[25] https://www.theverge.com/2015/2/4/7978647/fcc-enforcement-interconnection-peering-title-ii

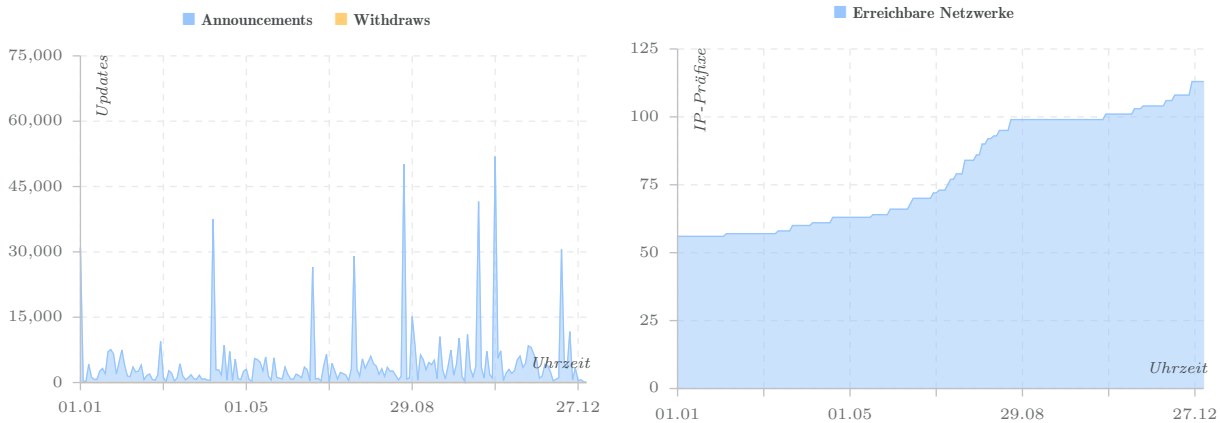
Gebühr von Level3 und drohte damit, Verkehre andernfalls zu blockieren. Die Regulierungsbehörde FCC war bei der Beilegung des Streits ebenfalls involviert, Details über die erzielte Lösung wurden nicht bekannt gegeben. Ein ähnlicher Vorfall ereignete sich, wenn auch weit weniger stark medial begleitet, zwischen Verizon und Cogent im Jahr 2013 [I50].

Wissenschaftliche Arbeiten Infolge immer wieder aufkeimender Peering-Konflikte vergleichbarer Art existiert eine Vielzahl von wissenschaftlichen Arbeiten zum Thema Peering zwischen Transit-Providern, aber auch zwischen Internet Service Providern und Content-Diensten [37, 38, 39]. Weitere Arbeiten befassen sich mit einem optimierten Ausgleich zwischen Paid-Peering und dem Aufbau von lokalen Caches [40] sowie mit dem Netflix-eigenen Content Delivery Network [41]. Zusätzlich sind im Zusammenhang mit ausgetragenen Peering-Machtkämpfen auch Arbeiten zum Thema Netzneutralität relevant. Entsprechende Untersuchungen betrachten mögliche Auswirkungen von Selbstregulierung im Vergleich zu gesetzlichen Vorgaben für Paid-Peering [42], explizite Folgen für ISPs und CDNs beim Wegfall von Netzneutralität [43] sowie allgemeine technische Fragen zur Umsetzung bzw. auch Umgehung der Netzneutralität [44].

2.2.6.2 Analyse der Control Plane

Anhand einer Analyse von BGP-Tabellen lassen sich langfristige Änderungen für das Netz und die Internet-Anbindung von Netflix untersuchen. Im Hinblick auf dessen kontinuierlichen Netzausbau ist dabei mit erhöhten Aktivitäten zu rechnen. Für die folgenden Auswertungen wird stets der Zeitraum von 01. Januar 2014 bis 02. Januar 2015 zugrunde gelegt. Da keine BGP-Daten direkt aus dem Netz von Verizon verfügbar sind, basieren die Analysen der Control Plane auf der Routing-Tabelle des größten RouteViews-Kollektors RV-OREGON2. Die IPv6-Anbindung von Netflix wurde im Auswertungszeitraum nur sporadisch genutzt, dementsprechend beschränken sich die Analysen auf IPv4. Alle Ergebnisse lassen sich auch über die interaktive Projekt-Webseite abrufen.

Zielanalyse Die nachfolgende Zielanalyse beschränkt sich auf BGP-Aktivität und annoncierte Netzbereiche des von Netflix für Peering-Verbindungen verwendeten Autonomen Systems (Abb. 2.68). Auf eine Transitanalyse wird verzichtet, da Netflix als Content-Anbieter keine Transitleistungen für andere Netzbetreiber erbringt.



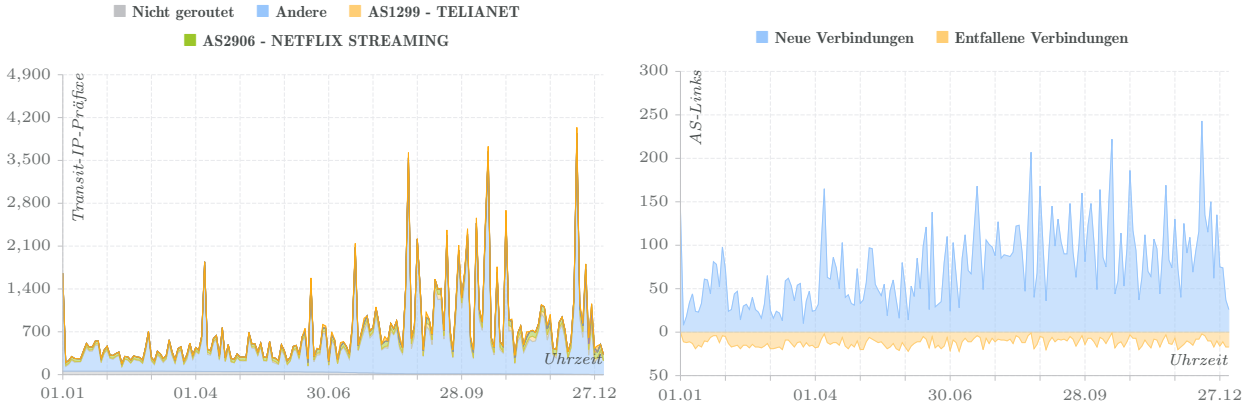
(a) BGP-Aktivität

(b) IP-Präfixe

Abbildung 2.68: [I49] **Zielanalyse** (Control Plane)

Im Betrachtungszeitraum ist zunächst keine wesentliche Zunahme der BGP-Aktivität ersichtlich. Allerdings sind einzelne Spitzen deutlich zu erkennen, die jeweils mit einem Anstieg der annoncierten IP-Präfixe, d.h. einer Netzerweiterung von Netflix einhergehen. Hier zeigt sich innerhalb eines Jahres ein signifikanter Anstieg von 56 auf 113 geroutete IP-Präfixe, was einem Zuwachs von 88 /24-Netzwerken bzw. mehr als einem /18-Netzwerk entspricht. Ein Großteil dieser neuen IP-Präfixe wird dabei zwischen Mai und August sichtbar und steht somit in zeitlichem Zusammenhang mit dem Aufbau der Peering-Verbindung zu Verizon. Da hierfür jedoch keine zusätzlichen IP-Präfixe notwendig sind, ist davon auszugehen, dass Netflix bereits während der Beilegung des Peering-Streits konsequent am Ausbau des eigenen Content Delivery Networks arbeitete.

Änderungsanalyse Der von Netflix verfolgte Netzausbau lässt sich mit Hilfe einer Analyse der weltweiten Netzanbindung näher untersuchen. Im Folgenden werden dazu alle Transit- und Topologieänderungen im Betrachtungszeitraum analysiert (Abb. 2.69).



(a) Transitverlauf

(b) Topologieverlauf

Abbildung 2.69: [I49] **Änderungsanalyse** (Control Plane)

Im Transitverlauf zeigt sich analog zur Zielanalyse erneut ein deutlicher Ausbau des Netzes mittels zusätzlicher IP-Präfixe. In der Zusammensetzung der Transit-ASe selbst sind bis auf regelmäßig zu erwartende Schwankungen keine nennenswerten Änderungen sichtbar. Es ist insbesondere ersichtlich, dass Netflix individuelle Peering-Verbindungen gegenüber Transitleistungen einzelner großer Tier1-ISPs bevorzugt. Deren Zahl nimmt im Laufe des Jahres stetig zu. Dieses Bild spiegelt sich auch im Topologieverlauf wider. Die Zahl der beobachteten AS-Verbindungen, die an der Weiterleitung zum Netz von Netflix beteiligt sind, steigt kontinuierlich an, während kaum Verbindungen dauerhaft entfallen. Dies verdeutlicht erneut das Bestreben von Netflix nach möglichst breit angelegten Internet-Anbindungen und damit einer Unabhängigkeit von großen ISPs.

2.2.6.3 Analyse der Data Plane

Aufgrund des wesentlich geringeren Ausbaus der RIPE ATLAS Messinfrastruktur im Jahr 2014 stehen keine geeigneten IP-Messdaten für eine Bewertung der Data Plane des Peering-Vorfalls zur Verfügung. Stattdessen kann aber auf archivierte Datensätze des von Netflix selbst herausgegebenen ISP Speed Index zurückgegriffen werden, um Rückschlüsse auf die Effektivität des Paid-Peerings mit Verizon zu ziehen (Abb. 2.70).

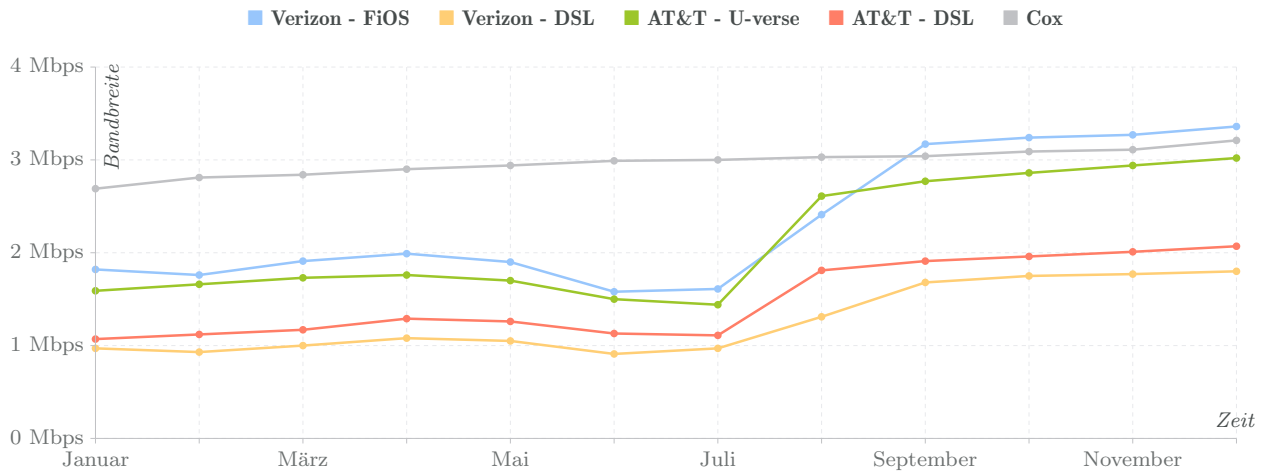


Abbildung 2.70: [I49] **Provider-Vergleich**, Quelle: Netflix[26](Data Plane)

Wie anhand der öffentlichen Berichterstattung zu erwarten, zeigt sich ab Juli 2014, d.h. drei Monate nach der getroffenen Übereinkunft, ein deutlicher Anstieg der Verbindungsqualität zu Verizon. Dies gilt sowohl für klassische DSL-Kunden als auch für die über Glasfaser angebundenen Kunden (FiOS). Letztere übertreffen im Laufe des Jahres auch den bis dahin bestangebundenen Anbieter des Rankings. Dies verdeutlicht, dass weder im Netz von Netflix noch von Verizon Engpässe vorhanden waren, sondern lediglich die Verbindung beider Netze unzureichend ausgelegt wurde. Ende Juli 2014 wurde von Netflix eine weitere offizielle Übereinkunft mit AT&T bekannt gegeben, um die Verbindungsqualität mittels Paid-Peering zur verbessern. Im Gegensatz zur Situation bei Verizon zeigt sich hier bereits im Vorfeld der Vereinbarung eine wesentliche Verbesserung der Dienstqualität. Dies unterstreicht, dass bei Einigung generell auch kurzfristige Lösungen im Sinne der betroffenen Kunden möglich sind, diese aber aus wirtschaftlichen oder strategischen Gesichtspunkten nicht zwangsläufig auch sofort umgesetzt werden.

2.2.6.4 Bewertung und Folgen

Basierend auf den vorangehenden Analysen und Recherchen lassen sich folgende zentralen Ergebnisse für den betrachteten Vorfall festhalten.

Charakteristische Besonderheiten Der namhafte Internet-Anbieter Verizon zwingt den Streaming-Anbieter Netflix mit Hilfe einer unzureichend dimensionierten Netzverbindung in einen Paid-Peering-Vertrag und nimmt währenddessen eine verminderte Dienstqualität bei gemeinsamen Kunden in Kauf. Besonders bemerkenswert ist der in der Folge öffentlich ausgetragene Schlagabtausch zwischen Verizon, Netflix und dem ebenfalls beteiligten Tier1-Provider Level3, insbesondere da zu diesem Zeitpunkt bereits eine Einigung erzielt wurde. Der Vorfall bietet einen tiefgründigen Einblick in technische und wirtschaftliche Mittel, mit denen Differenzen in der Internet-Branche ausgetragen werden.

Konsequenzen und Auswirkungen Im Netflix-eigenen Provider-Vergleich zeigt sich mit Aufnahme des Paid-Peerings eine deutliche Verbesserung der Dienstqualität für Verizon-Kunden, was auch zur Beilegung des öffentlichen Streits führt. Aufgrund dieses und ähn-

[26] `https://ispspeedindex.netflix.com/country/us/`

lich gelagerter Fälle kündigte die Regulierungsbehörde FCC an, künftig Peering-Verträge stärker zu überwachen, um den Missbrauch einer Vormachtstellung am Markt zulasten von Endanwendern zu unterbinden. Netflix treibt in der Zwischenzeit den Ausbau seines eigenen CDNs weiter voran, um unabhängiger von großen Providern zu werden.

Schutz- und Gegenmaßnahmen Technisch gesehen sind keine geeignete Schutz- und Gegenmaßnahmen vorhanden, um die negativen Effekte eines Peering-Streits für das eigene Netz abzumildern. Kapazitätserweiterungen zwischen Netzbetreibern sind in der Regel zwar kurzfristig realisierbar, jedoch im Zuge von Machtkämpfen nicht immer gewollt. Aus Sicht einzelner Endanwender besteht zwar generell die Möglichkeit eines Anbieterwechsels, was allerdings mit großem zeitlichen Aufwand und oft auch mit einem längeren Ausfall des eigenen Internet-Anschlusses verbunden ist. In Einzelfällen kann die Nutzung eines Virtual Private Networks (VPN) Abhilfe verschaffen, da hiermit Quelle und Art des vom Peering-Streit betroffenen Verkehrs verborgen und dieser über das unabhängige Netz eines VPN-Anbieters geleitet werden kann. Dies führt meist jedoch zu zusätzlichen Kosten. Die einzige Möglichkeit, wirtschaftlich motivierte Qualitätseinbußen zu vermeiden, besteht in einer klaren Gesetzgebung zur Netzneutralität mitsamt Maßnahmen für deren konsequente Durchsetzung, um den Missbrauch von Marktmächten einzelner ISPs oder Content-Anbietern in Zukunft dauerhaft zu unterbinden.

Wesentliche Erkenntnisse Aufgrund der unzureichenden Datenlage des weit zurückliegenden Vorfalls kann der Aufbau der Paid-Peering-Verbindung nicht direkt nachvollzogen werden. Im Netflix-eigenen Provider-Ranking zeigt sich jedoch eine deutliche Verbesserung der Dienstqualität. Gleichzeitig ist über Routing-Analysen ein langfristig angelegter Zuwachs des Netzes von Netflix zu verzeichnen, sowohl in Größe als auch Qualität der Anbindung. Beides sind klare Indizien für den verstärkt vorangetriebenen Ausbau eines eigenen CDN-Dienstes und damit einer Änderung der Peering-Strategie von Netflix.

Einschätzung: Durch die in der Europäischen Union seit 2015 geltende Verordnung zur Netzneutralität [27] *ist in Deutschland derzeit nicht mit ähnlichen Machtkämpfen zu rechnen. Netzbetreiber dürfen weder gezielt Dienste benachteiligen, noch sind sie rechtlich legitimiert, Dienste ohne Vorhaltung ausreichender Kapazitäten für den restlichen Datenverkehr zu bevorzugen. Seit Inkrafttreten der Verordnung wurden bereits mehrere Verstöße unterbunden [45]. Ungeachtet dessen führt die zunehmende Abhängigkeit der deutschen Internet-Landschaft von internationalen Dienstanbietern auch weiterhin zu Risiken im Hinblick auf eine mögliche Benachteiligung deutscher Verkehrsströme außerhalb der Europäischen Grenzen. Dies gilt umso mehr seit der Abkehr der US-amerikanischen Regulierungsbehörde FCC von der Netzneutralität im Jahr 2017* [28].

[27] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32015R2120&from=EN

[28] https://netzpolitik.org/2017/schwarzer-tag-fuers-internet-usa-demolieren-netzneutralitaet/

2.3 Zusammenfassung

Mit Hilfe einer methodischen Auswertung von über Hundert realen Internet-Vorfällen wurden konkrete Gefahrenquellen für den Internet-Backbone identifiziert und in einem kategorisierten Vorfallskatalog gebündelt. Isolierte Ausfälle weisen demnach eine hohe Eintrittserwartung auf, die daraus resultierenden Schäden sind jedoch meist begrenzt. Unerwünschte Verkehrsumleitungen hingegen bergen ein hohes Schadenspotential, treten aber in der Praxis weniger häufig auf. Das größte Risiko im Internet geht sowohl in Bezug auf die Eintrittserwartung als auch auf mögliche Schäden von gezielten Angriffen aus.

Basierend auf den gewonnenen Erkenntnissen wurden Defizite bestehender Schutz- und Gegenmaßnahmen erörtert und konkrete Verbesserungspotentiale aufgezeigt. Schließlich wurden Handlungsmöglichkeiten für die deutsche Internet-Infrastruktur diskutiert und dabei die Sicherstellung eines einfachen, aber flächendeckenden Basisschutzes empfohlen.

Im weiteren Verlauf wurden fünf besonders lehrreiche Fallbeispiele herausgegriffen und in großem Detail analysiert. Neben einer manuellen Recherche des jeweiligen Vorfallshergangs und der Aufarbeitung wissenschaftlicher Arbeiten konnten insbesondere durch messgestützte Analysen wertvolle Einblicke in Ursachen und Auswirkungen der betrachteten Vorfälle gewonnen werden. Zwar konnte nicht jeder Ausfall vollständig anhand der verfügbaren Messdatenlage nachvollzogen werden. Durch manuelle Hinzunahme weiterer öffentlich zugänglicher Datenquellen ließen sich Beobachtungslücken jedoch in allen Fällen zuverlässig kompensieren und darüber gleichzeitig bisherige Erkenntnisse bestätigen.

Anhand der vielfältigen Analyseergebnisse wurden charakteristische Besonderheiten der jeweiligen Vorfälle herausgearbeitet und die jeweils fallspezifische Anwendbarkeit der verfügbaren Schutz- und Gegenmaßnahmen untersucht. Im Rahmen einer abschließenden Einschätzung wurde die Übertragbarkeit der einzelnen Vorfälle auf die deutsche Internet-Landschaft diskutiert und Ausblicke auf zukünftig zu erwartende Entwicklungen gegeben.

Durch die Bereitstellung einer umfassenden Web-Anwendung zur interaktiven Betrachtung aller Analyseergebnisse konnten wertvolle Erfahrungen mit einer teilautomatisierten Vorfallsanalyse gesammelt werden. Zukünftig ließe sich darauf aufbauend ein öffentlich zugängliches Werkzeug konzipieren, mit dessen Hilfe Vorfälle gemeinschaftlich gesammelt und vollautomatisiert ausgewertet werden können. Anhand von qualitativen und quantitativen Ergebnissen wären dadurch sowohl detaillierte Einblicke in einzelne Vorfälle möglich als auch längerfristige Entwicklungen und Trends zuverlässig erkennbar. Kombiniert mit einer Ausweitung von Schutz- und Gegenmaßnahmen kann nicht zuletzt auch das Wissen um Gefahren im Internet selbst einen wichtigen Beitrag zur Verbesserung der Sicherheit der deutschen Internet-Landschaft leisten.

Kapitel 3

Fiktive Ausfallszenarien

Dieser Abschnitt ist Fallstudien gewidment, die fiktive Ausfälle relevanter Internet-Infrastruktur analysieren. Auf der Grundlage bekannter Vorfälle und Erfahrungen werden die Ausfälle konkretisiert, ihre Eintrittsmöglichkeiten und -wahrscheinlichkeiten evaluiert sowie ihre Auswirkungen qualitativ und quantitativ eingeschätzt. Konkret werden die Fälle

1. Totalausfall einer internationalen Kabelverbindung
2. Ausfall aller Transitverbindungen durch ein Land
3. DDoS-Angriff auf einen zentralen Internetdienst
4. Totalausfall eines wichtigen Internetknotenpunktes

behandelt. Dabei werden in diesem Kapitel insbesondere viele Detailabläufe ausgearbeitet, welche die genannten fiktiven Ausfälle ganz oder teilweise bewirken könnten. Für jedes Detailszenario werden Auswirkungen und erwartete Dauer sowie konkrete Maßnahmen zur Schadensbehebung diskutiert.

3.1 Methodisches Vorgehen

3.1.1 Allgemeiner Analyseansatz

Die Studie nähert sich den fiktiven Ausfallszenarien in vier Schritten: Zunächst sammeln wir die verfügbaren Informationen und fassen die Auswirkungen und möglichen Ursachen des jeweiligen Ausfallszenarios in einer Vorfallsübersicht zusammen. Hiernach stellen wir im Detail die Ausgangssituation und Rolle der betroffenen Systemkomponente(n) dar und diskutieren ihre Bedeutung im globalen und regionalen Internet-Kontext. Im dritten Schritt evaluieren wir auf der Basis von passiven und aktiven Messungen sowie von Analysen weiterer verfügbarer Daten und Studien empirisch die möglichen Reichweiten und Auswirkungen der betrachteten Vorfälle. Schließlich werden mögliche Ursachen, deren Auswirkungen und Schutzmaßnahmen im Detail beleuchtet.

Analog zu den vorgestellten realen Vorfällen kategorisieren wir die konkreten möglichen Ursachen folgendermaßen:

- BGP-Hijacking
- Denial-of-Service
- Hacking-Angriff
- Kabelschäden
- Menschlicher Fehler
- Peering Dispute
- Route Leak
- Software-Fehler
- Staatliche Aktion
- Technischer Defekt

Findet die jeweilige Kategorie in dem Ausfallszenario Anwendung, so werden ausgewählte zugehörigen Hergänge und Ausfallursachen gemeinsam mit Beschreibungen ihrer erwarteten Dauer und möglichen Gegenmaßnahmen in einer differenzierten Darstellung diskutiert.

3.1.2 Verwendete Daten und ZwIBACK-Messstudien

Die Studie greift zum einen auf öffentlich verfügbare Dokumentationen und Darstellungen sowie veröffentlichte wissenschaftliche Studien (s. Bibliographie) zurück, zum anderen werden publizierte und auch im Rahmen von ZwIBACK gezielt gemessene Daten ausgewertet und analysiert.

Folgende Daten werden verwendet:

BGP Route Daten: Hier werden öffentliche Route-Server und Looking Glasses ausgelesen sowie die Tabellen unserer eigenen Peering-Infrastruktur analysiert.

Aktive Pfadmessungen: Aus unserer verteilten Meßinfrastrukutr heraus wird das Internet-Forwarding mithilfe aktiver Traceroute-Messungen erfasst.

Peering-Monitore: Dies sind insbesondere PeeringDB[1], Packet Clearing House (PCH)[2], IXPDB[3], und Hurricane Electric reports (HE)[4].

RIR-Datensätze: Die Daten der Regional Registries dienen zur Identifikation von Providern, Netzwerken und ihrer geographischen Zuordnung.

DNS Daten: Im Rahmen umfangreicher aktiver Messungen werden Namensauflösungen vorwärts und rückwärte im Domain Name System durchgeführt.

Top-Listen von populären Webservern: Populare Webdienste werden mithilfe der Top-Listen Alexa[5], Umbrella[6] und Majestic[7] (jew. 1.000 und 1 Million) identifiziert.

[1] `https://www.peeringdb.com/`(02.2020)
[2] `https://www.pch.net/ixp/dir`(02.2020)
[3] `https://ixpdb.euro-ix.net/en/`(02.2020)
[4] `https://bgp.he.net/report/exchanges`(02.2020)
[5] `https://www.alexa.com/topsites`(05.2020)
[6] `https://umbrella.cisco.com/blog/cisco-umbrella-1-million`(05.2020)
[7] `https://majestic.com/reports/majestic-million/`(05.2020)

Die verschiedenen Messungen und Datenanalysen werden jeweils im inhaltlichen Zusammenhang im Detail erläutert.

3.2 Totalausfall internationaler Kabelverbindungen

3.2.1 Kurzdarstellung

Transatlantische Seekabel gehören zu den tragenden Säulen internationaler Kommunikationsinfrastrukturen, da sie die Kommunikationsnetze zwischen dem europäischen und dem amerikanischen Kontinent verbinden und den (umfangreichen) bilateralen Datenverkehr übertragen. Ihre Errichtung und ihr Betrieb sind teuer, deshalb bleibt die Anzahl von Seekabeln in der Regel beschränkt und der Ausfall eines einzelnen kann zu empfindlichen Einbußen in der Übertragungskapazität zwischen den Kontinenten führen. TAT-14, welches hier betrachtet werden soll, zählt zu den leistungsfähigsten Überssee-Übertragungskanälen der frühen 2000-er Jahre. Auch wenn der Betrieb von TAT-14 am 15. Dezember 2020 eingestellt wurde, dient das Kabel aufgrund seiner langjährigen Nutzung als gutes Beispiel für mögliche Auswirkungen des Totalausfalls einer internationalen Kabelverbindung.

Dieses fiktive Szenario nimmt an, dass Kommunikationsverbindungen über das transatlantische Unterseekabel TAT-14 gestört werden. Wir betrachten unterschiedliche Störungsursachen im Rahmen von TAT-14: von Beschädigungen des Kabels bis zu Fehlern in den Vermittlungskomponenten. TAT-14 ist sowohl für die Deutsche Telekom AG, als auch für diverse andere europäische, amerikanische wie asiatische Provider relevant. Entsprechend führt ein Ausfall dieses Überseekabels zu Veränderungen im Routing und zu Kapazitätsverlusten bei den betroffenen Providern.

Potentielle Schwachstellen Überseekabel bilden eine fragile physische Infrastruktur, welche sowohl zu Lande wie unter Wasser leicht beschädigt werden können. Reparaturen an diesen Kabeln sind teuer und langwierig. Entsprechend bilden Verletzungen der physischen Komponenten die größte Bedrohung dieser Kabel. Darüber hinaus konzentieren die Kabel den Datentransfer zwischen Ländern und Kontinenten, was sie zu einem besonders einfachen Zugriffspunkt für geheimdienstliche Abhörung macht. Ebenfalls beachtenswert ist in diesem Kontext das Management eines komplexen, multinationalen Betreiberkonsortiums, welches u.U. im Dissenz zerbrechen kann.

Auswirkungen Der Ausfall des Überseekabels TAT-14 bedeutet zuvorderst einen Ausfall von Übertragungskapazität. Während in den frühen 2000-er Jahren die Kapazitäten von TAT-14 am Markt noch signifikant waren, haben in der kürzeren Vergangenheit verschiedene Konsortien, u.a. auch die großen Over the Top (OTT) Service Provider neue Kabel gebaut bzw. Kabelprojekte gestartet, welche die Übertragungsleistung von TAT-14 bei weitem übertreffen. Insofern gerät die leistungskritische Bedeutung von TAT-14 zunehmend in den Hintergrund.

3.2.2 Ausgangssituation

Das transatlantische Unterseekabel TAT-14 (*Transatlantic Telecommunications Cable no. 14*) ist eines von mindestens 471 Unterseekabeln weltweit[8]. Es wurde am 21. März 2001 in Betrieb genommen und ursprünglich von 50 Telekommunikationsunternehmen verlegt; darunter die Deutsche Telekom, die sich mit 10% an den Baukosten beteiligte. Momentan gibt es 31 Konsortiumsmitglieder mit unterschiedlichen Beteiligungsverhältnissen (siehe Tabelle 3.1).

TAT-14 besteht aus acht Glasfasern. Zwei Fasern werden für eine bidirektionale Kommunikation benötigt und gehören jeweils zu einem Paar. Insgesamt umfasst TAT-14 also vier Glasfaserpaare. Es verbindet die USA mit dem Vereinigten Königreich, Frankreich, den Niederlanden, Deutschland und Dänemark. Die Paare sind als Ring verlegt (siehe Abb. 3.1), so dass bei einem Kabelbruch noch alle Knoten erreicht werden können. Die mögliche Gesamtkapazität beträgt 9,38 Tb/s. Momentan sind bis zu 3,15 Tb/s nutzbar. Der verbleibende Kapazität wird als Reserve vorgehalten.

Unterseekabeln kommen nicht nur aufgrund ihrer hohen Übertragungsraten für die transkontinentale Kommunikation eine wichtige Bedeutung zu. Im Vergleich zu einer Verbindung mittels Satellit ist die Verzögerung um eine Größenordnung geringer.

Die Faserpaare sind durch Stahlarmaturen, Metallmantel und mehrere Kuststoffschichten geschützt. In geringer Tiefe liegen solche Kabel in einer separaten Wanne. Ab einer Meerestiefe von 1000 Metern liegt das Kabel aber ohne weiteren Schutz auf dem Meeresgrund. Häufige Gefahren für Beschädigungen gehen von Schleppnetzen und Schiffsankern aus, obgleich die Verlegung kartographiert ist. Ebenfalls können Großfische wie z.B. Haie Kabel beschädigen.

Ein Teil des TAT-14 Ringes verläuft südlich über Frankreich, der andere nördlich über Dänemark. Der Ausfall eines einzelnen Fasernpaares sollte demnach zu keinen spürbaren Störungen führen.

Die über das Unterseekabel übertragenen Signale werden durch Verstärker aufgewertet, welche in die Kabel eingebaut sind. An den Anlandungspunkten befinden sich sogenannten *Wavelength-Division Multiplexing (WDM)* Systeme, die es erlauben, eine einzelne Glasfaser durch Frequenzmultiplexing mehrfach zu nutzen. Hierbei werden unterschiedliche Wellenlängen erzeugt.

Fiktiver Ausfall TAT-14 Das folgende Fallbeispiel zeigt die von einem fiktiven Ausfall der transatlantischen Kabelverbindung TAT-14 betroffenen Internet-Ressourcen aus Sicht der Deutschen Telekom. Im Rahmen von ZwIBACK wurden die betroffenen IP-Präfixe mittels Internet-weiten IP-Pfadmessungen über das Netz der Deutschen Telekom identifiziert und die Router-Infrastruktur aufgedeckt.

Im Detail wurden die Ziel-IP-Adressen aller über TAT-14 gerouteten IP-Pfadmessungen auf die entsprechenden *most specific* IP-Präfixe, die im BGP Routing sichtbar sind, abgebildet. Die für TAT-14 relevanten IP-Router innerhalb des Netzes der Deutschen Telekom, und damit die relevanten IP-Pfadmessungen, wurden über statistische Auswertungen (siehe Abschnitt Infrastruktur) eingegrenzt und manuell recherchiert. Basierend

[8] `https://www.submarinecablemap.com/`

# Sitze im Generalausschuss	Unternehmen	Länder
4	AT&T	USA
4	CENTURY LINK	UK, USA
3	VERIZON	UK, USA
3	BT	UK
3	ORANGE	France
3	OTEGLOBE	Greece
3	SINGTEL	Singapore
3	VODAFONE	UK
3	ZAYO	USA
2	SOFTBANK	Japan
2	SPRINT	USA
2	STARHUB	Singapore
2	ETISALAT	UAE
2	GTT/KPN	The Netherlands
2	KDDI CORP	USA
2	MEO	Portugal
2	TURK TELECOM	Turkey
1	BICS	Belgium
1	CYTA	Cyprus
1	DTAG	Germany
1	STSE/DTAG	Slovak Republic
1	ELISA	Finland
1	ROSTELECOM	Russia
1	TATA	India
1	TATA	UK
1	TDC A/S	Denmark
1	TELE2	Sweden
1	TELENOR	Norway
1	TELESUR	Suriname
1	TELUS	Canada
1	TLFN	Spain
1	TSIC	Denmark

Tabelle 3.1: Verteilung der Firmen und ihrer Sitze im TAT-14 Generalausschuss. Die Anzahl der Sitze dient als Approximation der Anteilsverhältnisse. (Quelle: `https://www.tat-14.com/tat14/gclist.jsp`)

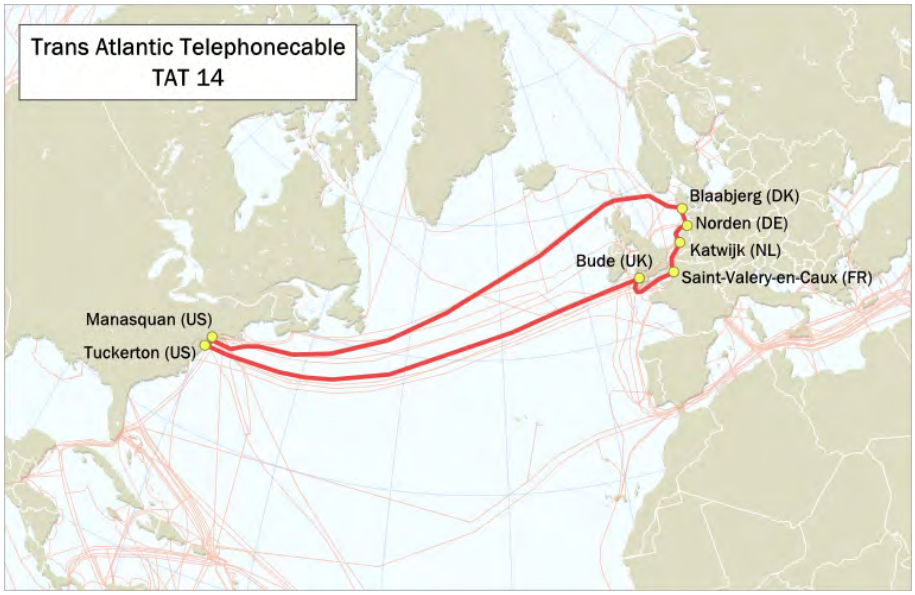


Abbildung 3.1: Verlauf des Transatlantik-Kabels Nr. 14, TAT-14 (Quelle: Wikipedia)

	Ziel ASNs	IP–Präfixe	/24–Äquivalente
Betroffen von TAT-14	7,821	58,769	1,675,192
Gesamtheit im Internet	67,616	800,103	11,153,424

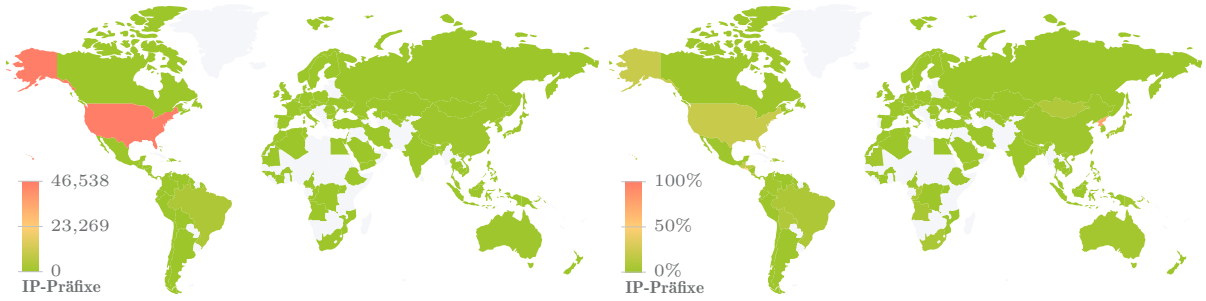
Tabelle 3.2: Anteil der von einem TAT-14 Ausfall betroffenen Internet-Resourcen

auf den Messungen in ZwIBACK wurden am Anlandungspunkt in Norden (Deutschland) zwei redundante Router der Deutschen Telekom identifiziert. Diese werden jeweils für Verbindungen in beide Richtungen des Kabels, d.h. Richtung New York und Richtung Washington, betrieben. Für IPv6 konnten wir keine entsprechenden Router identifizieren.

3.2.3 Auswirkungen und mögliche Reichweiten

Ein Totalausfall des Transatlantikkabels bedeutet zunächst, dass der bestehende Datenverkehr für die beteiligten Transitprovider abbricht und durch Re-Routing neue Wege gefunden werden müssen. Tabelle 3.2 zeigt eine Übersicht über die betroffenen Internet-Resourcen. Hierbei wird die charakteristische Nutzung durch große Provider deutlich: Während 11% der Autonomen System bzw. 7% der IP-Präfixe von dem Ausfall betroffen wären, umfassen diese 15% des weltweiten IP-Adressraums; die über das Kabel gerouteten Präfixe sind also überdurchschnittlich groß.

Die geographische Verteilung der betroffenen IP-Präfixe ist in Abb. 3.2 dargestellt. Wir unterscheiden hierbei zwischen der Anzahl der absoluten IP-Präfixe (siehe Abb. 3.2a) und einer prozentualen Bewertung relativ zu der Gesamtanzahl an IP-Adressen pro Land (siehe Abb. 3.2b). Naturgemäß würde sich ein Ausfall auf die USA konzentrieren. Andere Länder in Nord-, Mittel und Südamerika sind stärker von anderen transatlantischen Kabeln abhängig. Es sind nur 176 kanadische Präfixe betroffen, jedoch auch drei (von vier) nordkoreanischen Präfixen. Neben den Vereinigten Staaten verknüpft TAT-14 Euro-



(a) Absolut (b) Relativ

Abbildung 3.2: Geographische Verteilung aller vom Ausfall betroffenen IP-Präfixe bei einem Ausfall von TAT-14. Die relative Darstellung zeigt den Anteil der betroffenen IP-Adressen normiert über die Gesamtanzahl an IP-Adressen pro Land.

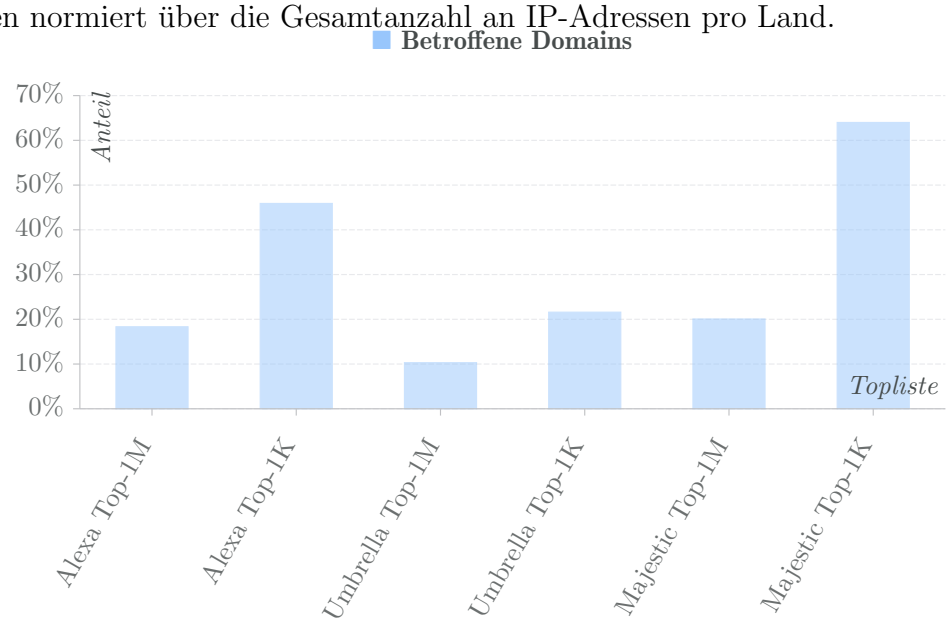


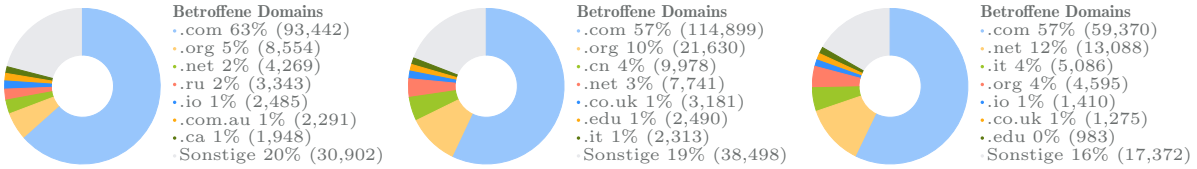
Abbildung 3.3: Relativer Anteil der betroffenen DNS Domains aus öffentlichen Toplisten bei einem Ausfall von TAT-14.

pa auch mit diversen autonomen Systemen in Lateinamerika, insbesondere in Brasilien, wo 578 (8%) ASes über TAT-14 angesteuert werden.

Insgesamt konnten 451,143 Domains identifziert werden, die populäre Webserver beherbergen und über TAT-14 erreichbar sind. Diese lassen sich 1.290 Top-level Domains zuordnen. Der realtive Anteil der 1 Million populären Web-Server ist in Abb. 3.3 dargestellt. Diese Angaben schwanken allerdings stark zwischen den Top-Listen, was listentypisch ist [46]. Die Alexa-Liste unterliegt zudem häufig zeitlichen Schwankungen, so dass sich das Ranking inbesondere für weniger populäre Webseiten stärker ändern kann. Zwischen ≈10% und ≈60% der Domains wären im schlimmsten Fall von einem Ausfall betroffen. Dieses Worst-Case-Szenario berücksichtigt nicht den Betrieb von IP-Präfixen über Anycast Routing, d.h. dass eine IP-Adresse an unterschiedlichen Orten lokalisiert ist. Viele Content Delivery Netzwerke nutzen aber Anycast, so dass bei einem tatsächlichen Ausfall in der Praxis vermutlich weniger Domains betroffen sein werden.

Mit dem Ausfall des TAT-14 Kabels geht neben den diskutierten Routen vor allem Übertragungskapazität verloren. Im Kontext der kooperativ von Telekommunikationsfirmen betriebenen Trans-Atlantik Telephonecables (TATs) nimmt TAT-14 mit seiner Kapazität im Terabit-Bereich eine herausragende Stellung ein: Die traditionellen Telefonkabel übertragen sonst in Größenordnungen von Mbit/s bzw. Gbit/s. In den letzten Jahren sind jedoch viele Datenkabel von einzelnen Betreibern (oder kleinen Konsortien) in Betrieb genommen worden. Diese *Private Cable Routes* verfügen z.T. über Kapazitäten im hohen Terabit-Bereich, wie z.B. MAREA (160 Tbit/s) oder das für dieses Jahr angekündigte Google-Kabel Dunant (250 Tbit/s). Betrachtet man diese Kapazitäten zusammen, beschränkt sich der Anteil von TAT-14 auf 0.7% der transatlantischen Datenkapazität. Gemessen an der Datenkapazität reduziert sich die Bedeutung von TAT-14 also. Entscheidend ist aber, dass TAT-14 primär von einem Konsortium getrieben ist, das keinen spezifischen Inhaltsdienst (wie Google oder Facebook) anbietet, und somit langfristig eine höhere Neutralität gewährleisten könnte.

Domain Namen, die von einem TAT-14 Ausfall betroffen sind, werden differenziert nach den Top-1-Million Listen Alexa, Majestic und Umbrella in Abb. 3.4 statistisch dargestellt. Dominant stehen hier kommerzielle `.com` Domainen im Fokus, während nachfolgende Ränge stark mit den Listenerhebungen variieren. Vom Ausfall betroffene Domainen erleben eine Wegeumleitung und ggfs. Einbußen in der Zugriffsgeschwindigkeit.



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.4: Anteil der betroffenen Domains je Top-Level-Domain bei einem Ausfall von TAT-14.

3.2.4 Mögliche Ausfallszenarien

Typ	Szenario	Verwandt	Betroffen	Behebung	Dauer	Reichweite
Denial-of-Service	Gezielter Angriff auf nachgeschaltete DTAG Core-Router	[I83]	Datenschicht	Intern	m	–
Kabelschäden	Beschädigung durch Schleppnetze in der Nordsee	[I40, I41, I42, I43, I44, I46]	Infrastruktur	Extern	d	o
Kabelschäden	Natürliche Einflüsse (Verbiss, Erdbeben, Korrosion)	[I40, I40, I43, I44, I45, I46, I47]	Infrastruktur	Extern	d	+
Menschlicher Fehler	Fehlerhafte Rekonfiguration eines optischen Multiplexers	[I17, I19, I22]	Management	Intern	m	o
Peering Dispute	Zerfall des Betreiber-Konsortiums aufgrund eines Rechtsstreits	[I48, I54, I55, I56]	Infrastruktur	Extern	∞	o
Software-Fehler	DWDM-Absturz nach Firmware-Upgrade eines Transponders	[I36, I38]	Infrastruktur	Intern	h	o
Staatliche Aktion	Sabotage der Kommunikation durch US-Sicherheitsbehörden	[I101, I103, I105, I106, I107]	Infrastruktur	Extern	∞	+
Technischer Defekt	Beschädigung durch Bauarbeiten in Norden auf Ostfriesland	[I40, I41, I42, I43, I44, I46]	Infrastruktur	Service	h	+
Technischer Defekt	Ausfall von Repeatern durch Sonnenstürme	—	Infrastruktur	Intern	w	+

3.2.5 Detailanalysen

Gezielter Angriff auf nachgeschaltete DTAG Core-Router
Denial-of-Service

Beschreibung Ein Angreifer setzt gezielt einen der am Anlandungspunkt befindlichen Router außer Kraft, so dass über diesen keine weiteren Daten geschickt werden können.

Betroffener Bereich (Datenschicht) Alle Dienste oberhalb der IP-Schicht.

Auswirkung und Reichweite (–) Der Schaden ist gering, wenn bei dem Backup-Konzept beide Router ausreichend provisioniert wurden.

Dauer (m) Über Interior-Routing-Protokoll lassen sich dynamisch innerhalb kurzer Zeit die Wege über den Backup-Router propagieren.

Fehlerbehebung (Intern) Unseren Messungen zufolge betreibt die Deutsche Telekom zwei Router pro Anlandungspunkt. Wenn einer der Router angegriffen wird, können die Daten über den Backup-Router verteilt werden.

Beschädigung durch Schleppnetze in der Nordsee
Kabelschäden

Beschreibung Nordseefischer missachten die Kabelschutzzone und brechen das Kabel in der Nordsee mit sich verfangenden Schleppnetzen.

Betroffener Bereich (Infrastruktur) Die Kommunikation bricht auf dem beschädigten Unterseekabel ab, denn die intakte Glasfaser ist die Basis für alle darüberliegenden Signale.

Auswirkung und Reichweite (o) Das TAT-14 Kabel ist redundant als Ring ausgelegt und es ist wenig wahrscheinlich, dass beide Teile des Rings gemeinsam zerstört werden. Ist der Nordring gestört, liessen sich Daten (deutlich verzögert) über den Südring versenden.

Dauer (d) Die Reparatur des Kabels in der See ist aufwändig und erfordert Tage, schlimmstenfalls Wochen. Der komplette Ausfall kann aber durch Konfigurationsänderungen zeitnah überbrückt werden.

Fehlerbehebung (Extern) Die Reparatur eines solchen Kabels in der See erfordert in der Regel den Einsatz spezieller Schiffe und wird durch externe Aufträge ausgeführt.

Eine Rekonfiguration des Kabelrings kann intern erfolgen. Bei langanhaltenden, flächigen Schäden lassen sich auch Satellitenübergänge für einen sehr eingeschränkten Teil der Internet-Dienste und -Nutzer in Betracht ziehen.

Natürliche Einflüsse (Verbiss, Erdbeben, Korrosion)
Kabelschäden

Beschreibung Das Kabel wird im Meer durch natürliche Einflüsse beschädigt. Diese Schäden können sowohl lokal als auch großflächig sein. Insbesondere bei schweren Naturkatastrophen wie Erdbeben kann dies zur Beschädigung beider Ringteile führen.

Betroffener Bereich (Infrastruktur) Die optische Übertragungsschicht ist ganz oder in Teilen betroffen, wodurch ein Datenaustausch darüber unterbrochen wird.

Auswirkung und Reichweite (+) Das TAT-14 besteht aus vier Glasfaserpaaren, die einzeln geschützt sind. Entsprechende Schäden sollten sich zeitnah durch die Überwachung der Signalausbreitung erkennen lassen. Der Ausfall aller Faserpaare hat jedoch eine umfangreiche Verkehrsflussveränderung zur Folge.

Dauer (d) Schäden durch Verbiss oder Korrission sollten bei einem Transatlantikkabel geringfügige Auswirkungen haben. Dennoch ist die Reparatur des Schadens unter Wasser aufwändig und erfordert Tage bis Wochen.

Erdbeben hingegen können deutlich komplexere Schäden hervorrufen, die nicht nur ein Kabelteil, sondern weite Bereich bis hin zu den Anlandungsstationen betreffen. Entsprechende Reparaturarbeiten sind langwierig, wobei die Ausfälle durch Verkehrsumleitungen kompensiert werden.

Fehlerbehebung (Extern) Die Reparatur des Kabels in der See erfordert in der Regel den Einsatz spezieller Schiffe und wird durch externe Aufträge ausgeführt.

Lokale Schäden können durch interne Rekonfiguration des Kabelrings überbrückt werden. Der komplette Ausfall kann durch ein Umrouten zeitnah überbrückt werden. Bei langanhaltenden, flächigen Schäden im Atlantik lassen sich auch Satellitenübergänge für einen sehr eingeschränkten Teil der Internet-Dienste und -Nutzer in Betracht ziehen.

Fehlerhafte Rekonfiguration eines optischen Multiplexers
Menschlicher Fehler

Beschreibung Ein optischer Multiplexer setzt unterschiedliche Wellenlängen über einen einzelnen Lichtwellenleiter (Faser) um. Dafür werden unterschiedliche Eingangssignale, welche über getrennte Ports eingehen, jeweils einer Wellenlänge (Farbe) zugeordnet. Jede Wellenlänge entspricht somit einem Übertragungskanal. Damit können über eine Faser mehrere Kanäle physikalisch differenziert werden.

Ein Techniker konfiguriert den optischen Multiplexer derart, dass die Wellenlängen zwischen Sende- und Empfangseinheit nicht mehr abgestimmt sind. Der Techniker nutzt eine Wellenlänge, z.B. „rot“ statt „grün“, welche beim Demultiplexer nicht bekannt ist. Dadurch können sich die Kommunikationsgegenstellen nicht mehr synchronisieren und keine optische Verbindung miteinander aufbauen. Über die Wellenlänge ist ein anderer Internet Service Providre angebunden.

Betroffener Bereich (Management) Primär ist das Management von Multi- und Demultiplexer betroffen sowie alle von einem funktionierenden Management abhängigen Dienste, d.h. alle Kommunikationsdienste oberhalb des DWDM-Systems, also der physischen Übertragungsschicht, welche über die fehlkonfigurierte Wellenlänge angebunden sind. In der Regel werden Wellenlängen bestimmten Service Providern und nicht dedizierten Anwendungen zugewiesen.

Auswirkung und Reichweite (o) Die Fehlkonfiguration eines Multiplexers hat zur Folge, dass die Signale nicht mehr richtig codiert werden können. Entsprechend lässt sich auf der optischen Schicht keine Verbindung aufbauen, wodurch alle darüberliegenden Netzwerkschichten betroffen sind.

In unserem Beispiel würde die Kommunikation zu einem ISP entfallen. Das betrifft nicht nur Endkunden des ISPs, sondern auch Kunden, die Transit einkaufen. Sollte wäh-

rend des Ausfalls z.B. eine Kunde der Deutschen Telekom eine Webseite bei AT&T aufrufen, würde dies zu Fehlern führen. Ebenfalls könnten Bestellungen bei kleineren ausländischen Webshops nicht funktionieren, da diese ihre Dienste in der Regel nicht über lokale Content-Netzwerke replizieren, also auf eine funktionierende Überseeleitung angewiesen sind.

Dauer (m) Solche Fehler können nach der Neukonfiguration sofort erkannt werden, da die Multiplexer über Management-Einheiten verfügen, die über Verbindungsaufälle informieren. Der Techniker würde erkennen, dass ein Wellenlängenkanal fehlt.

Die Firmware solcher optischen Multiplexer verfügt in der Regel über umfangreiche Log-Ausgaben, so dass der Fehler schnell eingegrenzt werden kann. Ebenfalls könnte der Techniker durch das Erzeugen und Prüfen der Differenz zwischen neuer und alter Konfiguration den Fehler identifizieren. Konfigurationsdateien werden bei solch wichtigen Geräte offline gesichert und in Versionierungssystemen hinterlegt.

Das Ändern und Einspiel der falschen Konfiguration dauert in der Regel wenige Minuten. sollte der Techniker eine komplexere Werkzeugkette für die Verwaltung der Konfiguration nutzen, lässt sich der Konfigurationsfehler in weniger als einer Stunde beheben.

Fehlerbehebung (Intern) Die Konfiguration des Multiplexers wird von internen Technikern vorgenommen. Dieser kann (auch ohne Zugriff auf den Multiplexer) erst einmal die ursprüngliche, funktionierende Konfiguration wieder herstellen.

Da das TAT-14 Kabel als Ring redundant ausgelegt ist, kann der Fehler einer Strecke zwischenzeitlich über den Backup-Weg des Ringes überbrückt werden. Dies passiert automatisch. Kunden merken davon nichts oder eventuell Latenzänderungen

Zerfall des Betreiber-Konsortiums aufgrund eines Rechtsstreits
Peering Dispute

Beschreibung Momentan gibt es 31 Konsortiumsmitglieder (`https://www.tat-14.com/tat14/gclist.jsp`). Das Konsortium könnte zerfallen, wenn eine kritische Menge an Mitgliedern Investionen anstrebt, die die anderen Mitgliedern nicht zu investieren bereit sind.

Aufgrund der wachsenden Kapazitäten im Bereich der 'Private Cable Routes' ist kein Betreiber bzw. Investor bereit, die Kabelinfrastruktur zu übernehmen.

Betroffener Bereich (Infrastruktur) Das Zersplittern des Konsortiums dürfte vor allem dazu dienen, Druck auf Mitbewerber, die ebenfalls Teil des Konsortiums sind, auszuüben und somit Marktgewichte zu verschieben.

Auswirkung und Reichweite (o) Ein solcher Streit könnte die Marktgewichte verschieben. Wenn ein Konsortiumsmitglied ausscheidet, dann werden dessen Anteile mit sehr hoher Wahrscheinlichkeit einem Mitbewerber übernommen. Die Kosten für den Bau eines neuen Unterseekabels sind deutlich höher als die möglichen Übernahmekonditionen.

Marktveränderungen, die das Konsortium verkleinern bzw. das Kabel ausser Betrieb setzen, können allerdings eine Marktmonopolisierung unterstützen und einseitige Abhängigkeiten erzeugen. Die DTAG z.B. scheint neben TAT-14 an keinem der aktuellen, hochkapazitären Transatlantikkabel beteiligt zu sein.

Dauer (∞) Veränderungen, welche sich aus einem solchen Zerfall ergeben, sind gewöhnlich dauerhaft. Mögliche Streitigkeiten im Konsortium dürften aber alleine zu keiner vollständigen Einstellung des Kabelbetriebs führen. Verträge können üblicherweise nur mit gewissen Fristen aufgelöst werden. Entsprechend sind Veränderungen vorab absehbar und die betroffenen Firmen können durch die Verlagerung von Internet-Routen bzw. dem Kauf alternativer Kapazitäten gegenlenken.

Fehlerbehebung (Extern) Staatliche Übernahmen könnten den (eher unwahrscheinlichen) Zerfall des Gesamtkonsortiums verhindern.

Wird TAT-14 infolge der Konkurrenzkapazitäten unwirtschaftlich, ist eine geordnete Außerbetriebnahme schadlos möglich.

DWDM-Absturz nach Firmware-Upgrade eines Transponders
Software-Fehler

Beschreibung Das DWDM-System (*Dense Wavelength Division Multiplexing*), welches die einzelnen Glasfasern nutzt, um ein optisches Multiplexing zu realisieren, stürzt ab. Damit funktioniert das Frequenzmultiplexing für ein Glasfaserpaar nicht mehr.

Betroffener Bereich (Infrastruktur) Kommunikationsdienste oberhalb des DWDM-Systems, also der physischen Übertragungsschicht.

Auswirkung und Reichweite (o) Die Auswirkungen sind gering, da das TAT-14-Kabel redundant ausgelegt ist. Der Ausfall eines einzelnen Glasfaserpaares sorgt dafür, dass darüber bestehende Verbindungen unterbrochen werden. Die höheren Schichten, wie z.B. TCP oder entsprechende Resilienzmechanismen von Anwendungsprotokollen, kompensieren das Problem. Laufzeitverzögerungen sind für die Reparaturzeit merkbar.

Dauer (h) Das Einspielen der ursprünglichen Firmware dauert wenige Minuten. In unserem Szenario kann der Fehler sofort erkannt werden, da er reproduzierbar unmittelbar nach einem Neustart auftritt. In anderen Fällen geht der Fehlerbehebung eine langwierige Diagnose voran, insbesondere bei schwer reproduzierbaren Software-Bugs.

Fehlerbehebung (Intern) Einspielen der ursprünglichen Firmware. Nutzung des redundanten Ringes während des Ausfalls und der Aktualisierung der Firmware.

Sabotage der Kommunikation durch US-Sicherheitsbehörden
Staatliche Aktion

Beschreibung Das Seekabel wird an einem der Anlandungspunkte von Sicherheitsbehörden angezapft. Hierfür wird das DWDM-System unter Kontrolle gebracht. Die Sicherheitsbehörden haben damit nicht nur die Möglichkeit, Daten mitzulesen, sondern auch Einfluss auf die Weiterleitung der optischen Schicht. Wellenlängen können so systematisch der regulären Weiterleitung entzogen werden.

Betroffener Bereich (Infrastruktur) Betroffen sind insbesondere gesellschaftliche und politische Bereiche.

Auswirkung und Reichweite (+) Passive Angriffe können lange Zeit unentdeckt bleiben. Ihre Reichweite auf den Betrieb ist zwar gering, aber die gesellschaftlich-politischen Folgen sind ggfs. hoch.

Dauer (∞) Wenn die Sabotage ausschließlich passiv erfolgt, d.h. Daten nur mitgelesen werden, kann die Erkennung solcher Vorfälle Jahre dauern. Bei einer aktiven Manipulation, wie z.B. dem Verwerfen von Wellenlängen, brechen optische Links zusammen und die Fehler werden schnell und automatisch entdeckt. Das zufällige Verwerfen von Daten hingegen ist schwer zu erkennen. Selbst bei einem systematischen Verwerfen muss für eine endgültige Klärung eine Rückverfolgung auf den Ausgangspunkt erfolgen, die langwierig sein kann.

Fehlerbehebung (Extern) Sabotagen durch einen Geheimdienst verlangen diplomatische Aktionen. Kurzfristig können die Kommunikationsunternehmen, die das Kabel nutzen, ihre Daten über andere Wege vermitteln. Diese Gegenmaßnahmen verliefen ähnlich zu einem Komplettausfall des Kabels. Der Einsatz von Verschlüsselungsverfahren setzt voraus, dass diese vom Geheimdienst nicht erfolgreich angegriffen werden können. Ebenfalls ist zu betonen, dass Verschlüsselung nicht vor dem Unterbinden des Netzwerkdienstes (z.B. Verwerfen von Paketen) hilft.

Beschädigung durch Bauarbeiten in Norden auf Ostfriesland
Technischer Defekt

Beschreibung Das TAT-14 Kabel ist in zwei Trassen verlegt, welche beide in Norden (Deutschland) beginnen. Eine Trasse führt über die Niederlande, die andere über Dänemark weiter nach Nordamerika. Jede der Trassen fasst zwei Faserpaare.

An den Stellen, an denen beide Trassen in Ostfriesland zusammenkommen, kommt es durch Bauarbeiten zu Beschädigungen der Kabel, so dass alle Glasfaser durchtrennt sind. Hierdurch werden alle Weiterleitungen unterbrochen und der Kabelring an der ostfriesischen Anlandungsstelle unbrauchbar.

Betroffener Bereich (Infrastruktur) Das Unterseekabel ist die Basis für alle darüberliegenden Signale. Mit dem Wegfall der Kabelverbindung können Pakete auf der Netzwerkschicht über diesen Weg nicht mehr weitergeleitet werden. Höherstehende Dienste, wie z.B. Social Media, Webplatfformen sind davon betroffen.

Auswirkung und Reichweite (+) Das TAT-14 Kabel ist redundant als Ring ausgelegt. Da beide Richtungen gestört sind, kann es tatsächlich zu einer Unterbrechung der Datenvermittlung insbesondere in die USA und UK kommen, da die Deutsche Telekom das Kabel für die transkontinentale Kommunikation nutzt.

Dauer (h) Im Gegensatz zu Beschädigungen im Meer, kann das Kabel an Land in Stunden repariert werden, da keine aufwändigen Bergungsarbeiten erfolgen müssen. Hierfür werden die Lichtwellenleiter „gespleißt“. Bei dem Spleißvorgang werden die Enden der zu reparierenden Leitung aufeinandergelegt. Die Justierung erfolgt automatisch über entsprechende Geräte. Nach der Positionierung der Faserenden werden sie „verschweißt“. Sobald die Fasern miteinander verbunden sind, können wieder Daten über die Leitung transportiert werden.

Neben der Reparatur der Fasern müssen noch die Trassen repariert und die Fasern wieder sachgemäß verlegt werden. Dies kann nachläufig erfolgen und betrifft somit die Weiterleitung der Daten über das TAT-14 Kabel nicht.

Im schlimmsten Fall dauert die Reparatur des Kabels Tage, wenn die Bauarbeiten

den Zugang zum Kabel selber unmöglich machen. Der komplette Ausfall kann aber durch Veränderungen von Routen zeitnah überbrückt werden.

Fehlerbehebung (Service) Die Reparatur des Kabels wird in der Regel über Service-Dienstleister durchgeführt. Aufgrund der Wichtigkeit des Anlandungspunktes kann davon ausgegangen werden, dass ein Service Team in näherer Umgebung verfügbar ist. Fahrtzeiten entstehen, werden aber als nicht signifikant (d.h. maximal wenige Stunden) eingeschätzt.

Das Umrouten über andere Peerings, welche auf anderen Transatlantikkabel verlaufen, kann intern erfolgen. Hierfür werden die betroffenen IP-Präfixe über BGP an anderen Internet-Knotenpunkte annonciert. Alternativ bestehen bereits Ersatzrouten. Diese werden automatisch aktiv, wenn die Routen-Bekanntgabe über das beschädigte Kabel unterbrochen ist.

Ausfall von Repeatern durch Sonnenstürme
Technischer Defekt

Beschreibung Bestimmte Sonneneruptionen können die Ausstrahlung von geladener Materie und magnetischen Feldern zur Folge haben. Wenn diese die Erde treffen, kann es zu geomagnetisch induzierten Strömen kommen, die wiederum elektrische Leitungen oder Geräte beschädigen [47]. Betroffen sind insbesondere Orte höherer Breitengrade. Diese korrelieren mit optischen Repeatern für Unterseekabeln.

Betroffener Bereich (Infrastruktur) Da nicht nur ein Unterseekabel betroffen wäre, würde das Internet teilweise fragmentiert werden, wenn nicht auf Caches zurückgegriffen werden kann. Basierend auf aktuellen Studien [47] wären die Rechenzentren von Facebook stärker betroffen im Vergleich zu Google, da Google in Asien und Südamerika besser verteilt ist.

Auswirkung und Reichweite (+) Der Ausfall mehrerer Repeater kann die optische Übertragung an mehreren Stellen unterbrechen, so dass die Redundanz eines Kabels nicht zum Tragen kommt. Unterseekabel sind besonders von Sonnenstürmen betroffen [47]. Die Konnektivität zwischen Nordamerika und Europa würde besonders Schaden nehmen. DNS-Root-Server wären aufgrund ihrer Verteilung nicht betroffen.

57% der autonomen Systeme haben einen Point-of-Presence in einem der betroffenen Gebiete [47]. Ein autonomes System, das weit verteilte Router betreibt, wäre von einem solchen Ausfall besonders stark betroffen.

Dauer (w) Die Lebenszeit eines Repeaters für Unterseekabel wird auf 25 Jahre geschätzt. Die Reperatur oder der Austausch verlangt den Einsatz von Schiffen und kann Tage bis Wochen dauern. Bisher gibt es keine Stresstests für den Ausfall von Repeatern durch Sonnenstürme. Entsprechend ist unklar, wie viele Repeater betroffen wären. Um die Unterbrechungszeit gering zu halten, müssten in jedem Fall parallele Reparaturarbeiten stattfinden.

Fehlerbehebung (Intern) Bei einem solchen Vorfall würden Repeater unterschiedlicher Unterseekabel betroffen sein, so dass ein Umrouten über andere Transatlantikverbindungen kaum Hilfe verspricht.

Spontane kabellose Ad-hoc-Netze oder lokale P2P-Netze könnten temporär Abhilfe für

die eher lokale Kommunikation schaffen.

3.3 Ausfall aller Transitverbindungen durch ein Land

3.3.1 Kurzdarstellung

Transit-Datenverkehr durch ein Land bekommt eine übergeordnete Bedeutung, wenn dieses Land geographisch, (kommunikations-)technisch oder wirtschaftlich ein Bindeglied zwischen Regionen mit relevantem Kommunikationsaufkommen darstellt. Schon aufgrund seiner geographischen Ausdehnung hat Russland das Potential, primäre Transitverbindung nach Asien sowie zu den ehemals sowjetischen Republiken zu sein. Russland ist zudem wirtschaftlich und technologisch weiter entwickelt als viele Staaten im Balkan und jenseits des schwarzen und kaspischen Meeres. Russland verfügt über eine leistungsfähige Transit-Kabelinfrastruktur in diese Regionen und darüber hinaus nach China. Russische Kabelinfrastruktur bleibt dabei jedoch nicht alleingestellt, denn alle Länder verfügen über Kommunikationsinfrastrukturen und -wege, welche russisches Territorium nicht tangieren.

In diesem fiktiven Szenario wird betrachtet, welche Ursachen und Auswirkungen ein vollständiger Transitausfall Russlands im Internet haben könnte. Wir betrachten vornehmlich menschliche, nichttechnische Beweggründe wie staatliche Aktionen oder menschliches Versagen. Allein technische Ursachen, welche einen territorialen Transit weitgehend ausschalten, sind nur schwer denkbar. Insbesondere in Moskau gibt es jedoch sehr große, partiell zentralistische Infrastrukturen, deren Ausfall weitreichenden Einfluss auf das Transitverhalten des Landes haben könnten.

Potentielle Hintergründe Staatliche, politische Beweggründe für eine Blockade des Transits lassen sich in zwei Kategorien einordnen: Die Abschottung des Informationszugangs durch das Land selber, der Weg in ein isoliertes ‘russisches Internet’ etwa, oder die gezielte Beeinträchtigung eines Nachbarlandes durch das Versagen von Dienstleistungen der Informationsinfrastruktur. Beide Szenarien können auch graduell implementiert werden, um politischen Drohungen Nachdruck zu verleiten. So könnten ausländische Provider beispielsweise von ausgewählten Peering-Angeboten ausgeschlossen werden. Ein unmittelbarer wirtschaftlicher Vorteil kann hingegen aus der Blockierung von Datentransfers nicht erkannt werden, weshalb wir ein entsprechendes Vorgehen der russischen Internet-Wirtschaft nicht diskutieren.

Auswirkungen Die Infrastrukturversorgung vieler ehemalig sowjetischer Republiken erfolgte traditionell vornehmlich aus der russischen Republik, weshalb die etablierten Abhängigkeiten auch weiterhin erkennbar sind: Insbesondere die zentralasiatischen Staaten wie Kasachstan und Nachbarn sind im ungestörten Fall primär über Russland zu erreichen. Alternative Kommunikationswege existieren jedoch und können – ggfs. unter Kapazitätseinbußen – aktiviert werden. Spezialisierte Transitprovider in der Region wie RETN nutzen auch Kabelwege außerhalb Russlands. Die Kommunikation in das ferne Asien, also Japan, China, Korea etc. bleibt von einer Transitblockade durch Russland weitgehend unbeeinträchtigt, da die primäre Infrastrukturerschließung über südasiatische Landwege sowie Seekabel erfolgen.

3.3.2 Ausgangssituation

Autonome Systeme können geographisch grenzüberschreitend Netze betreiben. Bei der Betrachtung des Wegfalls aller Transitverbindungen durch ein Land (z.B. Russland) gibt es grundsätzlich zwei Perspektiven. (1) Das AS gehört zu einer Firma, Organisation etc., die ihren Sitz in diesem Land hat. Das AS selber tauscht die Routen aber mindestens in einem weiteren Land aus. (2) Das AS gehört zu einer Firma, Organisation etc., die ihren Sitz in einem andere Land hat (z.B. USA), aber Daten in dem Land austauscht, dass den Transit unterbindet.

Fiktiver Ausfall von Verbindungen durch Russland In diesem fiktiven Ausfall gehen wir davon aus, dass alle Transitverbindungen durch Russland wegfallen. Betroffene IP-Präfixe wurden anhand von BGP Routing-Tabellen der Deutschen Telekom und des DE-CIX Public Peering identifiziert. Ein IP-Präfix gilt genau dann als betroffen, wenn dieses über ein russisches autonomes System erreichbar ist, selbst aber nicht Russland zugeordnet wird. Die AS-zu-Land- und Präfix-zu-Land-Zuordnung erfolgt mit Hilfe von RIR-Delegationsdaten.

3.3.3 Auswirkungen und mögliche Reichweiten

Fällt ein großes Land wie Russland für verbindende Kommunikationsdienste aus, stellt sich zunächst die Frage nach der physischen Infrastrukturerschließung: Wie bedeutsam ist die Kabelinfrastruktur des Landes für seine Nachbarn? Können alle Nachbarn ohne russische Kabel erreicht werden? Welche Rolle nimmt die Landesinfrastruktur im Weitverkehrstransit ein?

Abb. 3.5 zeigt eine Übersicht über die (öffentlich dokumentierten) Transitkabel im osteuropäischen und asiatischen Raum. Die Dokumentation zeigt deutlich, dass alle unmittelbaren russischen Nachbarn – insbesondere die ehemaligen sowjetischen Republiken – sowohl über eine (weitgehend redundante) russische Infrastruktur von Norden her, aber auch von Süden über den Balkan, den nahen Osten und den weiteren asiatischen Raum erschlossen sind. Kirgisistan verfügt zudem im Backbone über ein ausgedehntes Funknetz, welches direkte Links nach China und Usbekistan unterhält. Die Erschließung des gesamten südostasiatischen Raums ist zudem über umfangreiche Seekabel aus dem roten Meer abgesichert sowie über transpazifische Kabel, die mehrheitlich in Japan und Korea anlanden.

Das weltweite IP Routing ist für ungefähr 1,2% der ca. 800k IP-Präfixe von russischen ASes abhängig, wie in Tabelle 3.4 zusammengestellt. Etwa 35.000 aller /24 äquivalenten Präfixen, also maximal 9 Millionen der öffentlichen IP-Adressen, was auf der globalen Internet-Skala sehr wenig ist. Entsprechend kann geschlussfolgert werden, dass ein Ausfall von Russland als Transitland für IP-Verkehr nur geringe Auswirkungen hätte.

Die geopolitischen Abhängigkeiten zeigen sich in Abb. 3.6. Gemessen an der absoluten Anzahl an betroffenen IP-Präfixen (siehe Abb. 3.6a) sind bei einem Wegfall von Russland als Transit insbesondere Kasachstan (auch Usbekistan, Turkmenistan, Tadschikistan und Kirgisistan), die Ukraine und die Tschechische Republik betroffen. Während Tschechien

[9] `https://www.itu.int/itu-d/tnd-map-public/`

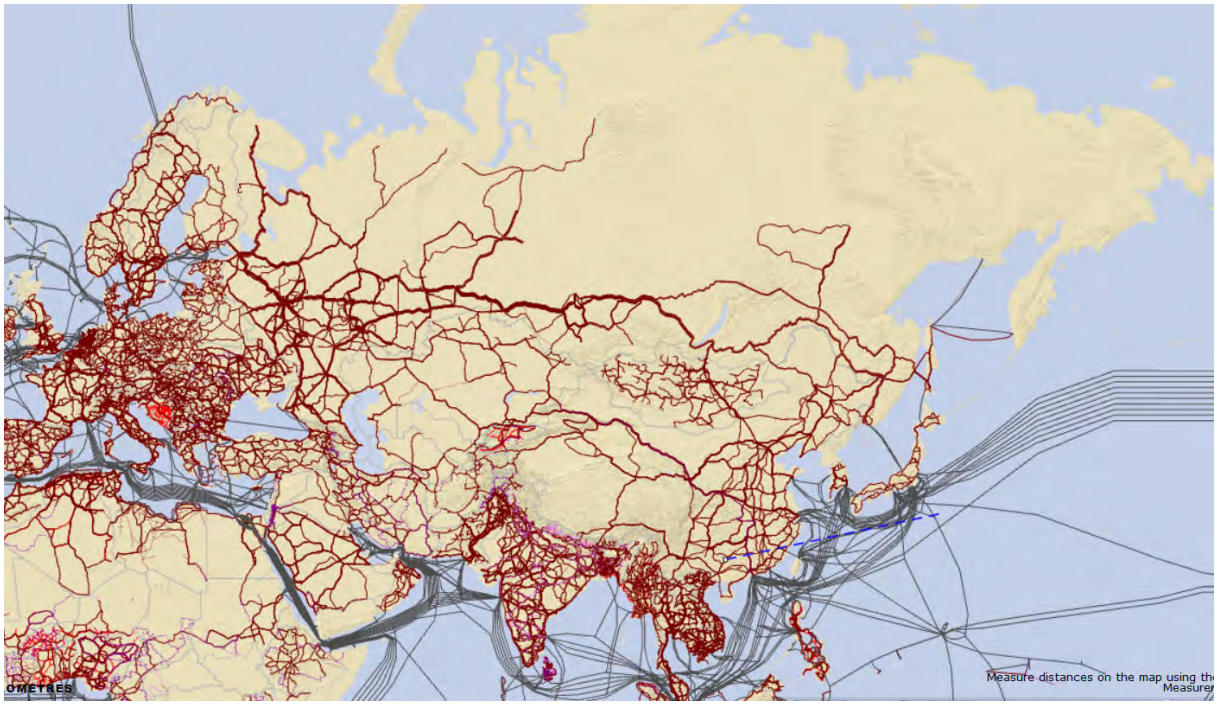
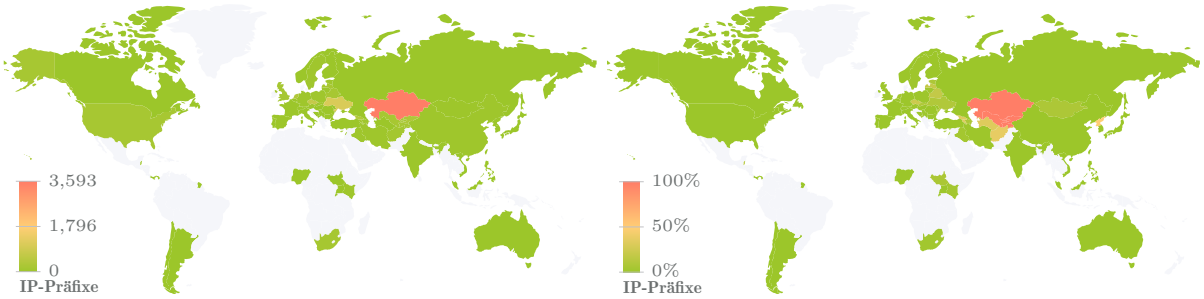


Abbildung 3.5: Verteilung der Transit-Kabelverbindungen im osteuropäischen und asiatischen Raum, Quelle: ITU[9]

	Ziel ASNs	IP–Präfixe	/24–Äquivalente
Betroffen vom Transitausfall	1,562	9.314	35,048
Gesamtheit im Internet	67,561	799,995	11,140,972

Tabelle 3.4: Anteil der von einem Verbindungsausfall durch Russland betroffenen Internet-Resourcen



(a) Absolut (b) Relativ

Abbildung 3.6: Geographische Verortung aller vom Ausfall betroffenen IP-Präfixe bei einem Ausfall von Russland als Transitland. Die relative Darstellung zeigt den Anteil der betroffenen IP-Adressen normiert über die Gesamtanzahl an IP-Adressen pro Land.

in Europa gut vernetzt ist und russischen Transit als eine Wahl unter vielen vornimmt, ändern sich für die zentralasiatischen Staaten die Versorgungswege grundlegend, berücksichtigt man die Anzahl der überhaupt möglichen IP-Präfixe pro Land (siehe Abb. 3.6b). Dies hat ggfs. Veränderungen in der Versorgungskapazität, der Stabilität und der Latenzverteilung zur Folge. Die diesen Ländern zuordenbaren IP-Präfixe sind – basierend auf unseren BGP-Daten – primär über russische autonome Systeme erreichbar und somit den stärksten Änderungen im Fall eines Ausfalls unterworfen. Obwohl Tschechien im Vergleich zu den anderen Staaten relativ betrachtet weniger stark betroffen ist, überrascht die erhöhte Abhängigkeit (753 von 3113 IP-Präfixen) dennoch. Das bedeutet letztlich, dass die Betreiber der 753 IP-Präfixe nicht direkt mit unseren Beobachtungspunkten (DTAG und DE-CIX) Routen austauschen und ihren Tranist über ein russisches AS beziehen. Dies kann historische Gründe haben.

Betrachtet man populäre Webdienste, sind von einem solchen fiktiven Ausfall 246.846 Domains und 508.055 IP-Hosts innerhalb der 1 Million populärsten Webserver betroffen (für eine Verteilung nach Toplistenn siehe Abb. 3.7). Wie populär diese Dieneste in Ländern sind, die primär Upstream-Konnektivität über Russland beziehen, können wir nicht sagen.

Die Aufteilung auf die entsprechenden Top Level Domains ist in Abb. 3.8 dargestellt. Im Detail unterscheiden wir zwischen drei Fälle: (Fall 1) Alle Webserver, die IP-Adressen haben, die durch den Wegfall nicht mehr über den bisherigen Pfad annonciert werden (siehe Abb. 3.9). In diesem Fall sind 48% Russland oder Kasachstan (33% `.ru`, 15% `.kz`) und 12% `.com` zuzuordnen. Sollte es für diese Adressen keine anderen Upstream-Möglichkeiten geben, wären die Adressen nicht mehr erreichbar.

(Fall 2) Alle Webserver, deren Namen durch einen autoritativen Nameserver, der in dem betroffenen Präfixbereich liegt, aufgelöst werden (siehe Abb. 3.10); weitere autoritative Name Server ohne russischen Transit stehen aber als Backup zur Verfügung. Im diesem Fall sind 54% `.com` und nur 11% `.ru` Domainen betroffen.

(Fall 3) Alle Webserver, deren Namen ausschließlich über autoritative Nameserver mit russischen Transit aufgelöst werden (siehe Abb. 3.11). Hier nähern sich die Ergebnisse Fall 1 an (31% `.ru`, 16% `.kz` und 12% `.com`).

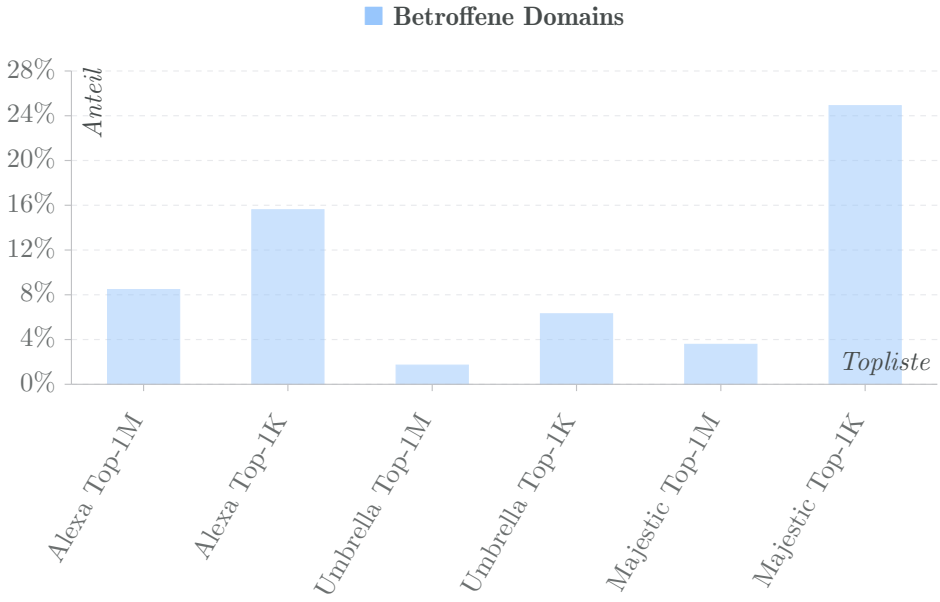
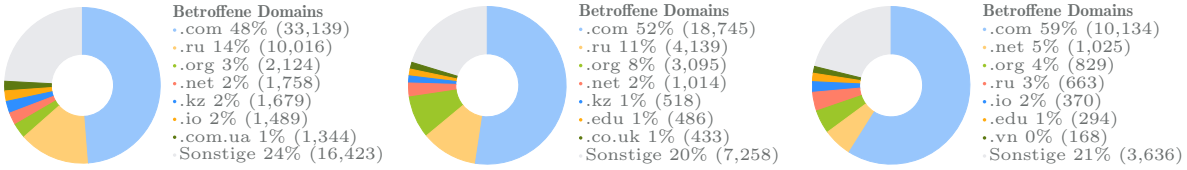
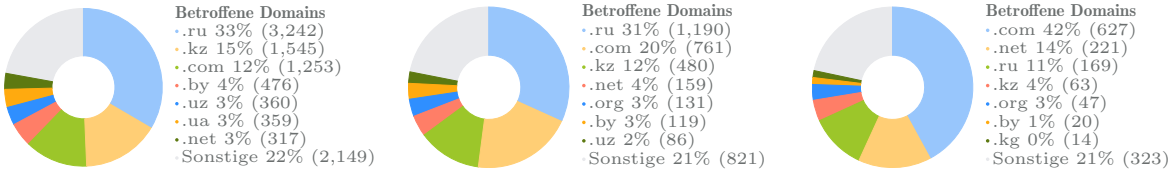


Abbildung 3.7: Relativer Anteil der betroffenen DNS Domains aus öffentlichen Toplisten bei einem Ausfall von Russland als Transit.



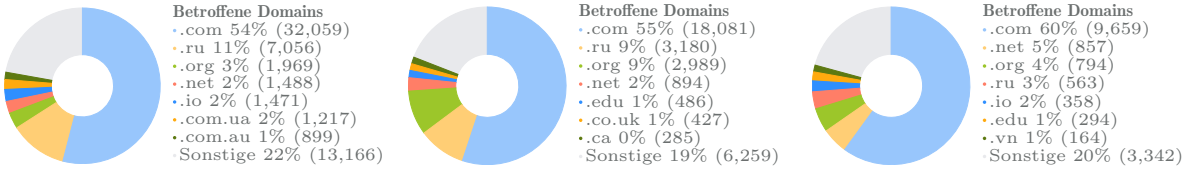
(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.8: Anteil aller direkt und indirekt betroffenen Domains je Top-Level-Domain bei einem Ausfall der Transitverbindungen durch Russland.



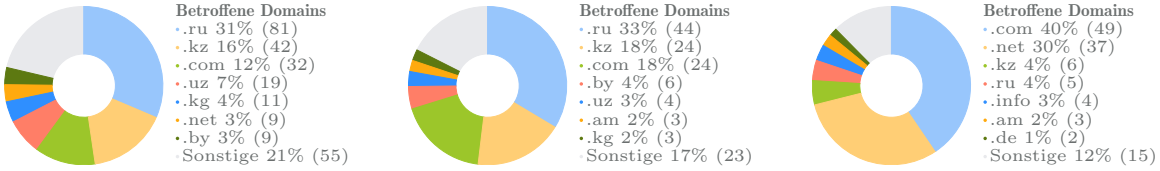
(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.9: Anteil der Domains je Top-Level-Domain, die direkt bei einem Ausfall der Transitverbindungen durch Russland betroffen sind, da sie über ein russisches AS erreichbar sind.



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.10: Anteil der Domains je Top-Level-Domain, die indirekt bei einem Ausfall der Transitverbindungen durch Russland betroffen sind, da ein autoritativer Name Server über Russland erreichbar ist, andere autoritative Name Server aber noch als Backup dienen können.



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.11: Anteil der Domains je Top-Level-Domain, die indirekt bei einem Ausfall der Transitverbindungen durch Russland betroffen sind, da alle autoritativen Name Server über Russland erreichbar sind.

Diese Beobachtung spiegelt direkt das DNS- und Web-Ökosystem wider. Bei einem Wegfall der Transitverbindungen durch Russland sind bei einer Betrachtung der Webserver vor allem russische Webserver betroffen, die entweder unter den Top Level Domains `.ru` oder `.kz` Inhalte anbieten – ein übliches Vorgehen bei russisch- (nicht-englisch-) sprachigen Webinhalten.[10] Ein solcher Ausfall betrifft aber nicht nur Webserver, sondern auch andere Infrastrukturkomponenten, wie DNS-Server. Viele autoritativen DNS-Server gehören zu DNS-Dienstleistern. Sind DNS-Dienstleister global aufgestellt, verteilen sie die von ihnen verwalteten Domainen auf ihre weltweit verteilten autoritativen DNS-Server. `.ru` nimmt hierbei automatisch einen untergeordneten Stellenwert ein. Wenn hingegen DNS-Dienstleister eher lokale Kunden bedienen, dann könnte aus den vorliegenden Ergebnissen geschlossen werden, dass diese Kunden voranging Domainen unter der `.com` TLD registrieren. In Kombination mit den Ergebnissen aus Fall (1) lässt sich zudem schlussfolgern, dass die zugehörigen Webserver bei Transitunterbrechungen über russische autonome Systeme nicht mehr erreichbar wären.

Insgesamt lässt sich festhalten, dass sehr viele ehemalige Länder der Sowjetunion massiv von Transit durch russische autonome Systeme abhängig sind. Innerhalb von Europa bestehen überraschende (moderate) Abhängigkeiten für Tschechien. Internet-Dienste in Deutschland, insbesondere auch `.de` Domainen sind hingegen von russischen autonomen Systemen nicht spürbar abhängig.

[10] Stichprobenartig hat sich auch gezeigt, dass die `.com` Domains russischsprachig geprägt ist.

3.3.4 Mögliche Ausfallszenarien

Typ	Szenario	Verwandt	Betroffen	Behebung	Dauer	Reichweite
BGP-Hijacking	Gezielte Deaggregierung europäischer Präfixe zur Umleitung über Nordamerika	[I73, I74]	Kontrollschicht	Intern	h	+
Hacking-Angriff	Aktivierung von Schläfer-Malware in Infrastruktur-Komponenten	—	Kontrollschicht	Hersteller	w	+
Menschlicher Fehler	Fehlkonfigurierte Routing-Policy von Hurricane für asiatischen Verkehr	[I17]	Kontrollschicht	Intern	h	+
Route Leak	Globale Filterung russischer Routing-Announcements nach Verkehrsumleitung	—	Kontrollschicht	Extern	d	+
Software-Fehler	Fehlerhafte Interpretation von geographischen BGP-Communities bei Level3	[I38]	Kontrollschicht	Intern	h	+
Staatliche Aktion	Schließung des Rechenzentrums M9 für ausländische Kunden	—	Infrastruktur	Intern	w	o
Staatliche Aktion	Politisch motivierte Abkapselung des Landes zur Informationssperre	—	Infrastruktur	Extern	∞	+
Staatliche Aktion	Staatlich angeordnete Routing-Filter für ein abhängiges Nachbarland	[I105]	Kontrollschicht	Extern	∞	+
Technischer Defekt	Ausfall von Rechenzentren in Moskau durch stadtweiten Stromausfall	[I2]	Infrastruktur	Extern	h	+

3.3.5 Detailanalysen

Gezielte Deaggregierung europäischer Präfixe zur Umleitung über Nordamerika
BGP-Hijacking

Beschreibung Nicht-russische ISPs annoncieren *more specific* Präfixe für (ost-)europäische Providernetze, so dass diese bei der Routen-Wahl bevorzugt werden. Der Verkehr wird entsprechend an die Deaggregierenden geschickt und nicht mehr nach Russland geleitet.

Betroffener Bereich (Kontrollschicht) Die Maßnahmen wirken aufgrund fehlerhafter Router-Announcements auf der Kontrollschicht.

Auswirkung und Reichweite (+) Die Fehlannouncements leiten Verkehr ohne Zustimmung der Quellen um.

Dauer (h) Eine Konfigurationsänderung des eigenen Routings kann unmittelbar erfolgen. Das Anlegen von RPKI Route Origin Objekten kann mit geeigneten öffentlichen Werkzeugen zeitnah erfolgen.

Fehlerbehebung (Intern) Betroffene ISPs können einerseits ebenfalls Routen deaggregieren, um den Verkehr teilweise zurückzuholen. Andererseits können sie für ihre IP-Präfixe RPKI ROAs anlegen und falsche Announcements filtern

Aktivierung von Schläfer-Malware in Infrastruktur-Komponenten
Hacking-Angriff

Beschreibung Der dominierende Anteil der Router, welche den Datenaustausch zwischen Russland und der übrigen Welt durchführen, beherbergt eine 'Schläfer-Malware', die internationale Kommunikationsbeziehungen zwischen Russland und dem Rest der Welt unterbindet. Diese Schadsoftware ist entweder durch einen externen Angriff über eine Systemschwachstelle eingeschleust worden, oder – ggfs. politisch motiviert – über den Hersteller im System implementiert.

Betroffener Bereich (Kontrollschicht) Das globale Routing wird gestört.

Auswirkung und Reichweite (+) Viele der zu erwartenden Aktionen bewirken gobal fehlerhafte Routen und können umfangreiche Verkehrsausfälle zur Folge haben.

Dauer (w) Die Entdeckung und Beseitigung von spezieller Malware erfordert Fachkenntnis und Zeit. Der Austausch von Router-Systemen in signifikanem Umfang ist ebenfalls langwierig.

Fehlerbehebung (Hersteller) Eine Aktualisisierung der Routersoftware ist notwendig. Soweit die Systeme dem nicht entgegenstehen, hilft eine zeitnahe Neuinstallation einer sichereren Firmware. Ist die Schadsoftware vom Hersteller vorgesehen, muss ein Herstellerwechsel in Hardware und Software vorgenommen werden.

Fehlkonfigurierte Routing-Policy von Hurricane für asiatischen Verkehr
Menschlicher Fehler

Beschreibung Hurricane Electric verkonfiguriert seine Routing Policies derart, dass alle Routen von und zu russischen ISPs (z.B. RETN) verworfen werden.

Betroffener Bereich (Kontrollschicht) Die Routenfindung wird durch den Fehler merklich eingeschränkt.

Auswirkung und Reichweite (+) Hurricane Electric ist ein wichtiger ISP, da er häufig kostenlos Transit bereitstellt.

Dauer (h) Sobald der Fehler bemerkt ist, kann unmittelbar korrigiert werden, ggfs. auch im Rahmen eines Update-Intervals.

Fehlerbehebung (Intern) Hurricane Electric kann seine Routing-Policy unmittelbar korrigieren.

Globale Filterung russischer Routing-Announcements nach Verkehrsumleitung
Route Leak

Beschreibung Der Route Leak eines russischen Kunden-ASs wird durch Rostelecom landesweit weiterverteilt und von so vielen russischen Netzwerken weitergegeben, dass die globalen Tier-1 Provider entscheiden, alle russischen Announcements pauschal zu filtern.

In der Folge wird in russische Provider eingehender Verkehr mehrheitlich unterdrückt und der Transit durch Russland kommt quasi zum Erliegen.

Betroffener Bereich (Kontrollschicht) Valide Routen russischer Provider werden auf der Kontrollschicht unterdrückt.

Auswirkung und Reichweite (+) Russische Präfixe werden unerreichbar und Transit durch Russland wird umgeleitet.

Dauer (d) Solche Gespräche sind i.d.R. langwierig und nicht innerhalb eines Tages abgeschlossen.

Fehlerbehebung (Extern) Die Auflösung des nach dem Leak entstandenen Peering Disputes erfordert wohl multi-laterale Verhandlungen und einen 'Vertrauensbeweis' gegenüber den Tier-1 Providern.

Fehlerhafte Interpretation von geographischen BGP-Communities bei Level3
Software-Fehler

Beschreibung Level3 (bzw. CenturyLink) verlangt von seinen Peers, dass sie durch ein spezifisches BGP-Community das Ursprungsland, über das die Route importiert wurde, markieren. Dafür nutzt Level3 eine private AS-Nummer (z.B. 65534) und den M49-Ländercode der Vereinten Nationen für Russland (643). Die BGP-Router von Level3 werten BGP-Communities nicht mehr richtig aus und verwerfen alle Routen, die als Ursprung Russland beinhalten, d.h. die BGP Community `65534:643`.

Die fehlerhafte Interpretation kann durch fehlerhafte Firmware erfolgen, welche fälschlich alle Routen mit einer privaten AS Community verwirft.

Deutlich realistischer sind menschliche Fat-Finger-Fehler, d.h. der Administrator sorgt aufgrund eines Vertippens für den Fehler (z.B. statt `65535:643` wird `65534:643` verwendet). Ein solcher *Policy*-Filter lässt sich einfach in einem Router implementieren. Für unser Beispiel könnte der Filter in Cisco wie folgt aussehen: `ip community-list 10 deny 65534:643`.

Betroffener Bereich (Kontrollschicht) Russischen Routen sind in den Routing-Tabellen von Level3 nicht mehr sichtbar. Entsprechend gibt es keinen Weg zu den IP-Präfixen.

Auswirkung und Reichweite (+) Level3 ist ein Tier 1 ISP. Verwirft dieser alle russischen Routen, können Kunden, welche Routen anderer Tier-1 Provider nicht beziehen, russische Präfixe nicht mehr erreichen.

Dauer (h) Die Behebung von Software-Fehlern kann Monate dauern. Das Problem kann zeitnah umgangen werden, indem die vorherige Firmware wieder eingespielt wird. Die neue Firmware wird in der Regel erst nach einem Neustart wirksam. Backbone-Router haben sehr umfangreiche Konfigurationsdateien, so dass ein solcher Neustart mehr als 15 Minuten dauern kann.

Einige moderne Router haben getrennte Management-Karten, die den störungsarmen Übergang von einer Management-Karte auf die andere erlauben, so dass mögliche Ausfallzeiten aufgrund eines Reboots entfallen. Die alte Firmware kann dann auf die Backup-Management-Karte eingespielt werden.

Fehlerbehebung (Intern) Update der Firmware oder Änderungen der Community-Semantik, so dass ein anderer Community-Wert für Russland genutzt wird. Hierfür müssen alle Peers informiert werden und ihre Konfigurationen anpassen. Letzteres erfolgt unter Umständen nicht sofort, sondern nur in festgelegten Wartungsintervallen.

Sollte der Software-Fehler im Rahmen einer aktiven Konfiguration auftreten, könnte diese Konfiguration entfernt werden.

Schließung des Rechenzentrums M9 für ausländische Kunden
Staatliche Aktion

Beschreibung Im Gebäude M9 haben ausländischen Nutzer keinen Zugang mehr. Das große Rechenzentrum M9 ist einer der *Points of Presence* für den Moskau-IX und Treffpunkt für sehr viele angeschlossene Provider. Entsprechend müssen alle ausländischen IXP-Kunden und sonstigen Peers in andere Kolokationsorte umziehen.

Betroffener Bereich (Infrastruktur) Mit dem Zugangsverbot können ausländische Provider im Rechenzentrum M9 keine Infrastruktur mehr betreiben.

Auswirkung und Reichweite (o) Ein Umzug in andere Peering Kolokationen bleibt ohne größere Auswirkungen, solange die benötigten Übergänge zu denselben Partnern mit entsprechenden Kapazitäten etabliert werden können. Dies ist eventuell nicht der Fall, wenn einzelne Partner in alternativen Rechenzentren nicht oder nur mit zu geringen Kapazitäten präsent sind.

Dauer (w) Die Verlagerung der Infrastruktur in andere Rechenzentrum kann nicht in wenigen Tagen erfolgen, sondern dauert wenigstens Wochen. Verlagerungen in Nachbarstaaten sind ggfs. noch aufwändiger.

Fehlerbehebung (Intern) Die betroffenen ausländischen Provider können vornehmlich ihr Peering an andere der 39 *Points of Presence* des MSK-IXs verlegen. Darüber hinaus ist eine teilweise Verlagerung des Peerings mit regionalen Providern u.U. im Ausland möglich.

Politisch motivierte Abkapselung des Landes zur Informationssperre
Staatliche Aktion

Beschreibung Die russische Politik möchte jedweden Datenaustausch mit ausländischen Internet-Akteuren kappen. Hierfür verfügt sie, dass sowhl innerhalb des Landes als auch außerhalb von Russland keine Daten mit ausländischen ISPs ausgetauscht werden. Dies hat zur Folge, dass alle ausländischen ISPs ihre Präsenz an russischen *Points of Presence* (PoP) aufgeben und dass sich alle russischen Provider von ausländischen PoPs und Austauschpunkten zurückziehen müssen. In der Folge gibt es ein russisches und ein sonstiges Internet in voneinander getrennter Weise.

Neben dem Abbau von physischen Verbindungen kann eine Separierung auch auf der logischen Schicht erfolgen. Hierfür wird allen russischen Providern verboten, ihre IP-Präfixe an nicht russische ISPs zu annoncieren. Folglich hat keiner der ausländischen ISPs Information über ein russisches IP-Präfix und kann dieses auch nicht erreichen. Verkehr zu ausländischen Zielen wird zudem mittels Firewall-Regeln unterbunden. Damit sind Hin- und Rückweg der Datenpakte gesperrt.

Um zu verhindern, dass inländische ISPs IP-Präfixe ausländischer ISPs anderweitig erhalten und Daten dorthin schicken, können russische Transit-Provider sogenanntes Präfix-Hijacking durchführen. Hierbei annonciert ein russischer Transit-Provider alle nicht russischen IP-Präfixe. Damit mit hoher Wahrscheinlichkeit dieser Pfad gewählt wird, enthält die falsche Routen-Bekanntgabe das richtige Ursprungs-AS bei, setzt aber sich als Upstream (d.h. Nachbarn des Ursprungs-AS) auf den Pfad.

Betroffener Bereich (Infrastruktur) Gemäß staatlicher Anordnung dürfen ausländische Provider keine Links mehr mit inländischen Providern unterhalten. Die physische Infrastruktur von ausländischen ISPs in Russland wird schrittweise zurückgebaut, da das Mieten von Rechenzentrumsflächen Kosten ohne Mehrwert erzeugt. Der weitere Rückbau der Infrastruktur betrifft Kabel, insbesondere Anlandungsstellen in Russland.

Auswirkung und Reichweite (+) Soweit internationale Links effektiv unterbrochen werden können, wird die Internet-Kommunikation zwischen Russland und dem Rest der Welt unterbunden – es entstehen zwei getrennte 'Internets'.

Dies hat zur Folge, dass niemand innerhalb Russlands irgendeine IP-Adresse, die nicht zu einem russischen ISP gehört, erfolgreich kontaktieren kann. Es können auch keine ausländischen VPN-Verbindungen aufgebaut werden, da der VPN-Punkt außerhalb Russlands liegen müsste. Sollten umgekehrt ausländische IP-Pakete einen russischen ISP erreichen, werden diese direkt gefiltert und gelangen nicht zu einem russischen Server oder Endkunden.

Dauer (∞) Bei effizienten staatlichen Kontrollen ist eine Aufhebung der staatlichen Einschränkungen erst nach einer Änderung des politischen Willensbildungsprozesses möglich.

Russische Internet-Nutzer könnten Schlupflöcher nutzen, indem sie auf funk- bzw. satellitenbasierte Kommunikation ausweichen und sich so direkt mit ausländischen ISPs verbinden. Dies wäre in unserem Szenario illegal. Es ist davon auszugehen, dass solche Umgehungsmaßnahmen innerhalb von Wochen, spätetestens Monaten entdeckt und eingedämmt werden.

Fehlerbehebung (Extern) Abhilfe gegen eine solche staatliche Zwangsmaßnahme kann auf politischer Ebene diplomatisch erreicht werden. Provider könnten nur in (konspirativ)

kooperativer Weise versuchen, das Peering-Verbot heimlich zu umgehen, z.B. auch durch die Nutzung von Satellitenlinks.

Staatlich angeordnete Routing-Filter für ein abhängiges Nachbarland
Staatliche Aktion

Beschreibung Die russische Regierung weist alle russischen Provider an, BGP-Announcements von kasachischen ISPs nicht mehr anzunehmen. Hierdurch werden kasachische Provider in Russland unerreichbar und ein Transit zu kasachischen ASes durch Russland unterbunden.

Betroffener Bereich (Kontrollschicht) Durch das Unterdrücken von BGP-Announcements wird eine regionale Unerreichbarkeit von IP-Präfixen erreicht.

Auswirkung und Reichweite (+) Vorrangig betroffen sind alle kasachsischen IKT-Dienste, die einen nationalen Upstream-Provider nutzen.

Dauer (∞) Die Dauer einer solchen Maßnahme ist vom politischen Willensbildungsprozess abhängig. Sie wird auch dadurch beeinflusst, wie wirksam sie den Zugriff auf Inhalte kasachischer ISPs unterdrückt.

Fehlerbehebung (Extern) Die politischen Entscheidungen können nur auf diplomatischem Weg verändert werden. Wenn die Filternug ausschließlich auf den RIR-Daten basiert, könnten die kasachischen ASes diese ändern oder ggfs. durch Sibling-ASes gegensteuern. Der Ort von Webinhalten könnte zudem über CDNs oder ausländisches Hosting verschleiert werden.

Ausfall von Rechenzentren in Moskau durch stadtweiten Stromausfall
Technischer Defekt

Beschreibung Von einen stadtweiten Stromausfall sind mehrere Rechenzentren in Moskau betroffen, darunter insbesondere das M9-Gebäude, welches einer der wichtigsten *Point of Presence* des Moskau-IX ist.

Betroffener Bereich (Infrastruktur) Ein stadtweiter Stromausfall betrifft alle Komponenten des Kommunikationsökosystems, von aktiven Medienwandlern bis zu anwendungsspezifsichen Gateways und kritischen Diensten. Die Absicherung über Notstromaggregate bleibt nutzlos, weil die gesamte Stadtinfrastruktur ausfällt.

Auswirkung und Reichweite (+) Relevante Infrastrukturpunkte verfügen über Notstromgeneratoren. Fallen diese aus, kann es im schlimmsten Fall zu kaskadierenden Effekten kommen, so dass mangelnde Kommunikationsmöglichkeiten den Neustart der Energieversorgung verhindert. Transitverbindungen durch Moskau können aber dynamisch umgeleitet werden, ggf. unter der Einbeziehung neuer Upstream-Provider.

Dauer (h) Ein stadtweiter Stromausfall in Moskau dürfte schnelles Handeln zur Folge haben. Vergleichbare Fälle, wie z.B. der Stromausfall in Italien 2013, haben zwischen drei und 12 Stunden gedauert.

Fehlerbehebung (Extern) Der stadtweite Stromausfall kann auch bei professionellem Rechenzentrumsbetrieb nicht kompensiert werden, da vorhandene Dieselaggregatoren nur den Betrieb der lokalen Infrastruktur erlauben.

3.4 DDoS-Angriff auf einen zentralen Internetdienst

3.4.1 Kurzdarstellung

Das Domain Name System (DNS) gehört seit den frühen Tagen des Internets zu einem der wichtigsten Dienste, da fast alle relevanten Internet-Anwendungen wie z.B. das Web oder Email auf Namen basieren. Um seine Rolle im Internet-Betrieb zu untersuchen, werden in diesem Kapitel mögliche folgenschwere Ausfallszenarien für einen DNS-Dienstleister betrachtet.

In diesen Szenarien gehen wir davon aus, dass ein Betreiber der DNS-Infrastruktur angegriffen wird. Wir betrachten den DNS-Dienstleister IONOS (*Registrar*), der für Deutschland hohe Relevanz hat, da er für Geschäfts- wie Privatkunden im deutschprachigen Raum eine große Zahl von Domain-Namen anbietet. IONOS betreibt auch die DNS-Infrastruktur für die Mehrzahl der dort registrierten Namen. Ein Angriff auf die DNS-Infrastruktur von IONOS könnte dazu führen, dass sich Domain-Namen nicht mehr korrekt auflösen lassen, wodurch namensbasierte Dienste nicht mehr wie gewünscht funktionieren würde: Sie sind entweder unerreichbar oder werden durch eine vom Angreifer kontrollierte Infrastruktur vorgetäuscht.

Angriffsvektoren Das Domain Name System (DNS) ist eine verteilte Infrastruktur zur globalen Namensauflösung. Die Informationen zu einem Namen werden auf mindestens zwei DNS-Servern hinterlegt, den sogenannten autoritativen DNS-Servern. Des Weiteren werden Abbildungen von Namen zu IP-Adressen auf anderen Server dynamisch zwischengespeichert (*Caches*). Für das Worst-Case-Szenario müsste also nicht nur die IONOS-Infrastruktur, sondern auch alle Caches von dem Angriff betroffen sein. Wie für alle anderen Dienste im Internet können Angriffe durch falsche Routen, Überlast oder Hacking erzielt werden. Bei einer geschickten Verteilung der DNS-Infrastruktur ist ein solches Worst-Case-Szenario aber deutlich schwerer zu erzielen als der Angriff eines einzelnen Servers oder Netzes.

Angriffsszenarien Das DNS ist ein öffentliches System, so dass sich ein Großteil der Informationen über die DNS-Infrastruktur des Dienstleisters auch öffentlich einsehen lassen. Der Angreifer kann die autoritativen DNS-Server für eine Menge von Namen abfragen und diese gezielt schädigen, indem er z.B. über ein Botnet ein DDoS durchführt. Alternativ könnte er durch die Übernahme von autoritativen Servern falsche Namensinformationen ausliefern. Wenn kein weiterer Schutz auf der Anwendungsschicht z.B. durch Zertifikate besteht, ließen sich so vertrauenswürdige Informationen von Endnutzern sammeln oder u.U. Malware ausliefern.

3.4.2 Ausgangssituation

Das DNS verfolgt zwei Grundprinzipien, um Skalierbarkeit und Robustheit zu erreichen: Delegation und Caching. Die Namensvergabe erfolgt dezentral. Die ICANN delegiert einzelne Top-Level Domains, z.B. `.de`, an sogenannte *Registries*, welche hingegen die Vergabe von Second-Level Domains, z.B. `bsi.de` an *Registrars* deligieren. Viele Privat- und Geschäftskunden registrieren ihre Domains nicht selber bei einer Registry, sondern nutzen einen Registrar.

Wenn ein Domain-Name registriert wurde, erfolgt die Verwaltung des Teilnamensbaums (*Zone*) über DNS-Server. Diese halten die Abbildung von Namen zu Resource Records (z.B. `A` für die IPv4-Adresse) vor. Auch hier wird das Delegationsprinzip umgesetzt, um Skalierbarkeit und Robustheit zu erreichen. Der Besitzer einer Domain muss den DNS-Server nicht selber betreiben. Er kann externe Dienstleister nutzen. Insbesondere im Privatkundengeschäft werden häufig die DNS-Server der Registrare genutzt, da die Nutzung im Rahmen der Namensmietung keine Mehrkosten erzeugt.

Die Namensauflösung kann rekursiv oder iterativ erfolgen und wird im gegenwärtigen Standardbetrieb des Internets 'server-assistiert iterativ' durchgeführt. Hierbei fragt ein Stub-Resolver seinen lokalen, rekursiven DNS-Server, welcher die Anfrage iterativ von der Wurzel absteigend bis zum eigentlichen Domain-Namen weiterleitet. Jeder DNS-Resolver bzw. DNS-Server kann die Namensauflösung beschleunigen, indem er Daten aus seinem lokalen DNS-Cache nutzt.

Fiktiver Ausfall der IONOS DNS-Infrastruktur Die IONOS gehört zu einem der größten deutschen DNS-Registrars und ist mit seinen Tocherfirmen weltweit unter den Top Ten Registrars zu verorten[11]. Unter den 1 Million populärsten Domain-Namen verwaltet die IONOS 20,900 Domain Namen in 223 Top-Level Domains, welche für die Erreichbarkeit von 150.282 Hosts verantwortlich sind.

Wenn IONOS ausfällt, betrifft das bis zu 20.900 Domain Namen unter den weltweit 1 Million populärsten Namen. Darunter befinden sich Vereine (z.B. `berliner-mieterverein.de`), kleine und größere Unternehmen (z.B. `anwaltskanzlei-motte.de`, `gmx.net`), Kommunen (z.B. `luebben-rathaus.de`) und wichtige Infrastruktureinrichtungen (z.B. `malteser-krankenhaus-bonn.de`, `stadtwerke-karlsruhe.de`).

Ein Angreifer kann im *schlimmsten* Fall einen erheblichen Teil der digitalen Infrastruktur in Deutschland zum Erliegen bringen. Ähnlich dem Fehlen eines Telefonbuchs können Endkunden dann nicht mehr ihr eigentliches Ziel erreichen. Aber auch Störungen innerhalb von Firmennetzen sind hierdurch leicht möglich, da viele Maschinen-zu-Maschinenen-Kommunikation auf der Nutzung des DNS basiert und hierfür oft der öffentliche Namensraum verwendet wird. Solche *Worst-Case-Situationen* sind aber aufgrund der DNS-Architektur nicht einfach zu erreichen.

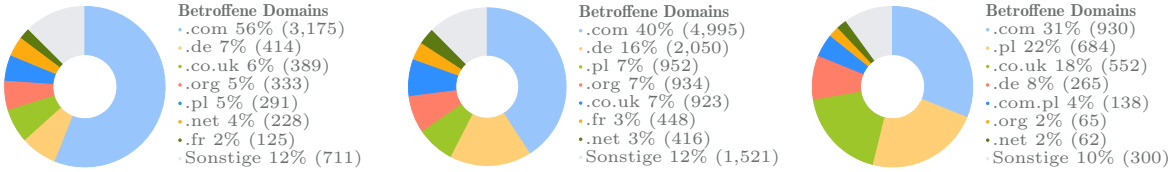
Das nachfolgende Fallbeispiel zeigt die von einem fiktiven Ausfall der DNS-Infrastruktur des deutschen Anbieters IONOS betroffenen Internet-Ressourcen basierend auf den Namen der 1 Million populärsten Webseiten. Wir betrachten hier die drei populären Top-

[11] Basierend auf `https://www.domainstate.com/top-registrars.html` verantwortet alleine die 1&1 4,7M Domain Namen.

Listen Alexa, Majestic und Umbrella. Betroffene IP-Adressen wurden in unseren Messungen in zwei Schritten identifiziert. Zunächst wurden für alle Namen der Top-Listen die DNS-Zonen-Einträge mit dazugehörigen autoritativen IONOS Name Servern identifiziert. Hiernach wurden die betroffenen IP-Adressen über `A` Records, d.h. IPv4-Adressen, dieser Zonen zusammengetragen und auf die entsprechenden *most specific* IP-Präfixe in BGP abgebildet. Eine IP-Adresse gilt genau dann als betroffen, wenn mindestens ein zugehöriger Name Server von IONOS betrieben wird. In unserem Datensatz gibt es nur 28 (von 20.900) Namen, die zusätzlich über autoritative Name Server außerhalb der IONOS-Infrastruktur verfügen. Die Liste der IONOS IP-Präfixe für den Betrieb von Name Servern wurde durch IONOS bereitgestellt.

3.4.3 Auswirkungen und mögliche Reichweiten

Sollte die IONOS-Infrastruktur ausfallen und sämtliche autoritativen Namens-Server nicht mehr erreichbar werden, sind hiervon vor allem Domains unterhalb von `.com` betroffen (siehe Abb. 3.12). Weiterhin treten vermehrt Ausfälle in den Länderdomains von Deutschland `.de`, Polen `.pl`, dem kommerziellen Teil von Großbrittannien `.co.uk` auf. Die verleibenden Domains verteilen sich divers über Namensräume und schwanken naturgemäß auch stark zwischen den Messungen der Top-Listenanbieter.

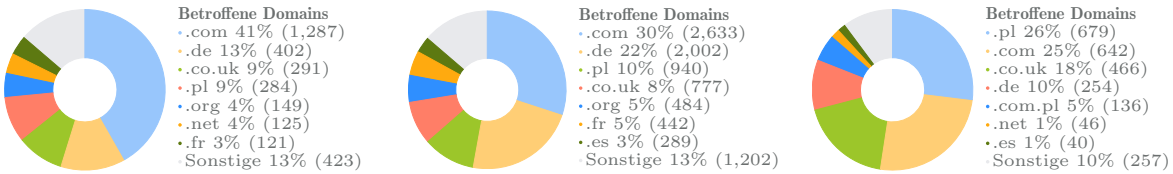


(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.12: Verteilung der betroffenen Top-Level-Domains im Fall eines Ausfalls der IONOS-Infrastruktur

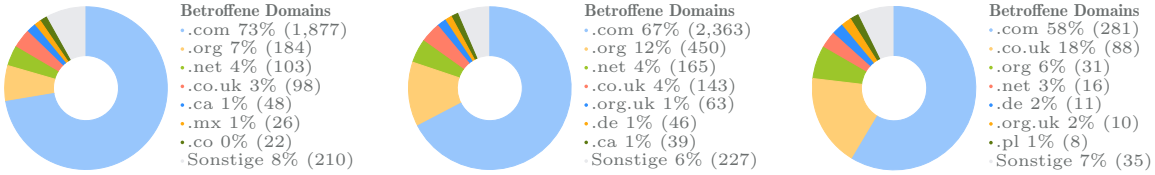
Im folgenden wollen wir die Abhängigkeiten von IONOS nach den Regionen aufschlüsseln. Abb. 3.13 – 3.18 zeigen die entsprechenden regionalen Verteilungen für die betroffenen Namen auf die Top-Level Domains. Hierfür wurden die zu den Domain-Namen gehörenden IP-Adressen auf ihren kontinentalen Standort abgebildet, wobei zwischen Nord- und Südamerika differenziert wurde.

Es ist klar ersichtlich, dass sich die Beeinträchtigungen vornehmlich auf Europa und Nordamerika konzentrieren – alle anderen Regionen sind quantitativ vernachlässigbar. In Europa sind neben kommerziellen Diensten (`.com`) vor allem europäische Ländernamen



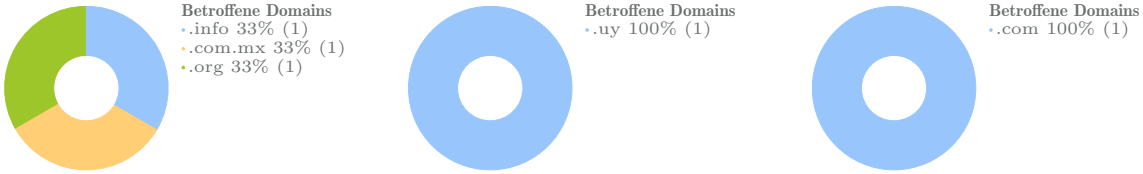
(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.13: Verteilung der betroffenen *europäischen* Top-Level-Domain im Fall eines Ausfalls der IONOS-Infrastruktur



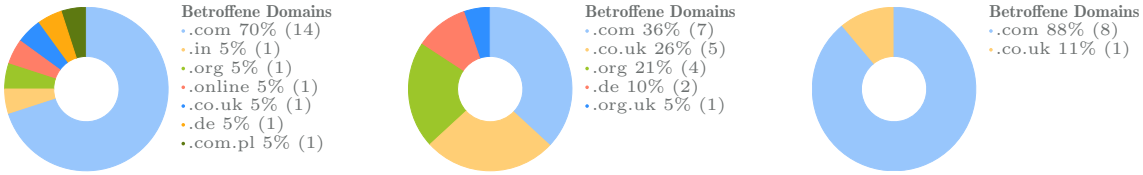
(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.14: Verteilung der betroffenen *nordamerikanischen* Top-Level-Domain im Fall eines Ausfalls der IONOS-Infrastruktur



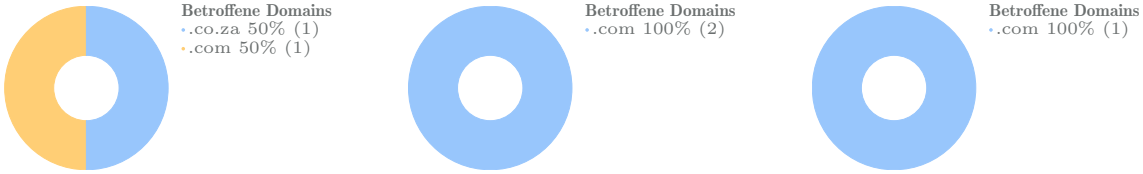
(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.15: Verteilung der betroffenen *südamerikanischen* Top-Level-Domain im Fall eines Ausfalls der IONOS-Infrastruktur



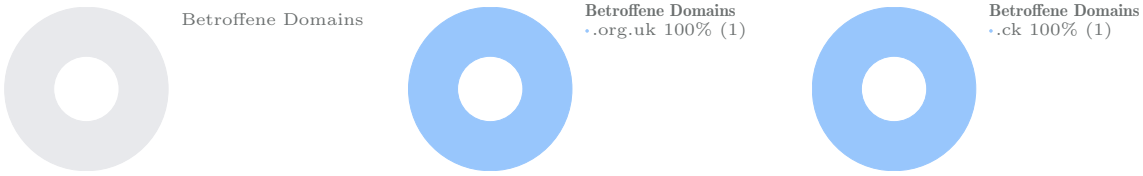
(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.16: Verteilung der betroffenen *asiatischen* Top-Level-Domain im Fall eines Ausfalls der IONOS-Infrastruktur



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.17: Verteilung der betroffenen *afrikanischen* Top-Level-Domain im Fall eines Ausfalls der IONOS-Infrastruktur



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.18: Verteilung der betroffenen *ozeanischen* Top-Level-Domains im Fall eines Ausfalls der IONOS-Infrastruktur

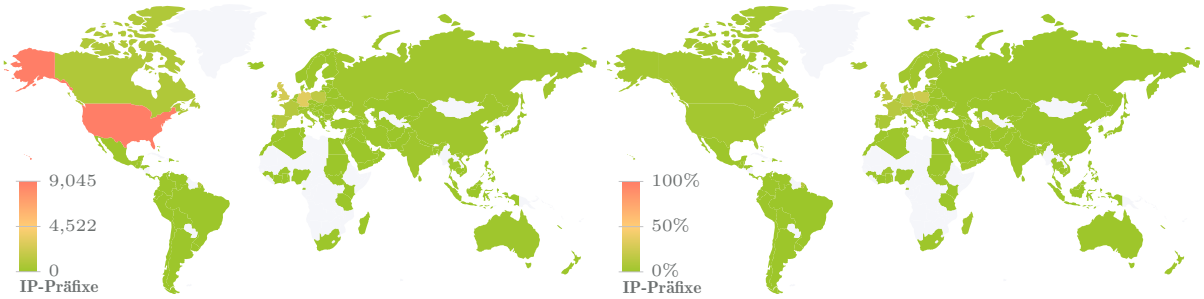
betroffen. Dagegen haben in Nordamerika die Namensräume `.org` und `.net` stärkeres Gewicht. In allen weiteren Regionen ist IONOS nur mit einem sehr geringen Anteil an populären Namen vertreten.

Betrachtet man die Orte der Endgeräte, die mit einem von IONOS verwalteten Domain-Namen verknüpft sind, tritt überraschend zutage, dass ein großer Teil der Webserver in Nordamerika, genauer den USA verortet sind. Abb. 3.19 zeigt die Verteilung der im BGP-Routing zugehörigen IP-Präfixe pro Land sowohl in absoluten Zahlen (siehe Abb. 3.19a) als auch relativ zu der Anzahl aller IP-Adressen pro Land (siehe Abb. 3.19b). Rund 10.075 IP-Präfixe wurden für Nordamerika identifiziert, aber nur 3.181 für Deutschland. Ein relativ ähnliches Bild zeigt sich bei der Verteilung für die /24 Präfixe.

Unter der Annahme, dass ein Großteil der IONOS-Kunden den deutsprachigen Raum bedienen, sind die Ergebnisse aus zwei Gründen bemerkenswert. Einerseits würde man vermuten, dass unter den 1 Millionen populären Webseiten der Einsatz von Content Delivery Netzwerken ebenfalls populär ist. Die enstsprechenden CDN-Server sollten sich aber in Deutschland befinden, um Latenzen zu verringern. Andererseits lässt sich für die mittelgroßen bis kleinen Webseiten annehmen, dass die Webserver aus Kostengründen in lokalen Rechenzentren (wie z.B. Hetzner) betrieben werden.

Die Ergebnisse werden jedoch nachvollziehbarer durch die Beobachtung, dass die Präfixe, welche mit IONOS-Namen verknüpft sind, in Europa auf verschiedene Länder verteilt sind. Diese Länder sind insbesondere Polen, Großbritannien, Frankreich und Spanien. Außerdem bietet IONOS seinen Kunden die Wahl eines Serverstandorts in den USA an, so dass auch europäische Kunden dort Infrastruktur ohne Zusatzaufwände nutzen können. Dies sind Beispiele dafür, dass von IONOS verwaltete Namen auch außerhalb von Deutschland Einsatz finden können. Betrachtet man den Einsatz in Nordamerika relativ zu der Gesamtanzahl der dortigen IP-Präfixe, ist der Einsatz von IONOS zudem vernachlässigbar.

Abschließend ist anzumerken, dass selbst bei einem kompletten Ausfall der IONOS-Infrastruktur nicht zwangsläufig alle Dienste, die mit einem von IONOS verwalteten Namen verknüpft sind, unerreichbar werden. Namen, die sich in anderen DNS-Caches befinden, können weiterhin aufgelöst werden bis der Cache-Eintrag ausläuft. Ebenfalls könnte mindestens einer der autoritativen Name-Server für einen Namen von einem anderen Anbieter betrieben werden, was gegenwärtig aber nur selten der Fall ist.



(a) Absolut (b) Relativ

Abbildung 3.19: Geographische Verortung aller vom Ausfall betroffenen IP-Präfixe, die zu einem Namen gehören, der von einem IONOS Name Server verwaltet werden. Die relative Darstellung zeigt den Anteil der betroffenen IP-Adressen normiert über die Gesamtanzahl an IP-Adressen pro Land.

3.4.4 Mögliche Ausfallszenarien

Typ	Szenario	Verwandt	Betroffen	Behebung	Dauer	Reichweite
Denial-of-Service	Gezielte Ausschaltung der Name Server Infrastruktur	[I87, I82, I84, I85, I86, I88]	Infrastruktur	Intern	h	+
Hacking-Angriff	Server-Übernahme und gefälschte DNS-Antworten mit hoher TTL	[I97]	Anwendung	Intern	d	+
Hacking-Angriff	Hacking-Angriff fälscht DNS-Antworten auf kurze TTLs	[I97]	Infrastruktur	Intern	h	o
Hacking-Angriff	Totalausfall durch Cache-Poisoning für TLD-Server	[I87]	Anwendung	Extern	d	+
Kabelschäden	Verbindungsausfall zwischen Betreiberstandorten	[I39, I40, I41, I42, I43, I45]	Infrastruktur	Intern	h	–
Route Leak	Ausfall durch deaggregierte /24-Präfixe eines BGP-Optimizers	[I58, I63, I67]	Kontrollschicht	Intern	h	o
Software-Fehler	Fälschliche Rückgabe aller Domains an NICs	[I30]	Management	Extern	w	o
Software-Fehler	Veröffentlichung abgelaufener DNSSEC-Schlüssel	[I28]	Management	Extern	h	+
Staatliche Aktion	Staatlich angeordnete DNS-Sperren direkt beim Registrar	[I104]	Infrastruktur	Extern	∞	+
Staatliche Aktion	Stilllegung aufgrund erzwungener Herausgabe von Nutzerdaten	[I104]	Infrastruktur	Intern	∞	o
Technischer Defekt	Hardware-Ausfall eines Load Balancer Arrays	—	Management	Service	h	–

3.4.5 Detailanalysen

Gezielte Ausschaltung der Name Server Infrastruktur
Denial-of-Service

Beschreibung Der Angreifer möchte die DNS-Server des DNS-Dienstleisters gezielt ausschalten, d.h. deren Erreichbarkeit verhindern. Er kann damit prinzipiell zwei Ziele verfolgen: (1) den Zonentransfer, also den Transfer der DNS Records zwischen dem primärem und sekundären Servern verhindern, (2) die Auflösung des Namens von außen verhindern. Ziel (1) ist relativ schwierig zu erreichen, da viele große DNS-Dienstleister lokale oder separat geschützte Netze für die interne Kommunikation verwenden, so dass die Synchronisierung über das öffentliche Internet nicht gestört werden kann.

Ziel (2) hingegen ist wahrscheinlicher zu erreichen, da die Server von außen ansprechbar sein müssen, so dass dieser Weg als Einfallstor ausgegenutzt werden kann. Um die primären und sekundären autoritativen Name Server eines Namens zu ermitteln, fragt der Angreifer die öffentlich verfügbaren `SOA` bzw. `NS` Records ab. Durch das Abfragen mehrerer Namen lässt sich die gesamte Name Server Infrastruktur ermitteln. Der Angreifer kann nun durch DDoS, BGP Hijacking oder Hacking Attacken auf die enstprechenden Server bzw. Adressbereiche durchführen. Der Angriff ließe sich gezielt für einen einzelnen Namen durchführen. Das wäre aber nur dann gerechtfertigt, wenn die DNS Infrastruktur deutlich schwächer geschützt ist als das Opfer hinter dem Namen. Insofern gehen wir davon aus, dass der Angreifer vor allem das Ziel verfolgt, mit einem Angriff der DNS Infrastruktur mehrere Namen parallel zu attackieren, um entweder explizit dem Dienstleister zu schaden oder die dahinterliegenden Dienste nicht erreichbar zu machen.

Am Beispiel IONOS gibt es in den von uns untersuchten Namen nur 28 Fälle in IPv4 (bzw. 4 Fälle in IPv6), in denen zusätzlich autoritative Name Server außerhalb des IONOS-Netzes genutzt werden. Nur wenige Namensbesitzer machen sich also bei IONOS die Mühe, ihre Daten über mehrere Dienstleister zu verteilen, um eine höhere Robustheit zu erzielen. Umgekehrt sind die Daten für den Großteil der von IONOS verwalteten Namen über drei bis vier autoritative IONOS DNS-Server verfügbar, welche jeweils unterschiedlichen `/24`-Netzen zugeordnet werden können. Es gibt nur 20 Fälle, die über einen einzigen autoritativen IONOS DNS-Server verfügen – die weiteren autoritativen Server befinden sich dann außerhalb des IONOS-Netzes.

Der IP-Adressbereich von IONOS ist durch RPKI Route Origination Authorization Objekte geschützt. Der Adressbereich, der die autoritativen DNS-Server abdeckt, wird aber als aggregiertes `/22` Präfix annonciert. Ein Angreifer könnte *More Specifics* (`/24`) annoncieren. Da *More Specifics* vor *Less Specifics* bevorzugt werden, wäre ein Angreifer immer bei Providern erfolgreich, die kein Route Filtering betreiben.

Betroffener Bereich (Infrastruktur) Betroffen sind alle Endkunden des DNS-Dienstleisters. Im schlimmsten Fall könnten keine Aktualsieriungen der DNS-Daten vorgenommen werden. Ebenfalls können Namen, die sich nicht mehr im Cache anderer DNS-Server befinden, nicht mehr erfolgreich aufgelöst werden. Zu den von IONOS verwalteten Namen zählen mindestens vier Stadtwerke (Borke, Karlsruhe, Neustrelitz, Ülzen) und zwei Krankenhäuser, andere städtische Einrichtungen, Hotels etc.

Auswirkung und Reichweite (+) Die mit dem Namen verknüpften Dienste (z.B. Webseiten, Email, Voice-Dienste) sind nicht mehr erreichbar, wenn sie nicht (mehr) aus Caches bedient werden können. Die Bevölkerung kann dann z.B. die Webseite eines Krankenhauses nicht mehr direkt aufrufen und sich informieren. Ebenfalls könnten Sprach- und Videodienste gestört sein, da die Namensauflösung für die Konferenzendpunkte nicht mehr funktioniert. Viele Angebote von kritischen Diensten sind aber häufig über Drittanbieter verfügbar. So kann der Weg zu einem Krankenhaus auch ohne die Webseite des Krankenhauses selber gefunden werden (z.B. OpenStreetMap oder Google Maps), Hotels werden oft über Portale wie `hotel.de` gebucht usw. Alle asynchronen Kommunikationsdienste wie z.B. Email verfügen über Nachrichtenpuffer, so dass eine Nachricht in der Regel nicht verloren geht, sondern nur verspätet zugestellt wird. Direkt betroffen sind in jedem Fall synchrone Kommunikationsdienste wie IP-basierte Telefonie.

Dauer (h) Abhängig vom tatsächlich durchgeführten Angriff können die Auswirkungen mittelfristig sein. Da wir von einem Komplettausfall einer *verteilten* Infrastruktur ausgehen, ist die Wiederherstellung des Gesamtsystems kurzfristig eher nicht denkbar.

Fehlerbehebung (Intern) Die Schutzmaßnahmen müssen durch den Betreiber der Infrastruktur erfolgen. Dritte (z.B. Upstream-Provider) können nur lokal bzw. temporär helfen (z.B. durch Blackholing). Scrubbing-Center können vom Betreiber aktiviert werden, um DDoS-Angriffe abzumildern. Die bösartige Übernahme von IP-Präfixen kann durch das parallele Annoncieren von *More Specifics* abgemildert werden. RPKI-Objekte sollten in jedem Fall konfiguriert werden.

Server-Übernahme und gefälschte DNS-Antworten mit hoher TTL
Hacking-Angriff

Beschreibung Ein Angreifer übernimmt einen primären autoritativen DNS-Server des DNS-Dienstleisters und manipuliert DNS Records. Für die Übernahme nutzt der Angreifer Schwachstellen des Betriebssystems aus, so dass er entfernt den Datenbestand ändern kann. Es ist wichtig zu betonen, dass ein beliebiges *Remote Login* alleine nicht ausreicht. Der gekaperte Nutzer muss auch über Rechte verfügen, die die Manipulation zulassen.

Bei der Adressmanipulation werden Namen mit IP-Adressen verknüpft (`A` bzw. `AAAA Records`), die der Angreifer gewählt hat, so dass die ursprünglichen, namensbasierten Dienste nicht mehr genutzt werden können. Hierbei werden die TTLs sehr hoch eingestellt, wodurch die neu erzeugten, manipulierten Einträge in den weltweiten DNS-Caches sehr lange verbleiben. Ein solcher Angriff hat fatale Folgen für alle, die die betroffenen Namen aufrufen, da der Angreifer das Ziel (d.h. die IP-Adresse) vorgeben kann.

Dies kann im einfachsten Fall als Angriff auf die Verfügbarkeit (DoS) genutzt werden, indem etwa die Namen von `web.de` auf ungültige Adressen abgebildet wird. Angriffe auf die Verfügbarkeit werden bei populären Diensten allerdings sehr schnell bemerkt.

Deutlich interessanter sind subtile Angriffe, die nicht schnell bemerkbar sind. Ein Angriff könnte z.B. auch wie folgt ablaufen: Die Hacker nutzen ihren Zugang zu dem primären IONOS DNS-Server und manipulieren die Adress Records für einen Bannerwerber derart, dass Werbe-Feeds in populären Webseiten wie `Spiegel.de` nun von einem durch die Angreifer kontrollierten Server ausgeliefert werden. Die Bannerwerbung der Angreifer enthält Malware, welche über aktuelle Browser-Schwachstellen auf die Rechner der Besucher von

`Spiegel.de` u.a. gelangt. Durch die Popularität der bannerwerbenden Webseiten verbreitet sich einerseits die Malware rasch, andererseits verbreiten sich die manipulierten DNS Records in sehr viele DNS Cache-Server. Schließlich fällt dieser Angriff – soweit handwerklich gut umgesetzt – weder bei den Werbung einbettenden Websites noch bei den Konsumenten unmittelbar auf. Ein solcher Angriff hat eine sehr hohe Erfolgswahrscheinlichkeit, wenn die Angreifer uneingeschränkten (Admin-)Zugriff zu dem IONOS Primär-Server hätten.

Die Ausnutzung von Banner-Werbung für die Verbreitung von Malware, sogenanntes *Malvertising*, ist ein bekanntes Problem. Bannerplattformen wirken dem entgegen, indem sie die Bannerwerbung überprüfen und bestimmte Technologien (z.B. JavaScript) verbieten. In unserem Szneario ist der Angreifer auf die Banner-Plattform nicht angewiesen, da der Angreifer das Opfer über die Auslieferung einer falschen Adressen auf die eigene Plattform umlenkt. Hierdurch kann er dann ein Banner ausliefern, das maßgeschneidert die Browser-Schwachstellen ausnutzt. Auf diese Weise kann eine umfangreiche Angriffskampagne flächig umgesetzt werden, bevor die Systembetreiber den Schaden bemerken können.

Ein ebenfalls subtiler, wenn auch weniger erfolgsversprechender Angriff, ist der folgende: Der Angreifer möchte an die Kreditkarteninformationen von Endkunden gelangen. Dafür lenkt er den Namen eines Bezahldienstes (z.B. Paypal) auf eine betrügerische Ersatzinfrastruktur um. Dies ist prinizpiell möglich, doch sind diese Dienste in der Regel durch Zertifikate und Fremdauthentifizierung (z.B. mittels OAUTH) zusätzlich gesichert und können somit nicht alleine durch DNS-Modifikationen angegriffen werden.

Betroffener Bereich (Anwendung) Betroffen sind alle Dienste, deren DNS Namenseinträge manipuliert wurden. Unter der Prämisse des Admin-Zugriffs durch den Angreifer, ist der betroffene Bereich nur durch den Aufwand begrenzt, welchen der Angreifer investiert bzw. durch dessen strategische Überlegungen, dass kleinere Eingriffe schwerer zu entdecken sind.

Der Vorfall kann sowohl die Infrastruktur des DNS-Dienstleisters selbst betreffen, als auch beliebige Internet-Dienste seiner Kunden. Nach erfolgreicher Manipulation des DNS' haben die Kunden keine Möglichkeit mehr, sich gegen diesen Angriff zu schützen.

Auswirkung und Reichweite (+) Alle Dienstanfragen an manipulierte DNS Namenseinträge werden umgelenkt bzw. blockiert. Dabei wird der Angriff mit wachsender Popularität der betroffenen Dienste erfolgreicher, denn seine Wirksamkeit beruht darauf, dass in der Zeit zwischen der Manipulation und der Entdeckung bzw. Korrektur die DNS Records weit über bestehende Caches verbreitet werden.

Sehr hoch konfigurierte TTLs führen dazu, dass die manipulierten Resourcen mehrere Tage im DNS sichtbar bleiben, ohne dass der Dienstleister dies direkt beeinflussen oder korrigieren kann. Er müsste die Betreiber der Cache-Server kontaktieren und um das Löschen der Cache-Einträge bitten. Das ist nicht realistisch, da es eine überwältigende Anzahl von Servern gibt, die durch den Angriff fehlerhafte Cache-Einträge vorweisen.

Dauer (d) Die Dauer der Wirksamkeit des Angriffes hängt von der Höhe der TTLs, der Zeit bis zur Erkennung und zum Austausch des kompromitierten Servers ab. Letzteres kann – mit entsprechenden System-Backups – zügig erfolgen. Die maximale TTL im

DNS beträgt zwar 136 Jahre, typische DNS Software und Betreiber akzeptieren jedoch nur Werte von wenigen Tagen. Zum Beispiel verfügt Bind, eine populäre DNS-Server-Software, über einen `max-cache-ttl` Wert, der per Default auf 7 Tage gesetzt ist. Insofern verschwinden die manipulierten Namensauflösungen wenige Tage nach Wiederherstellung der Integrität aus den Internet-weiten Cache-Einträgen.

Fehlerbehebung (Intern) Die autoritativen DNS-Server sollten durch übliche Verfahren der Systemhärtung geschützt werden. Siehe hierzu auch *Umsetzungshinweise zum Baustein APP.3.6 DNS-Server* im IT-Grundschutz [48].

Hacking-Angriff fälscht DNS-Antworten auf kurze TTLs
Hacking-Angriff

Beschreibung Ein Angreifer übernimmt den primären autoritativen DNS-Server des DNS-Dienstleisters oder – als Man-in-the-Middle – einen Vermittlungsknoten und modifiziert die TTLs der Domain-Namen auf einen sehr niedrigen Wert. Hierdurch werden die Cache-Zeiten minimiert bzw. das Caching außer Kraft gesetzt ($TTL = 0$). Die Zugriffszeiten auf Dienste unter den betroffenen Namen erhöhen sich und die Infrastrukturlast auf die DNS-Infrastruktur, insbesondere die autoritativen Nameserver steigt.

Betroffener Bereich (Infrastruktur) Der Vorfall betrifft primär die Infrastruktur des DNS-Dienstleisters.

Auswirkung und Reichweite (o) Sollte der Angreifer sehr kurze TTLs konfigurieren, wird das globale Caching der vom DNS-Dienstleister verwalteten Namen unwirksam. Folglich werden deutlich mehr DNS-Auflösungen an die autoritativen DNS-Servers des Dienstleisters geschickt. Dies kann zu einer Überlast der Server führen. Netzprobleme sind eher unwahrscheinlich, es sei denn, der Angriff wird mit einem reflektiven Amplifkationsangriff gebündelt.

Dauer (h) Der Angriff kann unmittelbar beendet werden, sobald er bemerkt wird.

Fehlerbehebung (Intern) Die autoritativen DNS-Server sollten durch übliche Verfahren der Systemhärtung geschützt werden. Siehe hierzug auch *Umsetzungshinweise zum Baustein APP.3.6 DNS-Server* im IT-Grundschutz [48].

Totalausfall durch Cache-Poisoning für TLD-Server
Hacking-Angriff

Beschreibung Der Angreifer schafft es, falsche Referenzen auf die autoritativen Server einer Top-Level Domain zu implantieren. Alle Anfragen werden dadurch an einen vom Angreifer kontrollierten Server gestellt. Der Angreifer liefert dann für Second-Level Domain-Namen ebenfalls manipulierte Antworten aus, woduch die Einträge in den Internet-weiten DNS Caches verfälscht werden (Cache Poisoning). Dieses Verfahren setzt sich rekursiv für beliebige Namen unterhalb der TLD fort.

Betroffener Bereich (Anwendung) Sowohl die Top-Level Domain als auch alle Namen innerhalb dieses Teilbaums sind betroffen.

Auswirkung und Reichweite (+) Die Auswirkungen sind weitreichend, da der TLD-Server der Einstiegspunkt für alle Anfragen des Teilbaums ist. Da der Angreifer das Cache

Poisoning eingfügt hat, kann zudem davon ausgegangen werden, dass hohe TTLs konfiguriert sind, so dass der Cache-Eintrag lange bestehen bleibt.

Dauer (d) Gefälschte DNS-Einträge sind ohne DNSSEC nicht automatisch erkennbar. Der Nutzer müsste die ursprünglich richtigen Einträge kennen und die erhaltenen DNS-Antworten damit vergleichen.

Fehlerbehebung (Extern) Die TLD kann über DNSSEC gesichert werden. So kann der `NS` Record für die TLD verfiziert und Cache Poisoning erkannt werden. Die Resolver können dann direkt einen der Root Server befragen. Wird der Fehler anderweitig erkannt, können die fehlerhaften Caches bereinigt werden.

Verbindungsausfall zwischen Betreiberstandorten
Kabelschäden

Beschreibung Der DNS-Dienstleister betreibt seine Infrastruktur in unterschiedlichen Rechenzentren, so dass die autoritativen DNS-Server geographisch verteilt sind. Die Rechenzentren sind durch das interne Backbone auf Basis gemieteter Glasfasern bzw. Wellenlängen miteinander verbunden. Durch Kabelbeschädigungen wird die Konnektivität zwischen den Standorten unterbrochen.

Betroffener Bereich (Infrastruktur) Die gestörte Kabelinfrastruktur bewirkt den Kommunikationsausfall über die zugehörigen Wege.

Auswirkung und Reichweite (–) Die Auswirkungen und die Reichweite können als gering eingestuft werden. In der Regel werden Rechenzentren über mehrere Kabel angebunden. Selbst wenn es keine Backup-Verbindungen gibt und der primäre autoritative DNS-Server in dem betroffenen Rechenzentrum isoliert ist, bleibt der Schaden überschaubar. Die sekundären autoritativen DNS-Server, welche sich in einem anderen Rechenzentrum befinden, werden eingehende Anfragen beantworten. Einzig zwischenzeitlich veränderte DNS-Einträge würden nicht aktualisiert.

Dauer (h) Die Reparatur einer lokalen Kabelverbindung dauert in der Regel einige Stunden. Bei angemessener Netzplanung sorgt der Ausfall eines Kabels aber nicht zur Unerreichbarkeit der darüber angebundenen Infrastruktur.

Fehlerbehebung (Intern) Durch den Einsatz von Anycast kann automatisch auf einen anderen autoritativen Server ausgewichen werden.

Ausfall durch deaggregierte /24-Präfixe eines BGP-Optimizers
Route Leak

Beschreibung Ein BGP-Optimizer spaltet ein /24 Präfix in viele kleine IP-Präfixe auf (/25 . . . /32) und annonciert diese *More Specifics* statt des ursprünglichen Präfixes an die Upstream ISPs und P2P-Nachbarn. Typische BGP Routing Policies sehen vor, dass Präfixe > /24 global nicht akzeptiert werden.

Betroffener Bereich (Kontrollschicht) Die deaggregierten IP-Blöcke werden im Routing gestört. Hierdurch sind alle Dienste des DNS-Dienstleisters betroffen, die über eine IP-Adresse aus dem betroffenen Präfixbereich anzusprechen sind.

Auswirkung und Reichweite (o) Es gibt zwei Optionen: (1) Parallel zu den Präfixen

>/24 wird noch mindestens ein *Less Specific* IP-Präfix annonciert. Damit sind die IP-Adressen über einen alternativen (Um-)Weg erreichbar. Dieser kann weniger effizient sein; im schlimmsten Fall kommt es zu Verzögerungen oder Netzüberlastungen.

(2) Es gibt kein *Less Specific* IP-Präfix. In diesem Fall sind die im Adressbereich befindlichen Adressen nicht mehr erreichbar. Sollten autoritative DNS-Server IP-Adressen aus dem Bereich aufweisen, würden die Auflösung der von den Server verwalteten Namen nicht mehr erfolgreich sein, sobald die Cache-Einträge veraltet sind. Sollten Web-Server, die als Schnittstelle zur Konfiguration für die Endkunden dienen, betroffen sein, können DNS-Einträge nicht mehr aktualisiert werden.

Dauer (h) Die Störungsdauer hängt primär von der Zeit der Erkennung und dem BGP-Konvergenzprozess an. Wenn der DNS-Dienstleister BGP-Beobachtungswerkzeuge, z.B. BGPMon nutzt oder selber BGP-Dumps in Echtzeit auswertet, lassen sich falsche BGP-Announcements in wenigen Minuten erkennen. Die Bekanntgabe des eigentlich richtigen IP-Präfixes lässt sich sofort umsetzen. Bis alle BGP-Router die neue Route gelernt haben, vergehen typischerweise nicht mehr als 5 Minuten.

Fehlerbehebung (Intern) Der Netzbetreiber muss ein Präfix $\leq$ /24 annoncieren. Er sollte RPKI ROAs erzeugen, so dass Nachbarn prüfen können, ob die Präfix-Announcements richtig sind.

Fälschliche Rückgabe aller Domains an NICs
Software-Fehler

Beschreibung Der DNS-Dienstleister gibt alle Domains an die DNS Registry (auch Network Information Center genannt) zurück. Dies kann zum Beispiel passieren, wenn durch ein Software-Bug die Domains als ausgelaufen eingestuft werden.

Betroffener Bereich (Management) Alle mit dem Namen verknüpften Dienste sind betroffen. Sollte in der Übergangsphase der Name von einem anderen Registrar vergeben werden, sind die „neuen“ Namensbesitzer ebenfalls betroffen, da diese u.U. den Namen zurückgeben müssen.

Auswirkung und Reichweite (o) Normalerweise werden Domain-Besitzer über das Auslaufen ihrer Domains per Email informiert. Selbst wenn Domains ausgelaufen sind, werden diese normalerweise nicht sofort vom Registrar an die Registry zurückgegeben, sondern für eine gewisse Zeit (bei einigen Registrars bis zu 30 Tagen) vorgehalten. Insofern kann davon ausgegangen werden, dass der Fehler schnell erkannt wird und schadlos behebbar bleibt.

Dauer (w) Die Domains müssten von der Registry erneut dem Registrar zugeorndet werden. DNSSEC-Absicherungen müssten neu erzeugt werden. Technisch sind beide Schritte innerhalb von Minuten bis Stunden möglich. Zusätzlich greifen aber auch nicht-technische Aspekte, die deutlich mehr Zeit in Anspruch nehmen werden. Die Komplexität der Fehlerbehebung steigt, wenn einzelne Domains zwischenzeitlich von anderen Registries übernommen und ggf. sogar von anderen Domain-Besitzern registriert wurden.

Fehlerbehebung (Extern) Der ursprüngliche Domain-Besitzer könnte die Domain über einen anderen Registrar erneut registrieren.

Veröffentlichung abgelaufener DNSSEC-Schlüssel
Software-Fehler

Beschreibung Der DNS-Dienstleister nutzt einen ungültigen Key Signing Key, um den Zone Signing Key einer von ihm verwalteten Zone zu signieren. Ungültig bedeutet in diesem Fall, dass der öffentliche Schlüssel, der von der überliegenden DNS-Hierarchie bestätigt wurde, nicht mit dem privaten Schlüssel übereinstimmt, mit dem die Signatur für den Zone Signing Key erzeugt wurde.

Betroffener Bereich (Management) Alle Namen innerhalb der Zone sind betroffen, da DNSSEC eine rekursive Validierung der Vertrauenskette vornimmt.

Auswirkung und Reichweite (+) Wenn der Zone Signing Key nicht erfolgreich validiert werden kann, sind alle mit diesem Schlüssel unterschriebenen Signaturen ungültig, wodurch die signierten DNS-Einträge ebenfalls ungültig werden. Dies betrifft dann Resource Records aller Namen und damit auch alle mit den Namen verknüpften Dienste.

In der Folge werden durch die Fehlkonfiguration eines einzelnen Schlüssels alle Namen in dem darunterliegenden DNS-Teilbaum — also z.B. alle Namen, die auf `bund.de` enden — im DNSsec ungültig. Somit kann die Auflösung aller Namen in dem betroffenen DNS-Teilbaum fehlschlagen, soweit die Anfragenden eine DNSsec-Validierung vornehmen. Da DNSsec nur sehr eingeschränkt im Einsatz ist, werden weniger als 10% der Anfragen von diesem Fehler betroffen sein. Allerdings kann angenommen werden, dass die Betroffenen sicherheitsbewusster und ggfs. auch funktionskritischer sind als diejenigen, welche der Einführung von Sicherheitsprotokollen wie DNSsec keinerlei Beachtung schenken.

In unserem Beispiel kann das bedeuten, dass eine fehlkonfigurierte Domain `bund.de` für alle Landesbehörden unerreichbar wird, während Kunden von O2 keinerlei Beeinträchtigung erfahren.

Dauer (h) Die Bereitstellung neuer Schlüssel und Signaturen kann innerhalb weniger Minuten erfolgen. Bereits verteilte Informationen müssen aber aus den entsprechenden Cache-Servern entfernt werden. Dies ist abhängig von der vorher konfigurierten TTL.

Fehlerbehebung (Extern) Für die betroffenen Domain-Namen kann kurzfristig die DNSSEC-Validierung deaktiviert werden. Dies ermöglicht aber die Durchführung anderer Angriffe. Letztlich muss der Key Signing Key und die damit verbundenen Signaturen erneuert werden, was die Kooperation mit dem delegierenden DNS-Provider erfordert.

Staatlich angeordnete DNS-Sperren direkt beim Registrar
Staatliche Aktion

Beschreibung Der Staat erwirkt, dass die autoritativen DNS-Server des DNS-Dienstleisters für bestimmte Domain-Namen nicht mehr antworten.

Betroffener Bereich (Infrastruktur) Betroffen sind alle DNS-Resolver, die die gesperrten Domain-Namen auflösen wollen.

Auswirkung und Reichweite (+) Abhängig davon, welcher Teil des DNS gesperrt wird, können die Auswirkungen sehr umfangreich sein. Sollte bspw. eine Second Level Domain gesperrt werden, sind alle darunter befindliche Namen ebenfalls nicht erreichbar. Dies ist auch dann der Fall, wenn die Sub-Domains von einem anderen autoritativen

Namensserver verwaltet werden, da die Referenz über den `NS` Record versagt werden kann.

Dauer (∞) Die Dauer hängt von der Dauer der staatlichen Anordnung bzw. davon ab, wie schnell sich andere Wege der Informationsverbreitung durchsetzen.

Fehlerbehebung (Extern) Die zu den Namen gehörigen Resource-Record-Informationen (z.B. Host-IP-Adressen, SMTP-Relays) können außerhalb des DNS über erreichbare Webseiten o.ä. ausgetauscht werden.

Stilllegung aufgrund erzwungener Herausgabe von Nutzerdaten
Staatliche Aktion

Beschreibung Geschäftsvereinbarungen zwischen dem DNS-Dienstleister und seinen Kunden sehen vor, dass der DNS-Dienstleister Kundendaten nicht an Dritte weitergibt. Der Dienstleister wird gerichtlich aufgefordert, Kundendaten herauszugeben. Um dem zu entgehen, schließt der Betreiber die Firma und vernichtet die Daten.

Betroffener Bereich (Infrastruktur) Durch die Firmenschließung sind die Kunden unmittelbar betroffen.

Auswirkung und Reichweite (o) Die Stilllegung eines Registrars kann als weniger kritisch beurteilt werden als eventuell auf den ersten Blick angenommen. Der Registrar ist nur ein Mittler zwischen Domain-Besitzer und Registry. Der Name ist trotz Stilllegung weiterhin bei der Registry registriert, und der Besitzer kann sich gegenüber der Registry ausweisen. Bei einer geordneten Stilllegung ist zudem der Umzug der autoritativen DNS-Server unterbrechungsfrei möglich.

Sollte der DNS-Dienstleister eine ungeordnete Stilllegung vornehmen, d.h. alle Dienste ohne Vorwarnung herunterfahren, dann wären alle Domain-Namen, für die er die autoritativen Name Server betreibt, betroffen.

Dauer (∞) Die Stilllegung der Firma und die Datenvernichtung sind endgültig. Die Kunden des DNS-Dienstleisters können aber einen neuen Registrar auswählen. Der damit verbundene Domain-Transfer kann innerhalb weniger Stunden erfolgen. Die Verweise auf die autoritativen DNS-Server müssen aktualisiert werden und entsprechende Cache-Einträge auslaufen. Die Lebenszeit der DNS-Einträge kann manuel über die Aktualisierung der `TTL` vorab angepasst werden.

Fehlerbehebung (Intern) Die Kunden können einen anderen DNS-Dienstleister nutzen.

Hardware-Ausfall eines Load Balancer Arrays
Technischer Defekt

Beschreibung DNS Load Balancer erlauben es, DNS-Anfragen auf mehrere physische DNS-Server zu verteilen. Der Load Balancer agiert als Proxy für die dahinterliegenden autoritativen DNS-Server, welche leistungsfähige Hardware aufweisen. Fällt der Load Balancer aus, können die Anfragen an diese DNS-Server nicht mehr weitergeleitet werden.

Betroffener Bereich (Management) Der Ausfall betrifft alle Resolver, die per Anycast an den ausgefallenen Load Balaner weitergeleitet werden.

Auswirkung und Reichweite (–) Der Ausfall eines einzelnen Load Balancers sollte geringfügige Auswirkungen auf die vom DNS-Dienstleister verwalteten Namen haben, da mindestens zwei autoritative DNS-Server pro DNS-Zone vorzusehen sind.

Dauer (h) Sollte der Load Balaner ausfallen, kann die IP-Adresse von einem anderen Gerät übernommen werden. Durch Virtualisierungsmäsnahmen der IP-Adresse (z.B. Virtual Router Redundancy Protocol, VRRP) kann zudem von konkreten Geräten abstrahiert werden, so dass ein automatisches Umschalten erfolgt

Fehlerbehebung (Service) Der DNS-Betreiber kann mehrere IP-Adressen für autoritative DNS-Server im DNS hinterlegen. welche auf unterschiedliche Load Balancer verweisen. Darüber hinaus sollte er über Service-Verträge seine betriebskritische Infrastruktur abgesichert haben.

3.5 Totalausfall eines wichtigen Internetknotenpunktes

3.5.1 Kurzdarstellung

Internet Exchange Points (IXPs) bilden primär regionale, physische Infrastrukturen, welche es den ansässigen Providern ermöglichen, Daten multilateral direkt auszutauschen. IXPs bestehen in ihrem Kern aus einer Switch-Plattform (auf dem Layer 2), an welche sich teilnehmende Provider anschließen und so direkt Daten und Routing-Informationen austauschen können. Es ist gängige Praxis unter IXPs, öffentliche Route-Server bereitzustellen, um den Austausch von Routing-Informationen zu vereinfachen. Anstatt mit jedem teilnehmenden ISP eine BGP-Session zu unterhalten, brauchen die Provider lediglich mit dem Route-Server zu peeren, um alle öffentlichen Wegeinformationen zu erhalten. Neben öffentlichem Peering gibt es an den meisten IXPs auch privates Peering. Der Austausch der Routing-Informationen erfolgt dann direkt zwischen den privaten Peers – ohne Route Server. Öffentliches und privates Peering wird an vielen IXPs in unterschiedlichen IEEE 802.1Q VLANs separiert – so auch am DE-CIX.

In diesem fiktiven Szenario nehmen wir an, dass der größte (deutsche) Internet Exchange Point ausfällt, also die Switching-Infrastruktur des DE-CIX in Frankfurt funktionslos wird. Dies kann entweder dadurch geschehen, dass die physische Infrastruktur zusammenbricht, oder dass die logische Steuerung die Infrastruktur außer Funktion setzt. Dabei besteht die logische Steuerung der Infrastruktur sowohl in der Konfiguration der Switches, welche teilweise auch Software-Defined Networking (SDN) einsetzen, als auch im Betrieb der Route-Server. Im Ergebnis werden keine Datenpakete mehr am DE-CIX ausgetauscht.

Potentielle Schwachstellen IXPs sind heute komplexe Infrastrukturen und können vielfältig angegriffen werden. Dies gilt insbesondere für die martkführenden IXPs, die transregional und international Dienste anbieten, im Vergleich zu kleinen, regionalen IXPs. Neben physischen Ausfällen von Geräten und verbindenden Kabeln in und zwischen Rechenzentren, können die betriebenen Geräte, d.h. Switches, SDN-Controller, Route-Server, Fehler in Hardware und Software aufweisen sowie auf der Management-Ebene beeinträchtigt werden. Darüber hinaus ist der Route-Server von Fehlern betroffen, welche auf Anomalien in der Kontrollschicht zurückzuführen sind. Auch auf der Datenschicht kann ein IXP z.B. durch gezielte Überlast beeinträchtigt werden. Insgesamt bildet das Ökosystem bestehend aus Infrastrukturbetreiber und Teilnehmern an einem IXP ein System, welches aus vielen heterogenen Komponenten unterschiedlicher Betreiber besteht und so vergleichsweise einfach Betriebsschwankungen und -störungen ausgesetzt werden kann.

Auswirkungen Der DE-CIX ist als IXP eine Infrastruktur zur Optimierung der Verkehrsflüsse im Internet. Entsprechend bestätigt diese Detailanalyse, dass der DE-CIX zwar deutliche Beiträge zur Leistung der regionalen Internet-Kommunikation, nicht aber zur Erreichbarkeit erbringt. Ein Ausfall des Frankfurter Internet-Knotenpunkts bewirkt für viele Beteiligte vorhersehbare Kapazitätseinbussen und erhöhte Latenzen. Eine Fragmentierung des Internets ist jedoch nicht zu erwarten.

3.5.2 Ausgangssituation

Der DE-CIX in Frankfurt ist gemessen an seinem Datenaustausch der weltweit größte Internet eXchange Point und verzeichnet kontinuierlich wachsende Volumina (vgl. Abbildung 3.20). In diesem Frühjahr hat die Spitzenverkehrsrate während eines großen Online-Updates 9 Tbps sprunghaft überschritten.

Die Infrastruktur des DE-CIX besteht im Kern aus einer verteilten Switching-Plattform, welche sich über 37 Standorte in Frankfurt und Umgebung erstreckt, sowie die Route Sever `rs1` und `rs2` für das Public Peering sowie `rsbh` für den Blackholing-Dienst. Die Plattform basiert auf einem 48 Tbps vermaschten optischen Backbone mit Transportgeschwindigkeiten von bis zu 8 Tbps pro Glasfaser. Zum Einsatz gelangen die carrier-grade Switches 7950 XRS und 7750 SR-s von Nokia (ehemals Alcatel-Lucent), welche eine besonders hohe Portdichte aufweisen. Die DE-CIX Kunden können zwischen Zugangsports in Leistungsklassen von 1 Gbps bis 400 Gbps wählen.

Neben der physischen Präsenz an einem der 37 Frankfurter Standorte können Netzbetreiber auch aus der Ferne über Wiederverkäufer einen DE-CIX Anschluss erhalten. Infrastrukturbetreiber wie IXREACH oder Retn bieten aus ihrer international verteilten Präsenz Remote IXP Peering [49] an, indem sie (mithilfe von optischem Switching oder VLAN Tagging) virtuelle Layer-2 Links zum IXP führen, die dort auf ein endkundenspezifisches (Sub-)Interface geführt werden. Seit einiger Zeit entwickelt der DE-CIX selbst unter dem Namen ‘GlobePEER Remote’ ein ähnliches Angebot des Remote Peerings mit assoziierten oder wirtschaftlich beherrschten IXPs: So kann z.B. ein am BCIX Berlin lokal vertretenes Netz einen (virtualisierten) Zugang zu der DE-CIX Infrastruktur in Frankfurt erhalten. Grundlage für dieses Angebot bildet ein verbindendes Leitungsnetz zwischen den IXPs, wie in Abbildung 3.21 veranschaulicht.

Routen zu mehr als 225.000 IPv4 Präfixen sind an den DE-CIX Route Servern öffentlich verfügbar und damit knapp ein Drittel der vollständigen globalen Tabellen. Ein Peering-Kunde benötigt somit weitere Internet-Anbindungen, um volle Internet-Konnektivität

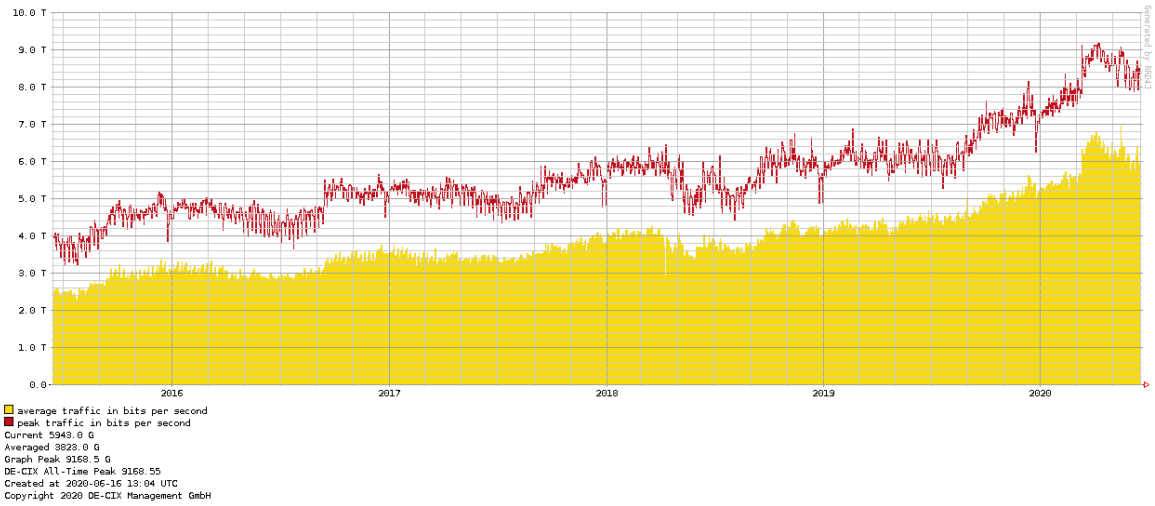


Abbildung 3.20: Verkehrsentwicklung am DE-CIX in den letzten 5 Jahren (Quelle: DE-CIX)

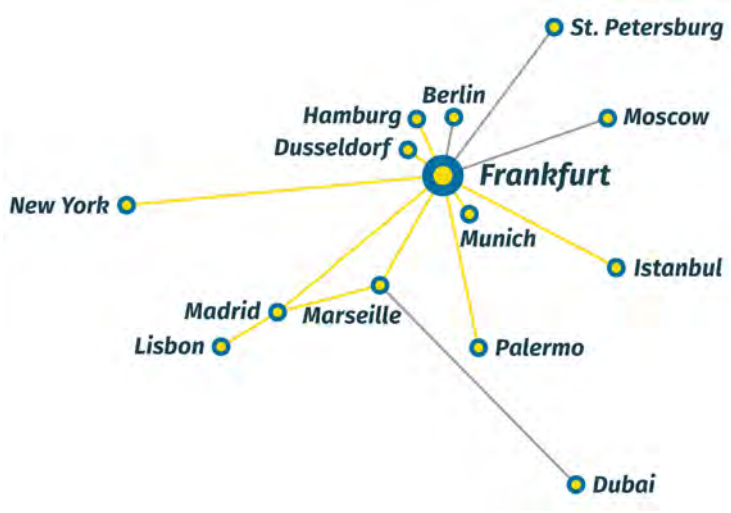


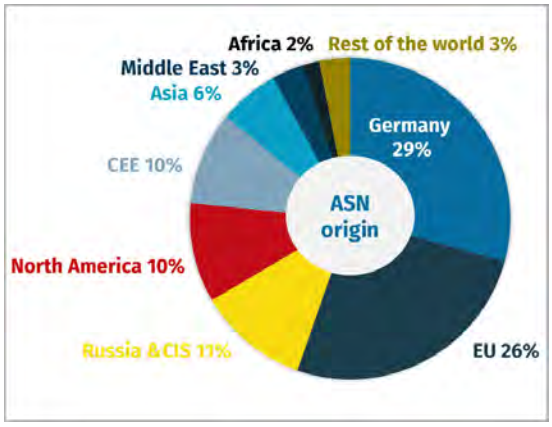
Abbildung 3.21: Inter-IXP-Links für ein Remote Peering am DE-CIX (Quelle: DE-CIX)

zu erreichen. Insbesondere ist der Einkauf von Upstream erforderlich, denn den Messungen von Böttger et al. [50] folgend kann auch durch die Präsenz im öffentlichen Peering auch an mehreren IXPs nicht mehr als $\sim$ 80% des IPv4 Adressbereichs im Internet erreicht werden. Eine Internet-Präsenz ohne eigentlichen Provider ist deshalb unüblich und nur in besonderen Ausnahmefällen sinnvoll. Die Anbindung eines DE-CIX Kunden an einen ISP kann jedoch über die DE-CIX Switching-Infrastruktur im Rahmen eines private Interconnects geschaltet werden. Entsprechend sind Installationen denkbar, die (kleine) Netze ausschliesslich durch die DE-CIX Infrastruktur mit dem Internet verbinden.

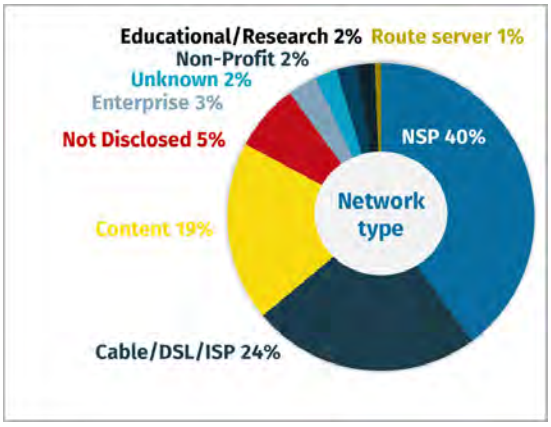
Gegenwärtig hat der DE-CIX $\sim$ 750 Kunden, die mit mehr als 900 Autonomen System in Frankfurt peeren. Diese Netze haben ihren Ursprung in weit verteilten Regionen (s. Abbildung 3.22a) und diversen Branchen (s. Abbildung 3.22b). Umfassend vertreten sind hierbei die nationalen Service-Provider (NSPs)[12] aus Europa und angrenzenden Kontinenten, die Endkunden (Eyeball) Provider sowie die Content-Provider und Hypergiants. Ergänzt wird das Kundenspektrum von einem über die Jahre gewachsenen Ökosystem von netzaktiven Unternehmen, die von der zentralen europäischen Lage des DE-CIX profitieren. Dabei repräsentieren die DE-CIX Kunden den durchschnittlichen Branchenmix in Europa weitgehend (s. Abbildung 3.23).

Die Kunden des DE-CIX profitieren vor allem von schnellem, lokalen Datenaustausch auf einer technisch leistungsstarken Plattform mit der großen Zahl ebenfalls lokal präsenter Netze. Im Internet-Regelbetrieb wirkt der DE-CIX damit vor allem (i) kapazitätserhöhend und (ii) latenzmindernd. Privatkunden der Eyeballs etwa können schneller auf CDN Inhalte (aus lokalen Caches) zugreifen, und der regionalen Internet-Wirtschaft stehen hohe Zugangskapazitäten zu fast allen europäischen NSPs zur Verfügung. Der durchschnittlich gewählte Anschluss am DE-CIX liegt – mit hohen Schwankungen – bei 10GE. Hierfür werden am DE-CIX überdurchschnittlich hohe Nutzungsgebühren fällig (s. Abbildung 3.24). Im Gegenzug entlastet der direkte Datenaustausch am DE-CIX die Upstream-Links der

[12]Die Klassifikation 'NSP' in der PeeringDB umfasst alle Internet Service Provider, die Transit für andere Netze anbieten. Sie grenzt damit zu Access-Providern (Eyballs) ab, welche als 'Cable/DSL/ISP' kategorisiert werden.



(a) Ursprung der ASNs



(b) Typ der ASNs

Abbildung 3.22: Die Struktur der am DE-CIX verbundenen Netzwerke (Quelle: DE-CIX)

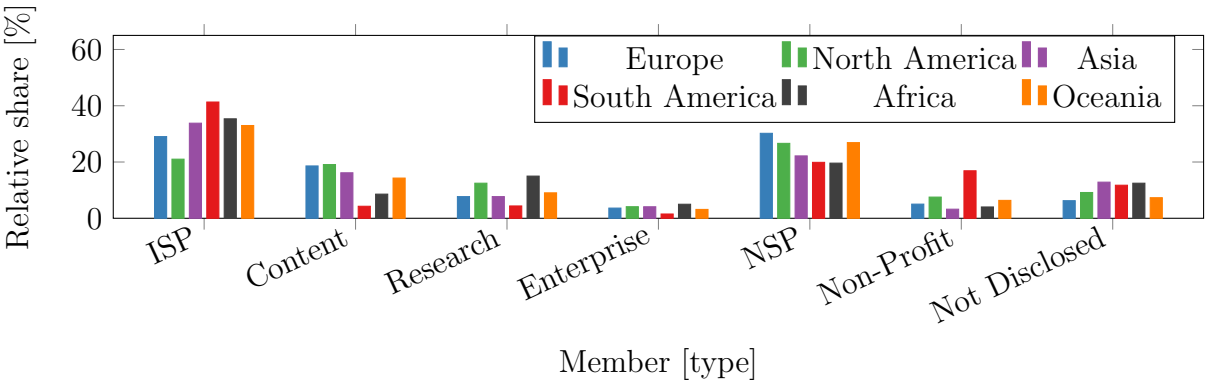


Abbildung 3.23: Verteilung der Kundenstrukturen an IXPs weltweit

Transitprovider und reduziert damit auch die Verkehrskosten, welche Kunden anderweitig an ihre ISPs zu entrichten hätten.

Die Switching-Infrastruktur am DE-CIX wird sowohl für das öffentliche Peering, als auch für bilaterale, private Interconnects verwendet. 37 ($\sim$ 4 %) der angeschlossenen Netze peeren ausschließlich privat, darunter die Deutsche Telekom AG (DTAG). Diese Kunden nutzen die verteilte Infrastruktur mit hoher Netzdichte vor Ort, um Vertragsbeziehungen mit ausgewählten Kunden technisch umzusetzen. Die tatsächlichen Beziehungen sind Geschäftsgeheimnisse und nicht öffentlich bekannt, wobei es grundsätzlich denkbar ist, dass einzelne (kleinere) Endkunden ihre Provideranschlüsse ausschließlich über die IXP Infrastruktur realisieren. Endkunden, die diesen Weg wählen, sollten sich allerdings der Abhängigkeit von der lokalen DE-CIX Infrastruktur bewusst sein.

3.5.3 Auswirkungen und mögliche Reichweiten

Ein Totalausfall der DE-CIX Infrastruktur bedeutet zunächst ein Re-Routing für die angeschlossenen Kunden: Übergänge am DE-CIX verschwinden und werden von Übergängen an anderen europäischen IXPs, privaten Peerings oder über Upstream-Transit

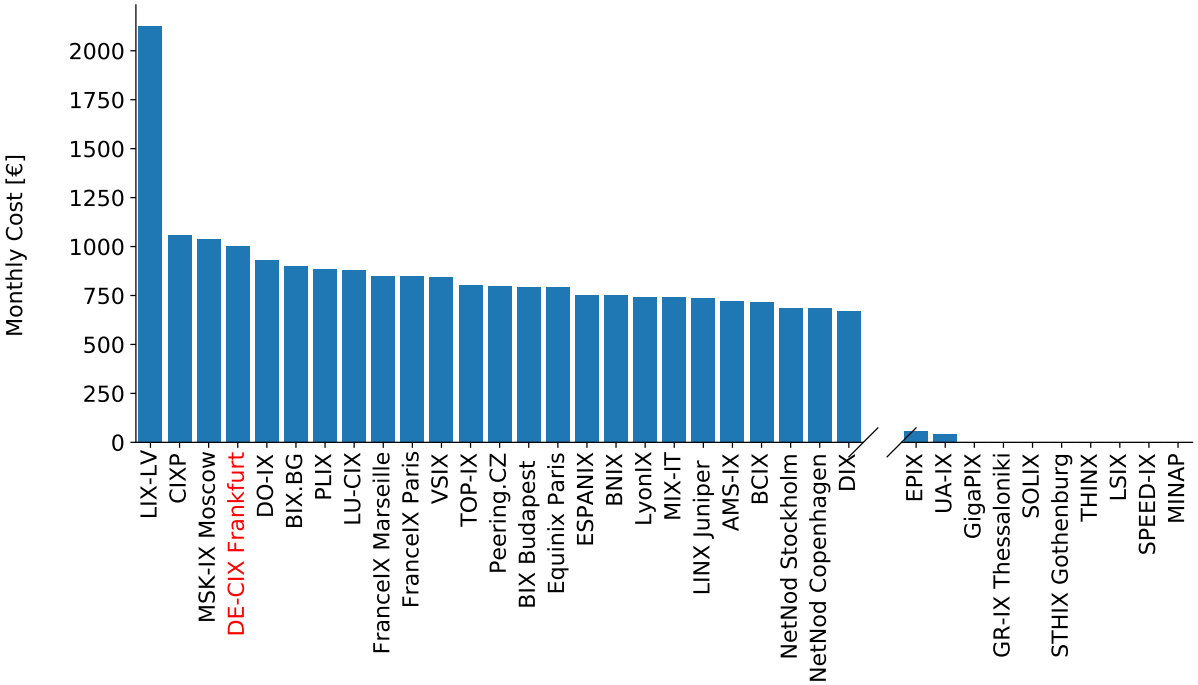


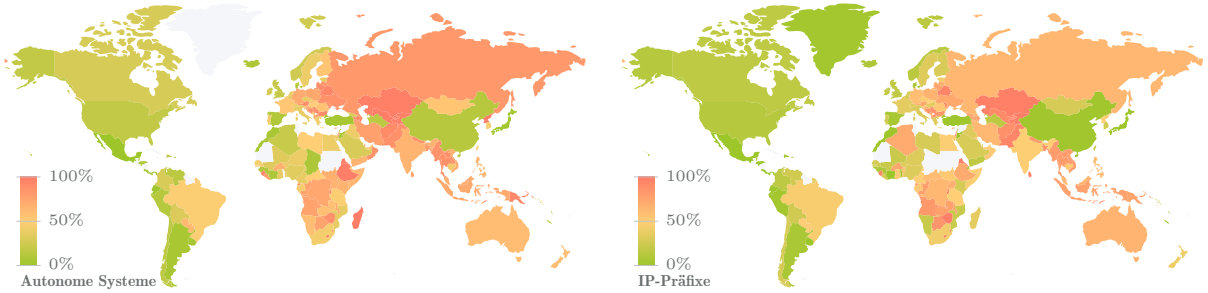
Abbildung 3.24: Verteilung der monatlichen Kosten für ein 10GE Interface an IXPs in Europa

ausgeglichen. Dieser Prozess wird im BGP automatisch angestoßen und konvergiert in der Regel innerhalb von Minuten. Hiernach können alle (nicht ausschließlich) am DE-CIX angeschlossenen Netze wieder mit dem restlichen Internet kommunizieren. Die tatsächlich zu erwartenden Auswirkungen des Ausfalls beschränken sich so auf regionale Latenzerhöhungen sowie den Wegfall der DE-CIX Kapazitäten.

Da der DE-CIX bisher nicht vollständig ausgefallen ist, liegen für diesen IXP keine realen Messergebnisse vor. Für den AMS-IX Ausfall vom 13. Mai 2015 allerdings haben Giotsas et al. [51] solche Auswirkungen des empirisch untersucht. Durch passive und aktive Messungen konnte die Gruppe zeigen, dass zwar die Mehrzahl der (sichtbaren) BGP-Routen von DE-CIX, LINX und anderen IXPs übernommen wurden, die ganz überwiegende Verkehrslast jedoch über Transitprovider abgwickelt wurde ($\sim$ 70%). Die Latenz verdoppelte sich für etwa die Hälfte der Flüsse, welche den AMS-IX ehemals durchquerten. Im Detail betroffen waren Datenflüsse, welche bereits vor dem Ausfall mit einer Round-Trip-Time (RTT) von mehr als 50 ms langsam waren: Blieben vor dem Ausfall 80% der Flüsse am AMS-IX unter einer RTT von 100 ms, so zeigten beim Ausfall 45% der Flüsse eine RTT oberhalb von 100 ms.

	Ziel ASNs	IP–Präfixe	/24–Äquivalente
Betroffen am DE-CIX	29,264	225,404	1,565,207
Gesamtheit im Internet	67,561	799,995	11,140,972

Tabelle 3.7: Anteil der von einem DE-CIX Ausfall betroffenen Internet-Resourcen



(a) Betroffene ASNs (b) Betroffene Präfixe

Abbildung 3.25: Relative geographische Verteilung aller vom Ausfall betroffenen Netze und IP-Präfixe. Rot entspricht dem Maximum, grün dem Minimum.

Im Allgemeinen sind von diesen Topologieänderungen alle Pfade betroffen, welche im Public Peering der DE-CIX Route Server announciert werden.[13] Tabelle 3.7 gibt eine quantitative Übersicht über die Präfixanzahl, ihre zugehörigen Autonomen Systeme sowie die Größe des betroffenen IP-Adressraums (in /24-Äquivalenten) im Verhältnis zum Gesamt-Internet. Hiernach sind gut 40% der weltweiten ASe und IP-Präfixe betroffen, hingegen nur $\sim$ 15% des IP-Raums.

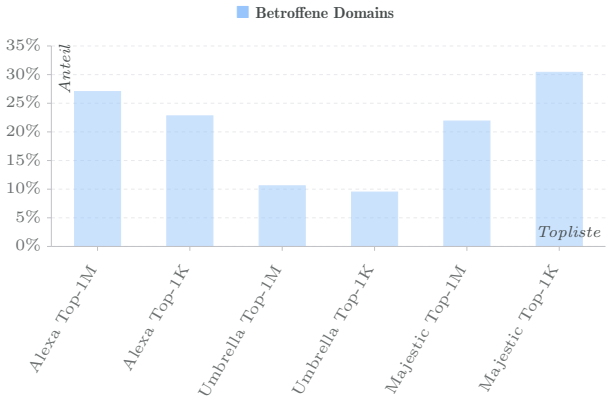
Für die Internet-Nutzer, also Endkunden genauso wie Verteilinfrastrukturen und den Geschäftsdatenaustausch, bedeutet eine Topologieänderung nach einem Ausfall zunächst eine kurzfristige Störung infolge des Re-routings. Kunden, die z.B. auf die Facebook-Seiten zugreifen, erleben einen momentanen Ladefehler im Browser, der aber nach kurzer Zeit (wenigen Reloads) wieder verschwindet. Betroffen sind dabei vor allem die regionalen Kunden, deren Zugriffsweg über den DE-CIX deswegen erfolgt, weil der dortige Übergang als Abkürzung zu einem ebenfalls am DE-CIX präsenten Provider genutzt wird – z.B. ein O2-Kunde aus dem mitteldeutschen Raum, der auf Facebook zugreift. Internet-Beziehungen zu weiter entfernten Zielen sind vor allem mit dem osteuropäischen Raum betroffen, wie im folgenden Abschnitt dargestellt wird.

Regionale Auswirkungen

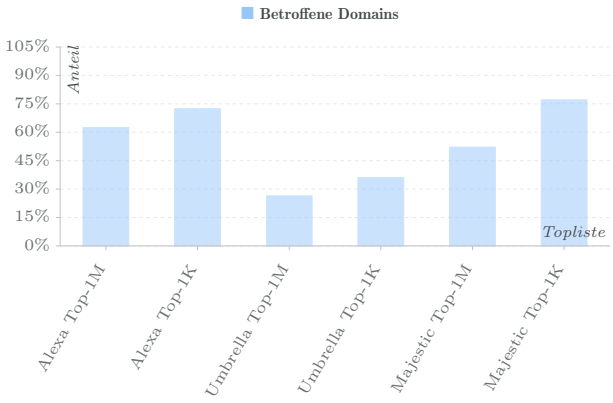
Diese Auswirkungen verteilen sich sehr unterschiedlich über die Regionen dieser Welt. Abbildung 3.25 visualisiert die geographische Verteilung der relativen ASN- und Präfix-Anteil. Deutlich sichbar ist der große Einfluss auf viele der ehemals sowjetischen Länder, was auf die starke Präsenz von regionalen Transitprovidern wie RETN zurückgeführt werden kann.

Beachtenswert ist bei dieser relativen Darstellung, dass ebenfalls sehr viele betroffene Netze in den Vereinigten Staaten angesiedelt sind, allerdings aufgrund der viel höheren Netzdichte dort anteilig weniger Gewicht haben. Verschiedene Darstellungen der geographischen Verteilungen können unter `https://zwiback.leitwert.net/#/fictional/ixp` interaktiv betrachtet werden.

[13] Privat ausgetauschte Pfade sind ebenfalls betroffen, aber nicht öffentlich sichtbar und können deshalb nicht untersucht werden.



(a) Betroffene Top-Domains in Europa



(b) Global betroffene Top-Domains

Abbildung 3.26: Verteilung der betroffenen populären Dienste gemäß der Top-Listen Alexa, Umbrella und Majestic.

Auswirkungen auf der Dienstebene

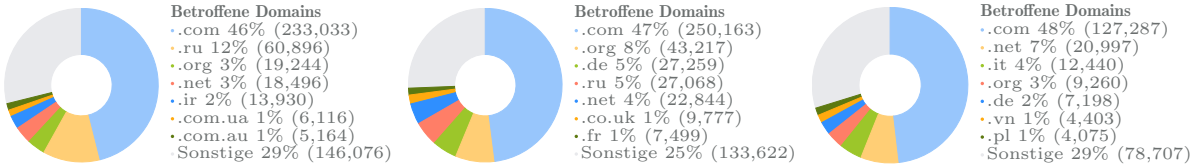
Die Auswirkungen des Ausfalls werden häufiger und als schwerwiegender wahrgenommen, wenn populäre Online-Dienste betroffen sind. Die Relevanz von Websites wird regelmäßig von verschiedenen Akteuren gemessen und in sogenannten Top-X-Listen veröffentlicht; Beispiele hierfür sind die Alexa-, Umbrella- oder Majestic-Toplist. Die Bewertungen dieser Top-Listen schwanken allerdings stark untereinander und von Tag zu Tag. Wir stellen die Statistiken von bei einem DE-CIX Ausfall betroffenen populären Domains deshalb parallel für die drei Top-Listen Alexa, Umbrella und Majestic jeweils für Rangordnungen von Eintausend und einer Million dar. Wir unterscheiden ferner nach europäischen und globalen Diensten.

Erwartungsgemäß fluktuieren die Ergebnisse stark, zeigen aber insgesamt signifikante Auswirkungen auf die Top-Domains: Etwa ein Drittel der globalen Top-Domains liegt in einem IP-Bereich, der im Falle eines DE-CIX Ausfalls umgeleitet werden müsste. 15% dieser Domains liegen dabei in Europa. Kunden, die diese Dienste im Normalfall über die DE-CIX Infrastruktur nutzen, könnten demnach eine Verschlechterung der Dienstqualität erleben.

Die hiervon betroffenen Dienste verteilen sich auf Top Level Domains (TLDs) wie in Abb. 3.27 (weltweit) und Abb. 3.28 (Europa) dargestellt. Erwartungsgemäß dominieren kommerzielle (.com) Domains, da diese auch in den Top-Listen häufiger vertreten sind. Bemerkenswert ist die überproportionale Verknüpfung mit russischen (.ru) Domains, was im Einklang mit den geographischen Beobachtungen in Abb. 3.25 steht. Deutsch gekennzeichnete (.de) Domains spielen lediglich in Europa eine sichtbare Rolle, was ebenfalls auf ihre geringe Präsenz in den Top-Listen zurückzuführen ist.

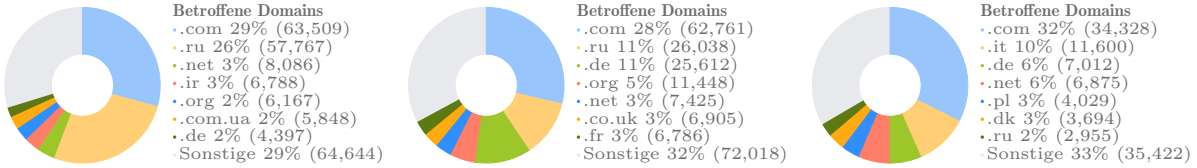
Netzwerke, die in Europa nur am DE-CIX peeren

NSPs und andere Netz-Provider peeren i.d.R. an diversen IXPs, um lokale Datenaustausche zu befördern und Transitkosten zu minimieren. Darüber hinaus unterhalten sie PoPs in weiteren Rechenzentren (facilities), wo sie bilateral mit anderen Betreibern vor



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.27: Verteilung der betroffenen populären Dienste gemäß der Top-Listen Alexa, Umbrella und Majestic.



(a) Alexa Top-1M (b) Majestic Top-1M (c) Umbrella Top-1M

Abbildung 3.28: Verteilung der betroffenen *europäischen* Dienste gemäß der Top-Listen Alexa, Umbrella und Majestic.

Ort Daten austauschen. Diese Netzbetreiber sind vergleichsweise unabhängig von einzelnen IXPs und können sowohl Routen wie Kapazitäten leicht und kontinuierlich verlagern. Die detaillierte Untersuchung der Peering-Präsenz aller Teilnehmer eröffnet einen weitergehenden Einblick in die Abhängigkeit vom DE-CIX und beleuchtet auch die Frage nach wahrscheinlichen Ausfallszenarien.

Abbildung 3.29 zeigt die Präsenzstatistik der Netze am DE-CIX. Wir unterscheiden nach IXPs und anderen PoPs in Europa und dem Rest der Welt. Dargestellt sind alle ASNs geordnet nach der Häufigkeit ihrer Präsenz an europäischen IXPs und PoPs sowie globalen IXPs und PoPs. Die überwiegende Mehrzahl der Teilnehmer unterhält mehr als 10 europäische Austauschpunkte, viele darüber hinaus auch eine multilaterale internationale Präsenz.

162 ASes sind am DE-CIX als einzigem IXP in Europa präsent. Diese Teilnehmer werden indivdiuell in Tabelle 3.8 aufgeführt. Unter diesen sind viele ASes aus fernen Ländern, wo deren eigentliches Peering-Umfeld liegt, und die per Remote Peering an den DE-CIX angeschlossen sind. Als Beispiel sei der südamerikanische Provider INTERNEXA (Nr. 161, AS262589) genannt, der an 13 IXPs und 21 sonstigen PoPs außerhalb Europas präsent ist. INTERNEXA ist Teil der ISA ‘Multi-Latin Business Group’, deren Ziel die Infrastrukturversorgung von Lateinamerika ist. Der Ausfall des 20G Links am DE-CIX würde sicherlich merkliche Leistungseinbußen in der europäischen Konnektivität bedeuten; das Kerngeschäft des ISPs in Südamerika wäre hiervon aber nicht betroffen.

44 ASes (Nr. 1–44) sind alleine am DE-CIX präsent. Sie verfügen über keinen anderen Link an einem IXP oder sonstigem PoP. Alle ASNs verfügen aber über einen Uplink zu mindestens einem Provider, so dass ihre Erreichbarkeit nicht primär vom DE-CIX abhängt. Viele dieser Netze sind regionale Organisationen, Eyeballs oder solche Firmen, die die räumliche Nähe zum DE-CIX ausnutzen, um ihre Netzanbindung nach Leistung und Kosten zu optimieren. Beispiele sind die BV-Zahlungssysteme (Nr. 25, AS43509) und die Porsche AG (Nr. 33, AS33848), die den regionalen Zugang zum DE-CIX nutzen, sonst

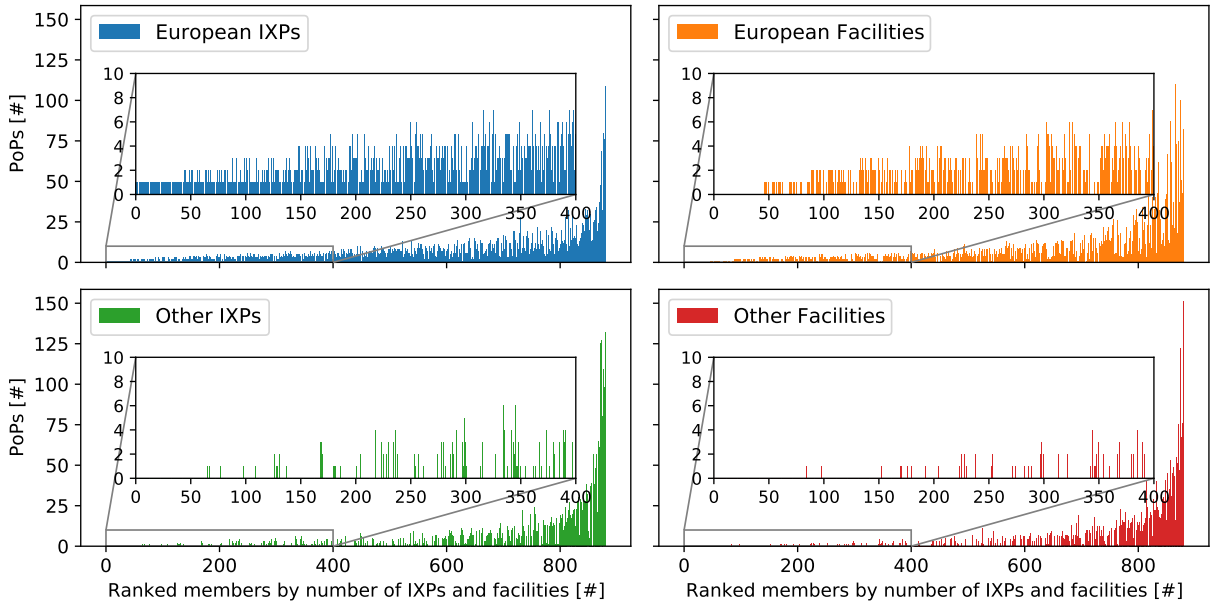


Abbildung 3.29: PoP-Präsenz von DE-CIX Netzwerken – angeordnet nach dem Rang ihrer Peering-Häufigkeit an IXPs und Präsenz an weiteren PoPs.

aber über zwei/drei Provider-Uplinks verfügen. Die so gewonnene Konnektivität (2 x 10G) hat vermutlich einen wesentlichen Anteil an der Qualität ihrer Internet-Versorgung. Im Gegensatz hierzu ist das US Unternehmen Avaya (Nr. 34, AS18676), das ebenfalls mit 2 x 10G ausschließlich am DE-CIX vertreten ist, über 10 Upstream-Provider weltweit verknüpft. Ein remote Peering aus den USA, wie es der DE-CIX anbietet, ermöglicht der Technologiefirma vermutlich, eine deutlich verbesserte europäische Konnektivität bei geringem Aufwand zu erlangen.

Ähnlich wie Porsche unterhält die SAP AG (Nr. 60, AS12510) zwei 10G Links am DE-CIXs in Ergänzung zu drei Upstream-Providern, ist allerdings zusätzlich noch an einem weiteren europäischen Datencenter vertreten. Ähnlich verhalten sich andere nationale Unternehmen wie MAN (Nr. 92, AS205881) oder Bechtle (Nr. 83, AS21161). NSPs und regionale ISPs sind oft stärker an weiteren Colocationen vertreten und oft auch an mehreren IXPs.

Alle Netze am DE-CIX halten Konnektivität zu einem oder mehreren Upstream Providern – mit Ausnahme von NOK-ION-LABS (Nr. 79, AS38016). Dieses Netz unterhält zwar Verbindungen zu einem nichteuropäischen IXP und peert an einem weitern Standort, hat allerdings gem. Peering-Daten keinen Zugriff auf die vollständige globale Routing-Tabelle mangels Provider. Da es sich hierbei aber um eine Forschungs- und Experimentiernetz zu handeln scheint, muss von einer bewussten Wahl ausgegangen werden.

Zusammenfassend bestätigt diese Detailanalyse, dass der DE-CIX zwar deutliche Beiträge zur Leistung der regionalen Internet-Kommunikation, nicht aber zur Erreichbarkeit erbringt. Ein Ausfall des Frankfurter Internet-Knotenpunkts bewirkt für viele Beteiligte vorhersehbare Kapazitätseinbussen und erhöhte Latenzen. Eine Fragmentierung des Internets ist jedoch nicht zu erwarten.

AS type colors:

ISP	Content	NSP	Non-Profit
Research	Enterprise	Not Disclosed	Route Server

	ASN	Owner	IXPs other	Fac. EU	Fac. other	UP-Link	Link speed
1	AS33082	ISC-F-AS, US	0	0	0	2	1G, 1G
2	AS6900	AS6900, DE	0	0	0	2	1G
3	AS8391	KNIPP-AS Martin-Schmeisser-Weg 9, DE	0	0	0	2	1G
4	AS42416	COMNET-AS, NL	0	0	0	5	1G
5	AS21336	INFORENT-AS, DE	0	0	0	2	1G
6	AS42605	FRA-VRNETZE, DE	0	0	0	3	1G
7	AS22300	WIKIA, US	0	0	0	2	1G
8	AS15743	NETDE net.de AG, DE	0	0	0	3	10G, 20G
9	AS9189	ACCOM, DE	0	0	0	2	200M
10	AS12348	AS12348 Hermann-Glockner-Str. 7, DE	0	0	0	4	1G
11	AS12316	FITSNET FITS Internet Backbone, DE	0	0	0	1	10G
12	AS10282	DIALIP-PR, US	0	0	0	1	10G
13	AS20633	UNIFFM-NET cords@rz.uni-frankfurt.de 20101227, DE	0	0	0	2	1G
14	AS12975	PALTEL-AS PALTEL Autonomous System, PS	0	0	0	8	1G
15	AS42459	FOBUL, BG	0	0	0	4	10G
16	AS200187	CLOUDKLEYER-AS, DE	0	0	0	2	1G
17	AS47169	HPC-MVM-AS, HU	0	0	0	3	1G
18	AS24582	SYNNET-1 synaix Gesellschaft fuer angewandte Informations-Technologien mbH, DE	0	0	0	3	1G
19	AS5409	TPL-ASN Robert-Bosch-Str. 20, DE	0	0	0	2	1G, 1G
20	AS25081	HDIT-AS, DE	0	0	0	3	1G
21	AS25068	KONICA-MINOLTA-EMEA-HEADQUARTER-AS, DE	0	0	0	2	10G
22	AS9038	BAT-AS9038, JO	0	0	0	7	10G
23	AS62363	EGW-AS, AT	0	0	0	3	1G
24	AS12625	AS12625 GERMANY, DE	0	0	0	3	10G, 10G
25	AS43509	BV-ZAHLUNGSSYSYSTEME-AS, DE	0	0	0	2	10G, 10G
26	AS197915	ALL-FOR-ONE-AS, DE	0	0	0	2	3G, 3G
27	AS199421	MTI-TELEPORT, DE	0	0	0	3	10G

28	AS34086	SCZN-AS, DE	0	0	0	2	5G
29	AS28748	ALPHACRON-AS AlphaCron Datensysteme, DE	0	0	0	2	1G
30	AS44974	REGIONETSW-AS, DE	0	0	0	3	2G
31	AS41033	D2-AS, GB	0	0	0	1	10G
32	AS200278	KNTINTERNET, DE	0	0	0	3	2G
33	AS33848	PORSCHE-AS, DE	0	0	0	3	10G, 10G
34	AS18676	AVAYA, US	0	0	0	10	10G, 10G
35	AS60051	EARTHLINK-DMCC, IQ	0	0	0	2	10G
36	AS47895	R-LINE-AS, RU	0	0	0	3	30G
37	AS203347	YALWA-AS, DE	0	0	0	1	N/A
38	AS197063	AS-PFALZCONNECT, DE	0	0	0	2	10G
39	AS196954	EPCAN epcan breitband loesungen, DE	0	0	0	5	10G
40	AS209400	KURPFALZTEL, DE	0	0	0	2	5G
41	AS21277	NEWROZ-TELECOM-ASN, IQ	0	0	0	7	10G
42	AS49958	EVO-AS, GB	0	0	0	2	10G, 10G
43	AS34432	PHH-AS, DE	0	0	0	4	10G
44	AS60979	KISG4, DE	0	0	0	2	10G, 10G
45	AS39257	INC, DE	0	1	0	2	10G
46	AS47215	FILOO-ASN Rhedaer Strasse 25, DE	0	1	0	3	10G
47	AS13054	FREINET Freiburg, Germany, DE	0	1	0	3	10G
48	AS29404	ELBRACHT-COMPUTER-AS, DE	0	1	0	2	10G
49	AS201764	MGMTP, DE	0	1	0	4	1G
50	AS9022	TWL-KOM-AS Donnersbergweg 4, DE	0	1	0	3	10G
51	AS198570	STNB-AS, DE	0	1	0	2	1G
52	AS61244	EURO-SAT, DE	0	1	0	1	10G
53	AS60169	GFIT-AS, DE	0	1	0	3	40G
54	AS203507	AVIRADE Kaplaneiweg 1, DE	0	1	0	6	10G
55	AS12480	ASILK, DE	0	1	0	3	1G, 1G
56	AS16316	TMT, DE	0	1	0	3	10G
57	AS199790	IPTELECOMBULGARIA-AS, BG	1	0	0	4	10G
58	AS198018	TRIVAGO-, DE	1	0	0	7	10G, 10G
59	AS20830	GLOBALAIRNETWORK-AS, DE	0	1	0	3	1G

60	AS12510	SAP_DC_WDF network/mail abuse to abuse@sap.com, DE	0	1	0	3	10G, 10G
61	AS29624	KRICK-TECHNOLOGIC-AS Mainparkring 4, DE	0	1	0	2	10G
62	AS9197	BECOMGMBH-AS Germany, D-35578 Wetzlar, DE	0	1	0	2	1G
63	AS30766	GGEWNET-AS Dammstrasse 68, DE	0	1	0	2	1G
64	AS60752	AOSSIA-AS, BG	0	1	0	4	1G
65	AS49666	TIC-GW-AS, IR	1	0	0	9	300G
66	AS12808	DTMS-AS, DE	0	1	0	1	1G, 1G
67	AS196714	TNETKOM-AS, DE	0	1	0	2	10G
68	AS396986	BYTEDANCE, US	0	0	1	3	100G
69	AS42587	MAGNAEU, AT	0	1	0	2	1G, 1G
70	AS207419	HYBRIS, DE	0	1	0	2	10G, 10G
71	AS207588	IQ-PRIMETELECOM, IQ	0	1	0	2	10G
72	AS12312	ECOTEL, DE	0	2	0	2	10G, 10G
73	AS2857	RLP-NET, DE	0	2	0	4	10G, 10G
74	AS41289	DWD-AS, DE	0	2	0	2	1G, 1G
75	AS20810	NETCOM-KASSEL Netcom Kassel, DE	0	2	0	1	20G, 20G
76	AS8823	AUTONOMOUSSYSTEMROCK DE	0	2	0	7	10G
77	AS20771	CAUCASUS-CABLE-SYSTEM CCS Autonomous System, GE	0	2	0	5	10G
78	AS24679	SSERV-AS, DE	0	2	0	5	10G
79	AS38016	NOK-ION-LABS Nokia IP/Optical Networks Labs, AU	1	0	1	0	1G
80	AS49024	FHE3, DE	0	2	0	2	10G
81	AS39216	ALSARD, IQ	0	2	0	7	10G
82	AS42390	THECLOUD-DE, GB	0	2	0	3	2G
83	AS21161	ASN-BECHTLE Neckarsulm, DE	0	2	0	6	10G
84	AS47372	BIG3AS, DE	0	2	0	3	10G
85	AS48152	DIGITAL-REALTY-, DE	0	2	0	4	10G, 10G
86	AS12748	IAV, DE	1	1	0	4	10G
87	AS42652	DELUNET, DE	0	2	0	4	100G
88	AS200185	XANDMAIL-ASN, DE	0	2	0	3	10G

89	AS196819	TWK-KL-AS, DE	0	2	0	3	10G
90	AS200561	PLACETEL, DE	0	2	0	3	1G
91	AS41998	NETCOMBW-AS, DE	0	2	0	4	100G
92	AS205881	MAN, DE	0	2	0	2	10G, 10G
93	AS196968	ILM-PROVIDER-AS, DE	0	2	0	2	10G
94	AS263626	G-LAB Telecom Informatica LTDA - ME, BR	2	0	0	4	1G
95	AS262376	NOVANET TELECOMUNICACAO LTDA, BR	2	0	0	1	1G
96	AS12857	TDS, DE	0	2	0	3	10G
97	AS8319	NETHINKS-AS NETHINKS GmbH, DE	0	3	0	2	10G
98	AS8879	DTS-SYSTEME DTS Systeme GmbH, DE	0	3	0	2	5G, 5G
99	AS8469	PIRONETNDH-AS CANCOM Pironet AG & Co. KG, DE	0	3	0	2	10G, 1G
100	AS39915	PREM-AS, IE	0	3	0	12	1G
101	AS41412	MIVITEC-AS, DE	0	3	0	4	10G
102	AS20849	CONTINUM, DE	0	3	0	3	10G
103	AS58010	UVENSYS, DE	0	3	0	4	10G
104	AS50061	PWC-EUROPE Pricewaterhou-seCoopers Europe, DE	0	3	0	2	10G
105	AS268696	TUDDO INTERNET LTDA, BR	3	0	0	2	500M
106	AS23201	Telecel S.A., PY	3	0	0	1	5G
107	AS52866	Iveloz Telecom, BR	2	0	1	3	500M
108	AS42705	TALIA Talia provides VSAT network and hosting services worldwide., GB	0	2	1	11	10G
109	AS21473	MANET-AS Koschatplatz 1, DE	0	4	0	2	10G
110	AS6083	POSIX-AFRICA, ZA	1	2	1	1	100M
111	AS29037	TELIKO-AS, DE	0	4	0	4	10G
112	AS34624	MEGASPACE-AS, DE	0	4	0	5	2G
113	AS62023	NYNEX, DE	0	4	0	2	10G
114	AS50533	ITENOS ITENOS GmbH, DE	0	4	0	5	10G
115	AS55805	MOBICOM-AS-MN MobiCom Corporation, MN	2	1	1	3	10G
116	AS50020	RACCOM-AS, BG	0	4	0	2	1G
117	AS13045	HTP-AS, DE	0	4	0	3	50G
118	AS52937	FHP TELECOMUNICACAO E COM VAREJISTA DE PRO-DUTOS DE, BR	4	0	0	4	500M
119	AS263421	NR Telecom EIRELI - ME, BR	3	0	1	3	1G
120	AS19318	IS-AS-1, US	2	0	2	4	10G

121	AS24088	HTCHCMC-AS-VN Hanoi Telecom Joint Stock Company - HCMC Branch, VN	2	0	2	7	1G
122	AS268976	P16 Telecom, BR	3	0	1	2	1G
123	AS11432	Telium Telecomunicacoes Ltda, BR	4	0	0	8	1G
124	AS53180	Infortel Telecomunicacoes e Servicos EIRELI - ME, BR	2	0	2	2	10G
125	AS25560	RHTEC-AS rh-tec IP Backbone, DE	0	5	0	2	10G
126	AS31400	ACCELERATED-IT, DE	0	5	0	5	10G
127	AS44066	DE-FIRSTCOLO www.first-colo.net, DE	0	5	0	6	50G, 50G
128	AS12678	BADOO-U, GB	2	1	2	5	20G
129	AS51862	PROFITBRICKS-AS, DE	0	4	1	4	N/A
130	AS12897	HEAGMEDIANET Darmstadt, Germany, DE	0	5	0	4	20G
131	AS35313	BH-INFONAS-ASN, BH	2	2	1	2	1G
132	AS39499	HAWE-AS, PL	0	5	0	0	10G
133	AS265269	MEGA TELEINFORMATICA EIRELI, BR	3	0	2	2	750M
134	AS61102	INTERHOST, IL	1	1	3	4	10G
135	AS262354	Ligue Telecomunicacoes Ltda, BR	5	0	0	2	1G
136	AS28202	Rede Brasileira de Comunicacao Ltda, BR	3	0	2	4	1G
137	AS29686	PROBENETWORKS-AS, DE	0	6	0	3	10G
138	AS20686	BISPING ISP & Citycarrier, Germany, DE	0	6	0	4	1G
139	AS21413	ENVIA-TEL-AS D-09114 Chemnitz, DE	0	6	0	5	20G, 20G
140	AS10158	KAKAO-10158-AS-KR Kakao Corp, KR	6	0	0	5	1G
141	AS53162	VOIPGLOBE SERVICOS DE COM MULTIMIDIA VIA INTERNET, BR	2	0	4	3	1G
142	AS262503	PAULO DE TARSO DE CARVALHO BAYMA FILHO, BR	6	0	0	3	500M
143	AS38193	TWA-AS-AP Transworld Associates (Pvt.) Ltd., PK	1	3	3	5	40G
144	AS20459	TELECOM-NAMIBIA-AS, NA	3	2	2	2	10G
145	AS3580	PLANET, US	3	0	4	2	1G
146	AS52873	SOFTDADOS CONECTIVIDADE, BR	6	0	3	3	20G
147	AS27281	QUANTCAST, US	4	1	4	3	10G, 10G

148	AS3786	LGDACOM LG DACOM Corporation, KR	5	1	4	7	20G
149	AS33011	BOXNET, US	4	1	5	7	2G
150	AS6695	DECIX-AS DE-CIX Management GmbH, DE	0	11	0	0	10G, 10G, 10G
151	AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	1	3	7	8	N/A
152	AS55967	BAIDU Beijing Baidu Netcom Science and Technology Co., Ltd., CN	6	1	5	4	10G
153	AS22381	Megatelecom Telecomunicacoes Ltda, BR	3	0	9	6	400M
154	AS17639	CONVERGE-AS Converge ICT Solutions Inc., PH	9	0	6	16	1G
155	AS61832	Fortel Fortaleza Telecomunicacoes Ltda, BR	7	0	8	9	20G
156	AS32425	SKB3-ARIN-BGP, US	10	0	6	3	N/A
157	AS28663	FLYS INTERATIVA LTDA, BR	11	0	6	6	1G
158	AS18403	FPT-AS-AP The Corporation for Financing & Promoting Technology, VN	11	1	6	13	20G
159	AS53889	MICFO, US	1	1	19	1	1G
160	AS22356	Durand do Brasil Ltda, BR	12	0	12	4	2G
161	AS262589	INTERNEXA BRASIL OPERADORA DE TELECOMUNICACOES S.A, BR	13	0	21	11	20G
162	AS29838	AMC, US	9	3	40	5	2G, 1G

Tabelle 3.8: Netzwerke, die in Europa nur am DE-CIX peeren, geordnet nach der Häufigkeit ihrer Präsenz an anderen IXPs und Rechenzentren (Fac)

3.5.4 Mögliche Ausfallszenarien

Typ	Szenario	Verwandt	Betroffen	Behebung	Dauer	Reichweite
BGP-Hijacking	Peering LAN Blackhole über manipulierte BGP Communitiy	—	Kontrollschicht	Intern	m	+
BGP-Hijacking	Verkehrsmanipulation über gespoofte BGP Updates	[I75, I74, I73, I72, I71, I70]	Kontrollschicht	Intern	m	+
Denial-of-Service	Terabit-Angriff auf single-homed DE-CIX Kunden	[I83, I87, I81, I79, I80]	Datenschicht	Extern	m	o
Hacking-Angriff	Unkontrolliertes Verkehrsfiltern nach Übernahme des SDN Controllers	—	Kontrollschicht	Intern	h	+
Hacking-Angriff	Unbemerkte Kompromittierung des Kundenportals	—	Management	Service	d	+
Kabelschäden	Kabelbrand im Meet-Me-Room von Interxion FRA2	—	Infrastruktur	Service	h	o
Kabelschäden	Ausfall mehrerer Metroverbindungen bei Bauarbeiten	[I47, I45, I43, I42, I40]	Infrastruktur	Extern	h	+
Menschlicher Fehler	Netzausfall durch fehlkonfigurierten VLAN-Trunk	—	Management	Intern	m	o
Menschlicher Fehler	Isolation des Route Servers durch fehlerhafte Filter-Policies	[I13]	Kontrollschicht	Intern	m	+
Peering Dispute	Erzwungene Teilnahme der DTAG am Public Peering	[I55, I56, I53, I48]	Kontrollschicht	Intern	m	o
Route Leak	Re-Announcement eines full-table Leaks durch den Route Server	[I69, I68, I65, I66, I61]	Kontrollschicht	Intern	m	+
Route Leak	Weltweites more-specific Announcement des Peering LANs	[I57]	Kontrollschicht	Intern	m	+
Software-Fehler	Wiederkehrende Reboots aller 7950 XRS Line-Cards	[I38]	Datenschicht	Hersteller	d	+
Software-Fehler	Verbindungsausfälle durch fehlerhaften ARP Proxy	—	Kontrollschicht	Intern	m	+
Software-Fehler	Überlastung der Route Server nach Konfigurations-Update	[I37, I36, I27, I24]	Kontrollschicht	Intern	m	o
Staatliche Aktion	Zensurversuch durch Deaggregation europäischer Netze	—	Kontrollschicht	Extern	∞	o
Staatliche Aktion	Totalausfall nach missglückter G10-Maßnahme	[I103]	Management	Intern	m	+
Technischer Defekt	Anhaltender Stromausfall im Stadtteil Ostend	[I11, I10, I8, I5, I2]	Infrastruktur	Service	d	+

3.5.5 Detailanalysen

Peering LAN Blackhole über manipulierte BGP Communitiy
BGP-Hijacking

Beschreibung Ein Angreifer manipuliert die Announcements des DE-CIX Peering LANs mit dem Zusatz der BLACKHOLE BGP Community (65535:666). Empfänger, bei welchen Remotely Triggered Blackholing [52] aktiviert ist, leiten daraufhin Pakete für das Peering LAN auf ein Totinterface und verwerfen so den Verkehr. Die Kommunikation im DE-CIX Peering LAN wird hierdurch zu etwa 90% unterbunden [53]. Fast alle BGP Sessions terminieren und das öffentliche Peering kommt zum Erliegen.

Betroffener Bereich (Kontrollschicht) Durch die missbräuchliche Signalisierung von DDoS Schutzanforderungen im BGP wird die Kontrollschicht am DE-CIX außer Funktion gesetzt. Dabei kann die Manipulation sowohl auf der Ebene von BGP Nachrichten (etwa über den Route Server), als auch durch ein Einspielen gefälschter L2-Pakete erfolgen.

Auswirkung und Reichweite (+) Mit dem Peering kommt auch der öffentliche Datenaustausch am IXP zum Erliegen.

Dauer (m) Der DE-CIX kann den Angriff durch Filterkonfigurationen unmittelbar abwenden.

Fehlerbehebung (Intern) BGP Filter können im Route Server einen entsprechenden Mißbrauch in der Standardkonfiguration verhindern. Paketinjektionen auf der Link Schicht können durch SDN-Regeln (aufwändig) gefiltert werden. Einfacher ist es, den Urheber der Manipulation auszuschliessen, welcher auf der Link-Schicht leicht identifiziert werden kann.

Verkehrsmanipulation über gespoofte BGP Updates
BGP-Hijacking

Beschreibung Ein Teilnehmer des öffentlichen Peerings am DE-CIX manipuliert BGP Announcements mithilfe von Leaking, Pfadverkürzungen oder Präfix Hijacking, um den Datenverkehr für ausgewählte Ziel-Präfixe anzuziehen. Dabei macht er sich die Reflektoreigenschaft des Route-Servers zunutze, um seinen Wirkungsgrad zu erhöhen.

Die fälschlich angeworbenen Daten werden entweder direkt verworfen (Blackholing Attack), abgefangen bzw. manipuliert (Interception Attack) oder deren Zustellung wird durch nicht ausreichende Transitkapazitäten stark verzögert. Letzteres führt zu einer deutlichen Verschlechterung der Dienstqualität für die betroffenen Präfixe.

Betroffener Bereich (Kontrollschicht) Der Angriff führt zu einer (beabsichtigten) Änderung der Topologie im BGP Routing mit nachfolgender Datenumleitung.

Auswirkung und Reichweite (+) Je nach Art und Umfang der Hijacks können wenige bis sehr viele Präfixe von der Umleitung betroffen sein. Da die gefälschten Announcements im kostenfreien Peering geschehen, werden sie i.d.R. bevorzugt akzeptiert.

Dauer (m) Die öffentlichen Wegeinformationen werden am Route-Server zwischen mehreren hundert Providern geteilt, von denen viele als Transitgeber an diversen Orten der Welt peeren. Diese breiter aufgestellten Provider haben so die Möglichkeit, Konsi-

stenzprüfungen für die empfangenen Updates durchzuführen. Zusätzlich haben viele Provider umfangreiche Topologie- und Betriebserfahrung sowie heuristische Testwerkzeuge für Plausibilitätschecks. Deshalb werden irreguläre Announcements im öffentlichen Peering gewöhnlich schnell bemerkt und können mit einfachen Filterregeln blockiert werden.

Fehlerbehebung (Intern) Der DE-CIX kann geeignete Filterregeln auf dem Route Server installieren.

Terabit-Angriff auf single-homed DE-CIX Kunden
Denial-of-Service

Beschreibung Eine sehr große DDoS Attacke richtet sich gegen einen Kunden des DE-CIX, der durch ein einzelnes Interface mit der Switch-Plattform verbunden ist. Der zugehörige Link ist sofort so überlastet, dass die bestehende BGP-Session funktionsgestört wird oder vollständig zusammenbricht.

Betroffener Bereich (Datenschicht) Der Datenlink des Opfers wird weitgehend außer Funktion gesetzt. Die DE-CIX Switch-Infrastruktur wird teilweise bis an ihre Grenzen ausgelastet.

Auswirkung und Reichweite (o) Primär von der Attacke betroffen ist die Anbindung des Opfers an den DE-CIX. Der Terabit-Angriffsverkehr traversiert allerdings die DE-CIX Switch-Plattform und belastet – je nach Datenweg – Backplanes und Inter-connects der Switches. Sollten unbalancierte Switch-Bereiche betroffen sein, also Datenübergänge, welche die Gesamtkapazität aller Switch-Ports unter Vollast nicht gleichzeitig bedienen können, so sind Kollateralschäden in Gestalt von Paketverlusten auf der Switch-Plattform wahrscheinlich.

Dauer (m) Der Angriff kann in kurzer Zeit über Mitigationsdienstleister wirksam gedrosselt werden (vgl. [I80]).

Fehlerbehebung (Extern) Durch einen Mitigationsdienstleister kann der Angriffsverkehr abgeleitet und damit von der DE-CIX Infrastruktur verdrängt werden, wobei ein solcher Dienstleister kostenpflichtig durch den betroffenen DE-CIX Kunden beauftragt werden muss. Ein solcher Schutz kann also erhebliche Kosten nach sich ziehen.

Der IXP-interne Mechanismus des Remotely Triggered Blackholing [52] würde bei umfassender Aktivierung die Einleitung des Angriffsverkehrs verhindern. Der Mechanismus erfordert aber eine intakte BGP Signalisierung und wirkt in seinem gegenwärtigen Implementierungsstand nicht vollständig [53].

Unkontrolliertes Verkehrsfiltern nach Übernahme des SDN Controllers
Hacking-Angriff

Beschreibung Software-defined Networking (SDN) wird am DE-CIX eingesetzt, um Pfadmanagement, Load-Balancing und DDoS Mitigation [54, 55] auf der Schicht 2 zu betreiben. Hierbei wählt ein zentraler Controller auf der Basis der lokalen Anschlusskonfigurationen sowie der dynamischen BGP Routing-Informationen Datenweiterleitungspfade in der DE-CIX Switch-Plattform aus und implementiert diese in die TCAMs (Ternary Content-Addressable Memory) der Switches. TCAMs sind zwar schnell, aber teuer. Die

Kommunikation zwischen Switches und Controller erfolgt über Standardprotokolle wie OpenFlow.

Der zentrale SDN Controller ist ein Rechner mit gängigem Betriebssystem, auf dem die SDN Kontroll-Software abläuft. Teil des Controllers ist zusätzliche Anwendungslogik – etwa zur Auswertung der BGP Announcements, zur Laststeuerung und zum Blackholing. Ein Angreifer, der die Kontrolle über den SDN Controller erlangt hat, kann die Datenpfade in der Plattform derart manipulieren, dass Pakete (i) an falsche DE-CIX Peers weitergeleitet werden oder (ii) ungewollt verworfen werden. Dies kann zu Datenumleitungen, verwirrendem Verhalten wie z.B. die Störung einzelner BGP-Sessions oder auch zu weitreichenden Ausfällen führen.

Die Möglichkeiten der Verkehrsstörung und -manipulation sind hierbei äußerst vielfältig, da SDN eine flexible Datenflusssteuerung erlaubt. Ein Angreifer könnte so z.B. Flüsse ausgewählter Quellen ("alle HTTP-Pakete aus dem Präfix der Hessischen Zentrale für Datenverarbeitung") herausfiltern und auf das Tot-Interface am DE-CIX leiten. In der Folge würden alle eGovernment-Dienste für diejenigen unerreichbar, welche über den DE-CIX vermittelt werden. Die Hessische Zentrale für Datenverarbeitung bliebe aber weiterhin sichtbar auch über den DE-CIX mit dem Netz verbunden. Entsprechende Fehlersuchen durch Standardwerkzeuge wie `ping` und `traceroute` blieben erfolglos. Der Fehler wäre nicht einfach zu finden.

DoS-Angriffe auf DE-CIX Teilnehmer werden durch Verkehrsumleitungen einfach möglich, ohne dass der Angreifer selbst über DDoS-fähige Infrastruktur verfügt. Es genügt, ausgewählte Dienste ("alle Videoströme von Netflix") auf die Interfaces der Opfer zu leiten. Ein erfolgreicher Eindringling in den SDN Controller ist insofern ermächtigt, sehr effektreiche Manipulationen bei der Paketweiterleitung zu veranlassen. Allerdings bliebe eine solche Aktion wohl nur wenige Minuten unbemerkt.

Manipulationsmöglichkeiten werden reichhaltiger für solche Angreifer, die direkt am DE-CIX peeren. Einen einfachen Fall bildet das unbemerkte Datenabhören, denn Pakete können mithilfe von SDN Flowprogrammierungen auf mehrere Switch-Ports geleitet und somit gezielt herausgespiegelt werden. Ausreichende eigene Interface-Kapazitäten vorausgesetzt, könnte ein Angreifer so umfangreichen Datenverkehr am DE-CIX zusätzlich auf seine eigene Infrastruktur leiten und offline analysieren. Crypto-Attacken auf verschlüsselten Datenverkehr werden so ebenfalls unbemerkt möglich.

Weitere Angriffe auf spezielle Anwendungsprotokolle wie SMTP (Email) oder das Domain Name System (DNS) könnten leicht realisiert werden. So könnte ein Angreifer, der auch über einen Zugang zur DE-CIX Plattform verfügt, DNS-Anfragen zu sich umleiten und in der eigenen DNS Infrastruktur gezielte Falschantworten verbreiten. Konkreter könnte ein solcher böswilliger Provider Anfragen an offizielle Stellen des Bundes und der Länder, etwa zu aktuellen Corona-Regeln, auf gefälschte Informationsseiten von Verschwörungsgruppen leiten. Die Voraussetzungen hierfür aber, nämlich mit eigener Infrastruktur am DE-CIX präsent und erfolgreich in das Management eingedrungen zu sein, sind vergleichsweise hoch für die überschaubare Wirkung der (zeitlich eng begrenzte) Aktion.

Die Kommunikation zwischen dem Controller und den Switches verläuft über die Management-Schnittstellen der Switches, also out-of-band. Ein erfolgreicher Angreifer des SDN Controllers muss deshalb zunächst in das Management-Netz des DE-CIX eingedrun-

gen sein. Dortselbst kann der Angreifer alle Geräte auf der Management-Ebene auch direkt angreifen, so dass der SDN Controller nur als ein mögliches Ziel im Management-Netz zu sehen ist.

Es kann davon ausgegangen werden, dass das Management-Netz des DE-CIX gut geschützt ist und ein Überwinden der Eintrittsbarrieren von außen sehr schwierig ist. Insofern muss ein erfolgreicher Angriff auf den SDN Controller als äußerst unwahrscheinlich eingestuft werden.

Betroffener Bereich (Kontrollschicht) Mit der im SDN programmierbaren Kontrollschicht der Switch-Plattform ist ein sehr grundlegender Mechanismus betroffen, der die Datenkommunikation aller höheren Schichten beeinträchtigen kann. Ein erfolgreicher Angreifer kann die Datenweiterleitung auf der DE-CIX Plattform umfassend manipulieren. Gleichzeitig betroffen ist die (abgeschottete) Management-Infrastruktur des DE-CIX.

Auswirkung und Reichweite (+) Der Angriff bleibt technisch auf die SDN-Domaine am DE-CIX beschränkt, wobei größere Störungen leichter identifizierbar sind als subtile Modifikationen. Gelingt es dem Angreifer, das Peering am DE-CIX gezielt zu beeinträchtigen, wirkt sich dieses auch auf das BGP Routing über den DE-CIX hinaus aus.

Dauer (h) Der Angriff sollte vom Intrusion Detection System (IDS) des Management-Netzes entdeckt werden, bevor eine Manipulation des SDN Controllers vorgenommen werden kann. Sollte dem Angreifer ein unbemerktes Eindringen in die Management-Infrastruktur des DE-CIX gelingen, sind die Fehler je nach Angreiferverhalten unter Umständen schwer erkennbar, etwa wenn dem Controler vom IDS unbemerkt vereinzelt falsche Datenpfade untergeschoben werden. Die Wiedererlangung der Kontrolle über das System und dessen Absicherung kann einige Stunden dauern. Ein ggfs. vorbereitete Rückfallposition kann die Basisfunktionen der Switch-Plattform auch schneller wiederherstellen.

Fehlerbehebung (Intern) Der SDN Controller ist unter der Kontrolle der DE-CIX Betriebsmannschaft. Der DE-CIX kann das System rekonfigurieren und neu aufsetzen, was je nach Vorbereitungsstand unterschiedlich aufwändig ist.

Unbemerkte Kompromittierung des Kundenportals
Hacking-Angriff

Beschreibung Ein unerkannter Hacker nutzt die Schwachstelle eines Web-Frameworks aus und erlangt uneingeschränkten Zugriff zum DE-CIX Kundenportal. Hierdurch gelingt es ihm, kundenspezifische Konfigurationen auszuspähen sowie Filterregeln gem. Internet Routing Registry (IRR) und Route Origin Validation (ROV) zu manipulieren.

Betroffener Bereich (Management) Betroffen ist das Management der Kontrollschicht.

Auswirkung und Reichweite (+) Kundenspezifische Anschlussdaten können ausgespäht und ggfs. zu deren Nachteil verwendet werden. Ausgewählte, i.d.R. nicht funktionskritische Konfigurationen der Kunden am Route Server können manipuliert werden.

Dauer (d) Bei nicht ausreichender Systemüberwachung bleibt die Kompromittierung für einige Zeit unbemerkt.

Fehlerbehebung (Service) Der Systemdienstleister des DE-CIX ist für die Reparatur

und Integritätswiederherstellung des Portalsystems zuständig.

Kabelbrand im Meet-Me-Room von Interxion FRA2
Kabelschäden

Beschreibung Durch einen technischen Defekt gerät ein Kabelschacht in Flammen und die darin verlegten Kabel werden unbrauchbar. Angesiedelt im Meet-Me-Room, dienen diese Kabel insbesondere direkten Verbindungen zwischen den lokal präsenten Providern, um große Datenmengen bilateral auszutauschen. Gemäß DE-CIX Mitgliederinventar sind am Standort Interxion FRA2 viele große Provider und CDNs an die Plattform angeschlossen (u.a. DTAG, Vodafone, Telefonica, Amazon), wobei die Mehrzahl der Teilnehmer Parallelanschlüsse an anderen Interxion-Standorten unterhält.

Betroffener Bereich (Infrastruktur) Kabeltrassen werden zerstört und damit physische Konnektivität unterbunden. Ggfs. treten weitergehende Folgeschäden durch Rauch bzw. Brandlöschung auf.

Auswirkung und Reichweite (o) Betroffen sind lediglich lokale Verbindungen, welche wahrscheinlich von anderen PoPs überbrückt werden können: Alle 15 Datenzentren von Interexion in Frankfurt befinden sich auf demselben Campus und sind durch wechselseitige Kabelverbindungen vermascht. Da betroffene Interconnects sehr hohe Datenkapazitäten haben können, sind kurzfristige massive Verkehrsverlagerungen wahrscheinlich.

Dauer (h) Die Beseitigung der direkten Brandschäden und die provisorische Wiederherstellung von (hausinternen) Kabelverbindungen erfordert voraussichtlich wenige Stunden.

Fehlerbehebung (Service) Die Schadensbehebung erfolgt durch den Rechenzentrumsdienstleister Interxion.

Ausfall mehrerer Metroverbindungen bei Bauarbeiten
Kabelschäden

Beschreibung Durch Tiefbauarbeiten in Frankfurt werden mehrere Kabelverbindungen durchtrennt, welche DE-CIX Standorte verbinden. Da die Rechenzentren i.d.R. über getrennte Trassen mehrfach angebunden sind, ist die vollständige Isolation eines Standorts zwar möglich, aber nicht wahrscheinlich. In jedem Fall entsteht durch den Wegfall der Kabelverbindungen ein eventuell erheblicher Kapazitätsverlust.

Betroffener Bereich (Infrastruktur) Der temporäre Verlust von Kabelinfrastruktur führt zum Ausfall mehrerer Links in der DE-CIX Switch-Plattform. Dies bewirkt ggfs. eine Überlastung verbleibender Links und im Extremfall die Isolation einzelner Standorte.

Auswirkung und Reichweite (+) Durch die Kabelausfälle sinkt die Datenaustauschkapazität des DE-CIX. Dies kann im günstigsten Fall von den Reserven aufgefangen werden, in ungünstigen Konstellationen entstehen Stau- und Erreichbarkeitsprobleme, die durch Korrekturen im Routing und Traffic Engineering ausgeglichen werden müssten.

Dauer (h) Die Reparatur von durchtrennten Glasfasern kann innerhalb eines Tages erfolgen.

Fehlerbehebung (Extern) Die Kabelreparatur wird von den Kabelbetreibern verant-

wortet.

Netzausfall durch fehlkonfigurierten VLAN-Trunk
Menschlicher Fehler

Beschreibung Eine oder mehrere Switch-Verbindung(en) werden im Rahmen eines Konfigurations-Updates nicht mehr als IEEE 802.1Q VLAN Trunk konfiguriert, sondern einem individuellen VLAN zugeordnet. Daraufhin bricht alle Kommunikation zwischen den Switches, die nicht in dem irrtümlich konfigurierten VLAN verläuft, ab.

Betroffener Bereich (Management) Der Fehler auf der Management-Schicht bedingt den Ausfall der Daten- und Kontrollschicht an den betroffenen Übergängen. Je nach betroffener Switch-Verbindung können dabei wenige bis sehr viele Peering-Sessions mit den Route-Servern betroffen sein, so dass das öffentliche Peering geringfügig bis stark beeinträchtigt wird.

Auswirkung und Reichweite (o) Die Wirkung des Konfigurationsfehlers hängt von dem speziell fehlkonfigurierten VLAN ab, betrifft aber in der Regel nur einen Teil des Datenverkehrs.

Dauer (m) Kompetentes Betriebspersonal kann unter Verwendung geeigneter Managementwerkzeuge solche Fehler in sehr kurzer Zeit erkennen und beheben.

Fehlerbehebung (Intern) Die VLAN-Konfiguration der Switches ist unter der Kontrolle der DE-CIX Betriebsmannschaft. Der DE-CIX betreibt ein separates Management-Netz, über welches die Betreiber jederzeit Konfigurations-Updates vornehmen können.

Isolation des Route Servers durch fehlerhafte Filter-Policies
Menschlicher Fehler

Beschreibung Eine Fehlkonfiguration der Firewall-Regeln (z.B. fehlende Zugriffserlaubnis aus dem Peering-LAN) isoliert den Route Server mit der Folge, dass BGP Peering-Sessions unterbunden werden und so das öffentliche Peering außer Funktion gesetzt wird. In der Folge werden alle im öffentlichen Peering erlernten Routen verworfen und der öffentliche Datenaustausch über den DE-CIX kommt zum Erliegen.

Betroffener Bereich (Kontrollschicht) Betroffen ist der öffentliche Austausch von BGP Kontrollinformationen. Private Peerings und der dazugehörige Datenaustausch sind nicht beeinträchtigt.

Auswirkung und Reichweite (+) Der Wegfall aller öffentlichen Peering-Sessions beendet den öffentlichen Datenaustausch am DE-CIX.

Dauer (m) Der eher grobe Fehler kann leicht erkannt und isoliert werden, so dass eine sehr zügige Behebung zu erwarten ist.

Fehlerbehebung (Intern) Die interne Firewall kann vom DE-CIX Betriebsteam unmittelbar rekonfiguriert werden.

Erzwungene Teilnahme der DTAG am Public Peering
Peering Dispute

Beschreibung Nach multilateralen Spannungen und gescheiterten Verhandlungen ent-

scheiden mehrere Content-Provider, das bilaterale Peering mit der DTAG einzustellen (Disput z.B. über Paid Peering). Hierdurch sind die 'Hypergiants' für DTAG nurmehr über andere Tier1-Provider erreichbar, und es kommt zu Verkehrsungleichgewichten zwischen den Transitprovidern, was zu weiteren Spannungen und einer Service-Verschlechterung der DTAG-Kunden führt. Als kurzfristige Gegenmaßnahme beschließt die Deutsche Telekom, am DE-CIX öffentlich zu peeren und so den Verkehr der Content-Provider lokal zu empfangen. Plötzliche, massive Verkehrsströme werden daraufhin auf die DE-CIX Plattform verlagert, worauf diese nicht vorbereitet ist.

Betroffener Bereich (Kontrollschicht) Der plötzlichen Änderung des Routing-Verhaltens folgen Datenströme im Tbps-Bereich, welche die Reserven der DE-CIX Plattform übersteigen und zu anhaltenden Verkehrsstaus auf dem IXP führen.

Auswirkung und Reichweite (o) Eine plötzliche massive Verkehrsexplosion am DE-CIX ist potentiell geeignet, die Leistungsfähigkeit des IXPs drastisch einzuschränken. Allerdings ist dieses Szenario sehr unwahrscheinlich: Gemäß PeeringDB ist die DTAG gegenwärtig mit einem 20 Gbps Interface am DE-CIX angeschlossen. Um signifikanten CDN-Datenverkehr über ein Public Peering abzuwickeln, müsste die DTAG zunächst ihre Zugangskapazitäten vervielfachen. Im Zuge dessen würde sie ihr Vorhaben mit dem DE-CIX abstimmen, so dass Vorsorge für die Kapazitätsveränderungen getroffen werden könnte.

Dauer (m) Der DE-CIX kann sofort lastausgleichende Konfigurationen auf seiner Plattform vornehmen.

Fehlerbehebung (Intern) Der DE-CIX kann Lastprobleme unmittelbar mittels Durchsatzbeschränkungen (Rate Limiting) an den verursachenden Interfaces beheben. Es ist weiterhin davon auszugehen, dass im direkten Kundendialog kurzfristig gemeinsam Lösungswege ausgehandelt werden.

Re-Announcement eines full-table Leaks durch den Route Server
Route Leak

Beschreibung Ein Teilnehmer des Public Peerings am DE-CIX Route Server propagiert seine vollständige Routing-Tabelle (full-table Leak), welche der Route Server ungefiltert weiterverteilt. Hierdurch signalisiert der Urheber an alle anderen Teilnehmer des öffentlichen Peerings, dass er kostenlosen Datentransfer in das gesamte Internet anbietet. Üblichen Peering-Policies folgend, senden die anderen DE-CIX Teilnehmer daraufhin ihre Daten an diesen kostenlosen Upstream und verstopfen so sehr schnell den Link zum Verursacher. Ein Blockade entsteht auf der DE-CIX Plattform.

Betroffener Bereich (Kontrollschicht) Infolge der fehlerhaften Weiterleitung des Route Leaks kommt es zu einer weitreichenden Rekonfiguration der Routing-Topologie im BGP.

Auswirkung und Reichweite (+) Die veränderten Routing-Informationen bewirken einen unmittelbaren, massiven Schwenk der Datentransfers hin zu dem verursachenden AS, welches zu regionalen Dienstbeinträchtigungen im Internet führt.

Dauer (m) Das Fehlerverhalten kann sehr schnell durch ein De-Peering des Verursachers abgestellt und dauerhaft durch das Einsetzen aktueller Filterlisten verhindert

werden.

Fehlerbehebung (Intern) Die BGP Route Server und ihre Konfigurationen sind unter der Kontrolle der DE-CIX Betriebsmannschaft.

Weltweites more-specific Announcement des Peering LANs
Route Leak

Beschreibung Die Teilnehmer am DE-CIX sind über eine Layer-2-transparente Switch-Infrastruktur verbunden, über die ein gemeinsames IP-Subnetz gespannt ist: Das Peering LAN. Das Prefix des Peering LANs muss zwischen den am DE-CIX teilnehmenden Routern nicht im BGP announciert werden, da es bereits auf den lokalen Interfaces konfiguriert ist. Announciert ein Peer dieses Netz dennoch mit korrekter Netzgröße im BGP Routing, wird es global erreichbar, aber die lokale Teilnahme bleibt hiervon ungestört.

Aufgrund der wachsenden Teilnehmerzahlen hat der DE-CIX die Größe dieses IP-Netzes im Mai 2018 auf /21 erweitert, so dass 1022 Router am DE-CIX peeren können. Netze dieser Größe können in kleinere Subnetze deaggregiert werden, denn im BGP-Routing werden üblicherweise Announcements bis zu einer Präfix-Länge von 24 bit (/24) akzeptiert.

Deaggregiert nun ein BGP Peer dieses Präfix des DE-CIX Peering LANs und signalisiert ein spezifischeres Announcement global im BGP-Routing, so empfangen auch die DE-CIX Teilnehmer diese Announcements. Sie lenken ihren Datenverkehr auf den Versender dieser genaueren ('more-specific') Routen, wodurch die bisherigen Peering-Partner – mit Ausnahme des fehlannouncierenden Autonomen Systems – in diesem Netz nicht mehr erreicht werden.

Ein solcher Vorfall hat sich 2019 am AMS-IX [I57] ereignet, verursacht durch den Tier1 Provider Telia. In der Folge akzeptierten die Empfänger die genauereren Routen und leiteten ihren Verkehr vom Peering LAN zu Telia um, wodurch bestehende (single-hop) BGP-Sessions beendet wurden. Danach konnten die AMS-IX Teilnehmer das interne Peering am IXP nicht mehr aufrecht erhalten.

Ohne Gegenmaßnahmen kommt in einem solchen Fall das öffentliche Peering am DE-CIX zum Erliegen. Allerdings werden solche Fehler i.d.R. sehr schnell bemerkt. Insbesondere ist es eher ausgeschlossen, dass ein Provider ein solches Verhalten absichtlich und wiederholt provoziert, da er im Wiederholungsfall sehr schnell vom Peering am DE-CIX ausgeschlossen würde.

Betroffener Bereich (Kontrollschicht) Fehlerhafte Topologieinformationen auf der Kontrollschicht führen dazu, dass Nachbarschaften im Peering-LAN aus dem Routing verschwinden.

Auswirkung und Reichweite (+) Mit dem Zusammenbruch des öffentlichen Peerings wird auch der öffentliche Datenaustausch am DE-CIX ausgesetzt. Da ein erheblicher Umfang des lokalen Internet-Verkehrs über IXPs geroutet werden, insbesondere zwischen Providern und Content-Netzwerken, könnte es zu Verzögerungen oder Paketverlusten bei der Datenzustellung kommen. Endnutzer, die Videos oder Musik streamen, sich größere Software-Updates herunterladen etc. wären vor allem betroffen.

Dauer (m) Es können unmittelbar eigene deaggregierte Announcements aktiviert

werden.

Fehlerbehebung (Intern) Der DE-CIX kann zunächst sein eigenes Präfix ebenfalls feingranular announcieren. Diese *More Specifics* würden von den Peers bevorzugt werden. Weiterhin können Konfigurationsfehler bei Peering-Partnern durch bilaterale Hinweise bereinigt werden.

Wiederkehrende Reboots aller 7950 XRS Line-Cards
Software-Fehler

Beschreibung Der DE-CIX setzt Nokia 7950 Extensible Routing Systems als die Kernvermittlungskomponenten in seiner Datenaustauschplattform ein. Die Geräte stellen eine sehr hohe Dichte an 100 Gbps und 400 Gbps Interfaces bereit. Diese Interface-Cards arbeiten flussbasiert und es ist denkbar, dass sie durch einen technischen Defekt in Software (und Hardware) im laufenden Betrieb plötzlich instabil werden – z.B. wenn eine kritische Zahl an Datenflüssen überschritten wird. Ein verwandter, weitreichender Fehler trat 2014 in BGP Routing-Tabellen des Herstellers Cisco auf [I38].

Ein häufiges Rebooten der Line-Cards kann den Betrieb am DE-CIX nachhaltig stören. Die Wirkung am DE-CIX wird durch die sehr homogene Plattform-Architektur verstärkt, und es ist schwierig, die auslösende Ursache auch nur zu erkennen. Solange aber kein Ursachenverständnis vorliegt (die 'überlaufende Flow Table') sind schnelle, schadensbegrenzende Gegenmaßnahmen schwer möglich und es muss auf eine Behebung durch den Hersteller gewartet werden. Während der Reparaturzeit kann ggfs. durch Umkonfiguration und direkte Verknüpfung der Edge-Geräte ein Notbetrieb unter deutlichen Leistungseinbußen realisiert werden.

Betroffener Bereich (Datenschicht) Der Fehler beeinträchtigt direkt den Austausch auf der Datenschicht, wobei die BGP-Kontrollschicht die Datenschicht benötigt und deshalb ebenfalls gestört wird.

Auswirkung und Reichweite (+) Bei schnell wiederkehrenden Neustarts der Schnittstellenkarten ist ein regulärer Betrieb am DE-CIX kaum möglich.

Dauer (d) Angesichts der Schwere des Defekts und des Einsatzfelds der (high-end) Geräte kann mit einer priorisierten Fehlerbehebung durch den Hersteller binnen Tagen gerechnet werden. Sollten auch Hardware-Fehler die Ursache sein, kann ggfs. mit der Bereitstellung von Ersatzsystemen (gem. SLAs) gerechnet werden.

Fehlerbehebung (Hersteller) Die Lieferung von fehlerbereinigter Firmware muss durch den Hersteller erfolgen.

Verbindungsausfälle durch fehlerhaften ARP Proxy
Software-Fehler

Beschreibung Proxy ARP [56] wird von der DE-CIX Plattform verwendet, um einen transparenten Kommunikationszugriff auf Schicht 2 zwischen den Standorten zu ermöglichen und gleichzeitig die ARP Broadcast-Last zu beschränken. Fällt der ARP Proxy durch Konfigurationsfehler oder fehlerhafte Updates aus, können MAC-Adressen von Rechnern der anderen Standorte nicht mehr ermittelt werden.

Betroffener Bereich (Kontrollschicht) Ein Ausfall der ARP-Auflösung verhindert neue Kommunikationsverbindungen, deren Adressen nicht im jeweiligen ARP Cache sind. Damit fällt die Kontrollschicht vollständig aus und in der Folge auch die Datenschicht.

Auswirkung und Reichweite (+) Die starke Verteilung des DE-CIX lässt erwarten, dass die Mehrheit der Teilnehmer sich paarweise nicht mehr ansprechen können.

Dauer (m) Sowohl ein Rekonfigurieren wie Aktualisieren der Software, als auch die Aktivierung von ARP-Forwarding können im Bereich von Minuten durchgeführt werden.

Fehlerbehebung (Intern) Der ARP Proxy kann i.d.R. einfach rekonfiguriert bzw. aktualisiert werden. Darüber hinaus besteht auch die Möglichkeit, zwischen den Standorten ein ARP-Forwarding zu aktivieren. Hierdurch werden ARP-Anfragen ebenfalls beantwortet, wenn auch langsamer und unter schlechterer Skalierbarkeit.

Überlastung der Route Server nach Konfigurations-Update
Software-Fehler

Beschreibung Im Rahmen eines regulären Konfigurations-Updates an den DE-CIX Route Servern wird irrtümlich eine Verarbeitungslogik (z.B. beim Prozessieren von Policies) aktiviert, welche die BGP Best Path Selection so häufig anstößt, dass die Maschinen dies im Rahmen der regulären BGP Announcements nicht mehr verarbeiten können. Der BGP Auswahlprozess kann nicht mehr zeitgerecht konvergieren. Hierdurch werden Route-Updates nicht mehr rechtzeitig verarbeitet und z.T. verworfen. Die Route Server übermitteln dementsprechend veraltete und unvollständige Topologieinformationen.

Betroffener Bereich (Kontrollschicht) Das öffentliche Peering am DE-CIX wird in seiner Funktion teilweise beeinträchtigt.

Auswirkung und Reichweite (o) Die zu erwartenden Folgen des Fehlers sollten gering und lokal beschränkt bleiben, zumal der Fehlerzustand einfach identifizierbar ist. Es ist wahrscheinlich, dass nur einzelne Routen kurzzeitig unterdrückt werden. Die absehbar größte Auswirkung entstünde, wenn die Überlast der Maschine zu TCP-Timeouts und damit zum Abbruch der BGP-Sessions führen würde.

Dauer (m) Fehlerhafte Konfigurationen des BIRD Route Servers können innerhalb von Minuten zurückgerollt werden.

Fehlerbehebung (Intern) Die BGP Route Server und ihre Konfigurationen sind unter der Kontrolle der DE-CIX Betriebsmannschaft.

Zensurversuch durch Deaggregation europäischer Netze
Staatliche Aktion

Beschreibung Um den Zugriff auf ausgewählte, entfernte europäische Netze einzuschränken bzw. zu verhindern, wird staatlich angeordnet, die betroffenen Prefixe so kleinzellig (≥ 25) zu announcieren, dass diese gemäß gängigen BGP-Filtern nicht weitergeleitet werden. Hierdurch werden diese IP-Adressbereiche für weite Bereiche des Internets unerreichbar. Wird die Deaggregation im öffentlichen Peering des DE-CIX angeordnet, sind viele regionale Übergänge betroffen.

Betroffener Bereich (Kontrollschicht) Hier werden Konventionen der Kontrollschicht

ausgenutzt, um die Funktionsfähigkeit derselben einzuschränken.

Auswirkung und Reichweite (o) Die Wirksamkeit der Maßnahme wird durch die Zahl und Relevanz der zensierten Präfixe definiert sowie durch mögliche Gegenreaktionen der regionalen Provider.

Dauer (∞) Die staatliche angeordnete Maßnahme hat solange Bestand, wie Exekutive, Judikative oder Legislative nicht dagegen einschreiten.

Fehlerbehebung (Extern) Das Abstellen der Maßnahme bedingt politische bzw. juristische Entscheidungsfindungen. Lokale Provider können allerdings ihre BGP Filterregeln anpassen, um der Zensur auszuweichen.

Totalausfall nach missglückter G10-Maßnahme
Staatliche Aktion

Beschreibung Auf der Basis von Artikel 10 GG initiieren Verfassungsschutzbehörden die Aufzeichnung des Internet-Verkehrs am DE-CIX. Durch Konfigurationsfehler (Netconf, SDN) oder Überlastung der Switches kommt es zu Fehlfunktionen, in deren Folge die reguläre Paketweiterleitung zugunsten der Ausleitung eingestellt wird.

Betroffener Bereich (Management) Der Fehler betrifft die Konfigurationen der Switch-Infrastrukutur bzw. ihre Wirkung unter Überlast.

Auswirkung und Reichweite (+) Als Folge der Maßnahme fällt die Datenschicht der Plattform ganz oder weitgehend aus. Der IXP wird funktionslos.

Dauer (m) Der Fehler wird i.d.R. sofort entdeckt. Seine Behebung kann aber mit den Zielen der G10 Maßnahme kollidieren, indem diese zu Datenverlusten der Überwachungsmaßnahme führen.

Fehlerbehebung (Intern) Der DE-CIX kann Konfigurationsfehler selbsttägig beheben. Im Falle von Leistungsbeschränkungen müssen die Zielkonflikte im Dialog mit den Behörden aufgelöst werden.

Anhaltender Stromausfall im Stadtteil Ostend
Technischer Defekt

Beschreibung Im Frankfurter Stadteil Ostend befindet sich nicht nur der Hauptsitz vom DE-CIX, sondern auch die (mehrheitlich genutzten) Rechenzentren von Interxion (FRA1–FRA15) sowie das NTT Datacenter Frankfurt 2 (e-shelter). Ein vollständiger Stromausfall in den Rechenzentren würde große Teile der DE-CIX Plattform außer Betrieb setzen (vgl. auch [I5]).

Neben redundater Stromversorgung verfügen die Rechenzentren typischerweise über eine Batteriepufferung von ca. 15 min. und Notstromversorgungen (Dieselaggregate) vorgetankt für 1–3 Tagen. Vertraglich garantieren sie Verfügbarkeiten um 99,99, wobei technische Fehlerketten wie bei Interxion 2018 [I5] dem entgegenstehen.

Im Fall eines Stromnetzausfalls sollten – überbrückt durch USVs – die Notstromaggregate anspringen und unterbrechungsfrei Strom weiterliefern. Auch bei anhaltendem Stromausfall können diese nachgetankt und prinzipiell auch wochenlang ohne Unterbrechung betrieben werden. Gelingt dies jedoch nicht, weil z.B. Wartungsarbeiten nicht sorg-

fältig ausgeführt worden sind, fällt die DE-CIX Infrastruktur regional solange aus, bis die Stromversorgung wiederhergestellt ist.

Betroffener Bereich (Infrastruktur) Die durch Stromverlust ausfallenden Komponenten bewirken den Ausfall der Kontroll-, Daten- und der Managementschicht an den betroffenen Standorten.

Auswirkung und Reichweite (+) Der Ausfall führt zu einem Verbindungsverlust aller regional in Ostend angeschlossenen Teilnehmer. Soweit sich ein oder mehrere der drei Route Server des DE-CIX in den betroffenen Rechenzentren befinden, führt deren Ausfall zum (Teil-)verlust der öffentlichen Peering-Sessions.

Dauer (d) Notreparaturen an Stromleitungen und -trassen sind i.d.R. innerhalb weniger Tage abgeschlossen.

Fehlerbehebung (Service) Die Reparatur von Versorgungskomponenten erfordert externe Dienstleister; die Wiederherstellung der städtischen Stromversorgung muß über die lokalen Netzbetreiber erfolgen.

3.6 Zusammenfassung und abschließende Bewertung

Zum Abschluss dieses Kapitels fassen wir die vier fiktiven Ausfallszenarien in technischen Übersichtseiten zusammen und geben damit einen Vergleich über die verschiedenen Störungseigenschaften. Die möglichen Ursachen für den jeweiligen Ausfall sind nach Risiken (○: gering, ◐: mittel, ● : hoch) und Dauer (m: Minuten, h: Stunden, d: Tage, ∞: mehr als Tage) bewertet. Wir unterscheiden zudem zwischen den betroffenen Schichten (physikalisch, Netzwerk, Anwendungen) und der Reichtweite (lokal, regional, global).

Darüber hinaus geben wir eine vergleichende Bewertung der Relevanz und der Wirkungsreichweite dieser betrachteten Ausfallszenarien am Ende des Kapitels.

3.6.1 Technische Übersicht: Ausfall eines Überseekabels

Allgemeines

Name: **Ausfall Überseekabel TAT-14**

Eintrittsrisiko: Niedrig | **Mittel** | Hoch

Verletzungen am Landungspunkt können trotz Redundanzplanungen zu Ausfällen führen.

Beziehung zu realen Vorfällen: **ja** | nein

Zwei Kabelbrüche Ende 2003. Im Rahmen der Snowden-Affäre wurde 2013 bekannt, dass der britische Geheimdienst GCHQ das Kabel abhört.

Auswirkungen

Betroffene Schichten: **Physikalisch** | Netzwerk | Anwendungen

Betroffene Anwender: Kunden von Tier 1 und großen ISPs, die interkontinentale Internet-Dienste anbieten oder nutzen.

Reichweite: lokal | regional | **global**

Erwartete Dauer: Tage

Eingeschränkte Erreichbarkeit: **ja** | nein

Durch Betroffene mitigierbar: **ja** | nein

Routenänderungen und Backup-Verbindungen erlauben, diese Verbindung zu umgehen.

Ursachen

	Reale Vorfälle	Risiken	Dauer
BGP-Hijacking			
Denial-of-Service	1	○●	m
Hacking-Angriff			
Kabelschäden	7		d
Menschlicher Fehler	3	◐●	m
Peering Dispute	4	○●	∞
Route Leak			
Software-Fehler	2		h
Staatliche Aktion	5	◐●	∞
Technischer Defekt	6	◐●	d

3.6.2 Technische Übersicht: Transitausfall durch ein Land

Allgemeines

Name: **Ausfall aller Transitverbindungen durch Russland**

Eintrittsrisiko: Niedrig | **Mittel** | Hoch

Angriffsvektoren sind vorhanden. Deren Anwedung setzt aber global politische Spannungen voraus.

Beziehung zu realen Vorfällen: ja | nein

Lediglich im Rahmen des Arab Springs bzw. in topologischen Randlagen ist die Internet-Konnektivität ganzer Länder biser weggefallen.

Auswirkungen

Betroffene Schichten: Physikalisch | Netzwerk | Anwendungen

Betroffene Anwender: Vor allem die ehemaliten sowjetischen Republiken Turkmenistan, Usbekistan und Kasachstan, aber auch die Ukraine, Afganistan und die Mongolei.

Reichweite: lokal | regional | global

Erwartete Dauer: unbestimmt

Eingeschränkte Erreichbarkeit: ja | nein

Durch Betroffene mitigierbar: ja | nein

Betroffene können durch Routenänderungen, Aktivierung von Backup-Verbindungen und Aufnahme neuer Transit-Beziehungen Russland umgehen.

Ursachen

	Reale Vorfälle	Risiken	Dauer
BGP-Hijacking	2	◐●	h
Denial-of-Service			
Hacking-Angriff	0		w
Kabelschäden			
Menschlicher Fehler	1		h
Peering Dispute			
Route Leak	0		d
Software-Fehler	1		h
Staatliche Aktion	1		∞
Technischer Defekt	1		h

3.6.3 Technische Übersicht: Ausfall eines DNS-Dienstleisters

Allgemeines

Name: **Angriff auf einen populären DNS-Dienstleister**

Eintrittsrisiko: Niedrig | Mittel | **Hoch**

Es sind aussichtsreiche, mehrschichtige Angriffsvektoren vorhanden.

Beziehung zu realen Vorfällen: **ja** | nein

Es gab staatliche Aktivitäten, DDoS-Angriffe, Hacking, BGP-Hijacking und Software-Fehler, die größere Teile eines Namensraums gestört haben.

Auswirkungen

Betroffene Schichten: Physikalisch | Netzwerk | **Anwendungen**

Betroffene Anwender: Betreiber von Internet-Diensten, welche ihre Dienstnamen bei dem DNS-Registrar gemietet haben und dessen DNS-Infrastruktur nutzen.

Reichweite: lokal | regional | **global**

Erwartete Dauer: Einige Tage

Eingeschränkte Erreichbarkeit: **ja** | nein

Durch Betroffene mitigierbar: **ja** | nein

Betroffene können mehrere authoritative DNS-Server in unterschiedlichen Netzen redundant nutzen.

Ursachen

	Reale Vorfälle	Risiken	Dauer
BGP-Hijacking	2		m
Denial-of-Service	6		h
Hacking-Angriff	2		d
Kabelschäden	6	○●	h
Menschlicher Fehler	3	◐●	h
Peering Dispute			
Route Leak	3	◐●	h
Software-Fehler	2		d
Staatliche Aktion	1		∞
Technischer Defekt	0	○●	h

3.6.4 Technische Übersicht: Ausfall eines Internet-Kotenpunktes

Allgemeines

Name: **Ausfall des DE-CIX Frankfurt**

Eintrittsrisiko: Niedrig | Mittel | Hoch

Die redundante, verteilte Infrastruktur verfügt über keine deutliche, gemeinsame Schwachstelle.

Beziehung zu realen Vorfällen: ja | nein

Es gab an IXPs u.a. Stromausfälle, Brände sowie Software- und Konfigurationsfehler. Der AMS-IX ist am 13.05.2015 weitgehend ausgefallen.

Auswirkungen

Betroffene Schichten: Physikalisch | Netzwerk | Anwendungen

Betroffene Anwender: Nutzer von Diensten der DE-CIX Kunden, die in Frankfurt peeren.

Reichweite: lokal | regional | global

Erwartete Dauer: Einige Stunden

Eingeschränkte Erreichbarkeit: ja | nein

Durch Betroffene mitigierbar: ja | nein

Betroffene können durch Routenänderungen, Aktivierung von Backup-Verbindungen und Aufnahme neuer Peering-Beziehungen den DE-CIX umgehen.

Ursachen

	Reale Vorfälle	Risiken	Dauer
BGP-Hijacking	6	◐●	m
Denial-of-Service	5	◐●	m
Hacking-Angriff	0	○●	h
Kabelschäden	5		h
Menschlicher Fehler	1		m
Peering Dispute	4	◐●	m
Route Leak	6		m
Software-Fehler	5		m
Staatliche Aktion	1	◐●	∞
Technischer Defekt	5		d

3.6.5 Abschließende Bewertung

Unsere fiktiven Ursachenbetrachungen und Analysen lassen sich in folgenden Einschätzungen zusammenfassen:

Ausfall TAT-14 Kabelverbindung

- Globale Auswirkung, insbesondere auf Kapazität und Latenz
- Wenige, aber realistische Ursachen, reale Vorfälle vorhanden
- Behebung der ursächlichen Schäden aufwändig und langsam

Transitausfall durch Russland

- Wirkt sich auf die Erreichbarkeit insbesondere in Zentralasien aus
- Wenige realistische Ursachen, keine vergleichbaren Vorfälle
- Umgehung des Transitausfalls weitgehend und schnell möglich

DoS Angriff auf den DNS-Provider IONOS

- Auswirkung ist global für betroffene Namen, betrifft Erreichbarkeit
- Realistische Verwundbarkeit insbesondere durch entfernte Angriffe, reale Vorfälle vorhanden
- Auch bei sorgfältiger Infrastrukturplanung sind die Auswirkungen nicht immer schnell behebbar

Ausfall des Internet-Knotenpunktes DE-CIX

- Auswirkung ist regional, betrifft Kapazität und Latenz
- Viele realistische Ursachen für Teilausfälle, reale Vorfälle vorhanden
- Meist schnell und vielfältig behebbar

Kapitel 4
Internationale Kabelverbindungen

4.1 Charakterisierung des deutschen Internets

Für die Sicherstellung der internationalen Internet-Konnektivität sind weltweit nahezu 500 Unterseekabel mit etwa 1.350 Anlandungspunkten und zahllose terrestrische Glasfaserstrecken im Einsatz. Die globale Gesamtstrecke aller optischen See-/Landkabel beträgt 2,7 Millionen Kilometer [1]. Abb. 4.1 zeigt einen europäischen Ausschnitt.

Abbildung 4.1: **Europäische Kabelverbindungen**, Quelle: ITU [2]

Die Komplexität dieser Infrastruktur trägt wesentlich zur Robustheit des Internets gegenüber Leitungsausfällen bei, erschwert aber gleichzeitig eine konkrete Bewertung von Optimierungsmöglichkeiten und Ausfallrisiken. Im Folgenden werden daher Abhängigkeiten der deutschen Internet-Infrastruktur von internationalen Kabelverbindungen quantifiziert und Möglichkeiten zur Verbesserung der Widerstandsfähigkeit diskutiert.

[1] https://www.itu.int/en/ITU-D/Technology/Pages/InteractiveTransmissionMaps.aspx
[2] https://www.itu.int/itu-d/tnd-map-public/

4.1.1 Methodisches Vorgehen

Die in der Einführung gezeigte Karte der europäischen Kabelverbindungen (Abb. 4.1) zeigt eindrücklich den hohen Vermaschungsgrad des physischen Internets. Welche dieser Leitungen allerdings für welche Kommunikationsabläufe besonders relevant oder wesentlich für die Funktionsfähigkeit des deutschen Internets sind, ist daraus nicht ersichtlich. Ziel dieses Kapitels ist daher, das Wissen über Kabelverläufe in Schicht 1 des OSI-Modells mit dem Wissen über Verkehrsweiterleitung in Schicht 3 in Verbindung zu bringen. Dazu müssen Kabelverbindungen in Routing-Daten identifiziert und bzgl. ihrer Weiterleitungseigenschaften ausgewertet werden. Das zu diesem Zweck erarbeitete analytische Vorgehen wird im weiteren Verlauf dieses Abschnitts näher erläutert.

4.1.1.1 Kabelidentifizierung

Weltweite Datensätze mit geographischen Informationen zu nationalen und internationalen Kabelverbindungen sind von einschlägigen Anbietern zu erhalten. Derartige Datensätze beinhalten zwar präzise Standortinformationen, eignen sich aber nicht für eine Charakterisierung des deutschen Internet-Routings. Zur Bestimmung regional bedeutsamer See-/Landkabel ist vielmehr eine messbasierte Analyse aus der Perspektive wichtiger deutscher Infrastrukturen notwendig, die auch eine Quantifizierung konkreter Abhängigkeiten und Ausfallrisiken erlaubt. Nachfolgend wird ein empirischer Ansatz zur Identifizierung und Bewertung relevanter Kabelverbindungen im deutschen Internet-Routing vorgestellt. Kern dieses Konzepts ist die Erkennung von häufig vermessenen IP-Verbindungen mit hohen Latenzdifferenzen, um auf längere darunter liegende Transportstrecken zu schließen.

Datenlage Für die Kabelanalyse wird auf Internet-weite IP-Pfadmessungen über den Zeitraum von einer Woche zurückgegriffen. Diese Messungen werden über IP-Transit der Deutschen Telekom (DTAG) und über das Public Peering am deutschen Internet Exchange Point DE-CIX kontinuierlich in alle gerouteten Netzbereiche, mindestens jedoch in jedes /21 IP-Präfix, durchgeführt. Im Betrachtungszeitraum stehen damit 13.644.000 (DTAG) bzw. 2.271.813 (DE-CIX) IP-Pfadmessungen zur Verfügung. Die Unterschiede in der Größe der Datensätze resultieren daraus, dass am DE-CIX nur ein Teil aller global gerouteten Netzbereiche sichtbar ist. Die Pfaddatensätze beinhalten insgesamt 128.631.357 verwertbare Latenzmessungen zu einzelnen Routern und Messzielen. Durch Bildung der Latenzdifferenz zwischen IP-Adressen, die in den vermessenen Pfaden aufeinander folgen, werden schließlich 102.894.428 Messwerte extrahiert. Diese Einzelwerte beschreiben demnach die differentielle Round Trip Time (Delta-RTT) aller vermessenen Point-to-Point Links. Für jede der resultierenden IP-Verbindungen wird zudem auch eine Liste aller darüber erreichbaren IP-Messziele vorgehalten. Darüber hinaus werden zugehörige IP-Präfixe mit Hilfe von BGP-Tabellen auf deren Ursprungs-AS und anhand von Vergabedaten Regionaler Internet Registrare (RIR) auf deren Registrierungsland abgebildet.

Leitungslänge Im Allgemeinen lässt sich bei gegebener Zeit t und einer Geschwindigkeit v die Länge der zurückgelegten Wegstrecke aus $s = v \cdot t$ berechnen. In optischen Medien erfolgt die Übertragung von Signalen mit etwa zwei Drittel der Vakuum-Lichtgeschwindigkeit, aus einer gemessenen Umlaufzeit RTT ergibt sich somit folgender Zusammenhang für die Länge l einer Verbindungsstrecke:

$$l = \frac{2}{3} \cdot c \cdot \frac{RTT}{2} \approx 100 \frac{km}{ms} \cdot RTT$$

Aus dieser physikalischen Schranke lässt sich eine zurückgelegte Wegstrecke und damit ungefähre Kabellänge von 100 Kilometern je Millisekunde Umlaufzeit als grober Richtwert ablesen. In der Realität kann diese Obergrenze aber (auch deutlich) unterschritten werden, bspw. durch Verzögerungen in der Paketverarbeitung von Routern und der damit verbundenen Überschätzung von Latenzen. Im Hinblick auf eine belastbare Kabelidentifizierung ist daher stets eine möglichst große Stichprobe von IP-Messungen anzustreben.

RTT-Konfidenz Für den überwiegenden Teil aller Internet-weit beobachteten IP-Verbindungen stehen mehrere Messungen und damit RTT-Differenzen zur Verfügung. Aufgrund von sporadischen Paketverzögerungen und periodischen Lastschwankungen, aber auch durch Einsatz von Lastausgleichspfaden und asymmetrischem Routing, können diese einzelnen Differenzen stark variieren. Selbst negative Delta-RTTs sind in der Datenlage prinzipiell möglich, nämlich dann, wenn aufeinanderfolgende Pakete nicht in der ursprünglichen Sendereihenfolge beim Empfänger eintreffen. Nicht zuletzt auch im Hinblick auf einzelne Ausreißer ist die Berechnung eines Durchschnittswertes für die Latenz einer IP-Verbindung daher wenig sinnvoll. Stattdessen werden im Folgenden RTT-Perzentile verwendet, über die sich die Konfidenz von Aussagen über Umlaufzeiten steuern lässt. Sollen bspw. alle IP-Verbindungen mit einer minimalen Latenz von 50 Millisekunden, d.h. einer maximalen Übertragungsstrecke von 5.000 Kilometern betrachtet werden, so ist es (bei hinreichend hoher Messhäufigkeit) ggf. zweckmäßig, diese Bedingung fallbezogen nur für 99% aller Messungen zu fordern und somit isolierte Extremwerte zu ignorieren.

Kabeldefinition Um weiterführende Aussagen über die Abhängigkeit der deutschen Internet-Landschaft von internationalen Kabelverbindungen treffen zu können, muss eine geeignete Kabeldefinition anhand einer minimalen Latenzdifferenz festgelegt werden. Zu niedrig gewählte Werte (unter 5 Millisekunden) sind anfällig für *false positives* aufgrund von nicht geradlinig verlegbaren Metronetzen und statischen Paketverzögerungen bspw. durch ICMP-Ratenlimitierung. Zu hohe Werte (größer als 25 Millisekunden) führen dagegen zu *false negatives* insbesondere für kürzere oder abschnittsweise durchquerte Kabelstrecken mit mehreren Anlandungspunkten. Nach Wahl der minimalen Latenzdifferenz kann eine passende Konfidenz, d.h. die erforderliche Beobachtungshäufigkeit je IP-Verbindung und das gewünschte RTT-Perzentil, festgelegt werden.

Auf der interaktiven Projekt-Webseite lassen sich verschiedene Kabelparameter und zugehörige Analyseergebnisse miteinander vergleichen. Über eine manuelle Betrachtung zahlreicher Einzelergebnisse wurden 10 Millisekunden bei einer Stichprobe von mindestens 500 Einzelmessungen je IP-Verbindung und einer Konfidenz von 95% als bestgeeignet identifiziert (Abb. 4.2). Diese Parameter werden den folgenden Analysen zugrunde gelegt.

4.1.1.2 Abhängigkeitsanalyse

Anhand der nach obigen Vorgaben identifizierten IP-Verbindungen lässt sich die Abhängigkeit der deutschen Internet-Infrastruktur von bedeutsamen See-/Landkabeln näher untersuchen. Trotz der Fokussierung auf Langstrecken (mind. 10 ms bzw. 1.000 km) können die empirischen Ergebnisse im Einzelfall von der Realität abweichen, in ihrer Gesamtheit ermöglichen sie aber eine belastbare Einschätzung der Ist-Situation in Deutschland.

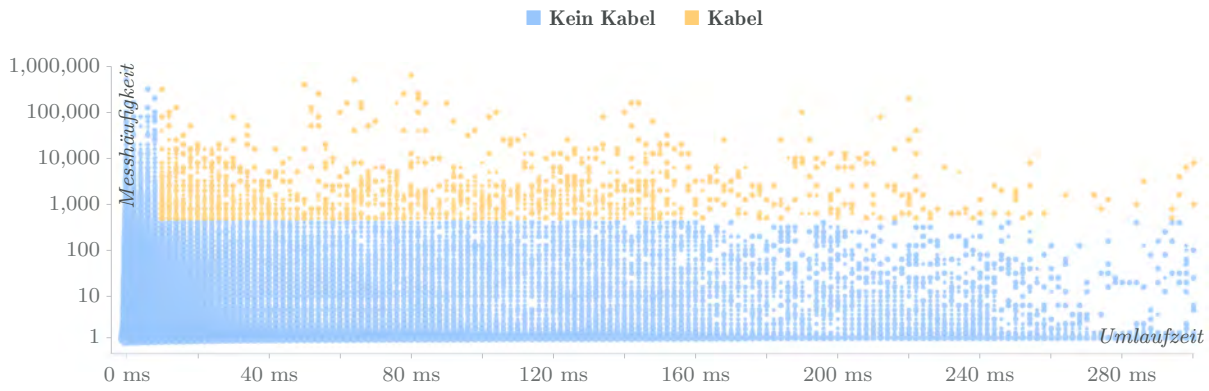


Abbildung 4.2: **Analyseparameter**

Ländervergleich Zunächst wird der Anteil aller weltweit über Kabelverbindungen erreichbaren autonomen Systeme und IP-Präfixe nach Ländern aufgeschlüsselt. Dies kann sowohl nach DTAG/DE-CIX-Messungen getrennt als auch aggregiert über beide Anbieter hinweg erfolgen und ermöglicht eine erste Bestandsaufnahme deutscher Kabelabhängigkeiten. Entsprechende Ergebnisse beschreiben dabei keine exklusiven Erreichbarkeiten, d.h. Alternativ-Verbindungen sind im Fehlerfall durchaus zu erwarten. Ein Vergleich von absoluten Kabelhäufigkeiten nach Land zeigt die vorhandenen Redundanzen auf.

Hoch-frequentierte Kabel Aus den erhobenen Daten lassen sich explizite IP-Verbindungen identifizieren, über die größere Teile des globalen Internet-Verkehrs geroutet werden. Diese können nach Autonomen Systemen bzw. AS-Verbindungen aggregiert und somit bedeutsame Transitanbieter aufgefunden werden. Eine Kabelbewertung anhand der Zahl der erreichbaren IP-Präfixe und Autonomen Systeme, aber auch des jeweiligen Länder- bzw. Kontinentalübergangs, ist ebenso möglich. Durch manuelle Analysen wird zudem versucht, mehrere in den Messdaten unabhängig auftretende IP-Verbindungen auf Schicht 3 einzelnen physischen Kabeln in Schicht 1 zuzuordnen. Der dabei gewählte Ansatz einer DNS-basierten Zuordnung von IP-Adressen zu Router-Interfaces mit einer topologischen Einordnung entsprechend identifizierter Router liefert für hoch-frequentierte Kabel wirklichkeitsnahe Ergebnisse. Auf deren Basis wurde in Abschnitt 3.2 auch eine tiefergehende Risikobewertung anhand eines fiktiven Kabelausfalls vorgenommen.

4.1.2 Bestandsaufnahme

Im Folgenden wird eine allgemeine Übersicht über zentrale Bestandteile der deutschen Internet-Infrastruktur gegeben. Im Anschluss erfolgt hierfür eine Evaluation weltweiter Kabelabhängigkeiten nach dem in Abschnitt 4.1.1 beschriebenen Vorgehen. Schließlich werden kritische Kabelverbindungen identifiziert, die für die internationale Konnektivität Deutschlands von wesentlicher Bedeutung sind.

4.1.2.1 Deutsche Internet-Infrastruktur

Die Deutsche Telekom und der Internet Exchange Point DE-CIX bilden die wichtigsten Eckpfeiler der deutschen Internet-Infrastruktur. Beide Plattformen nutzen internationale Kabelverbindungen, um einen länderübergreifenden Datenverkehr für ihre Kunden sicherzustellen. Im Folgenden wird die Netzinfrastruktur dieser Anbieter näher beleuchtet.

Deutsche Telekom Mit etwa 600 Kunden und ca. 3.500 Autonomen Systemen im Customer Cone zählt die Deutsche Telekom zu den größten Transitanbietern weltweit und wird in der Regel der höchsten Provider-Kategorie *Tier1* zugeordnet. In Norden, Ostfriesland, betreibt der Konzern einen Anlandungspunkt für die Seekabel TAT-14 und SEA-ME-WE 3, an deren Bau und Betrieb die Deutsche Telekom wirtschaftlich beteiligt ist. Ein weitläufiges glasfaserbasiertes Backbone-Netz verbindet alle größeren Städte in Deutschland und erstreckt sich in westlicher Richtung über die Niederlande, Großbritannien, Frankreich und die Schweiz bis nach Italien. In östlicher Richtung ist das Glasfasernetz über Polen in das Baltikum und über Tschechien bis hin zum Balkan ausgebaut.

Über das mittlerweile dekommissionierte Seekabel TAT-14 mit einer Kapazität von 9,4 Tbps (nutzbar: 3,15 Tbps) waren aus dem gesamten Telekom-Netz direkte Schicht-1-Verbindungen in die USA möglich. Der Anschluss an SEA-ME-WE 3 mit einer Kapazität von 4,6 Tbps erlaubt die Schaltung von Wellenlängen zu 38 Anlandungspunkten entlang der europäischen Atlantikküste über Nordafrika und den Nahen/Mittleren Osten bis nach Asien und Australien. Über Partner lassen sich weitere transatlantische und eurasische Kabelverbindungen nutzen. Das folgende Schaubild gibt einen Überblick (Abb. 4.3).

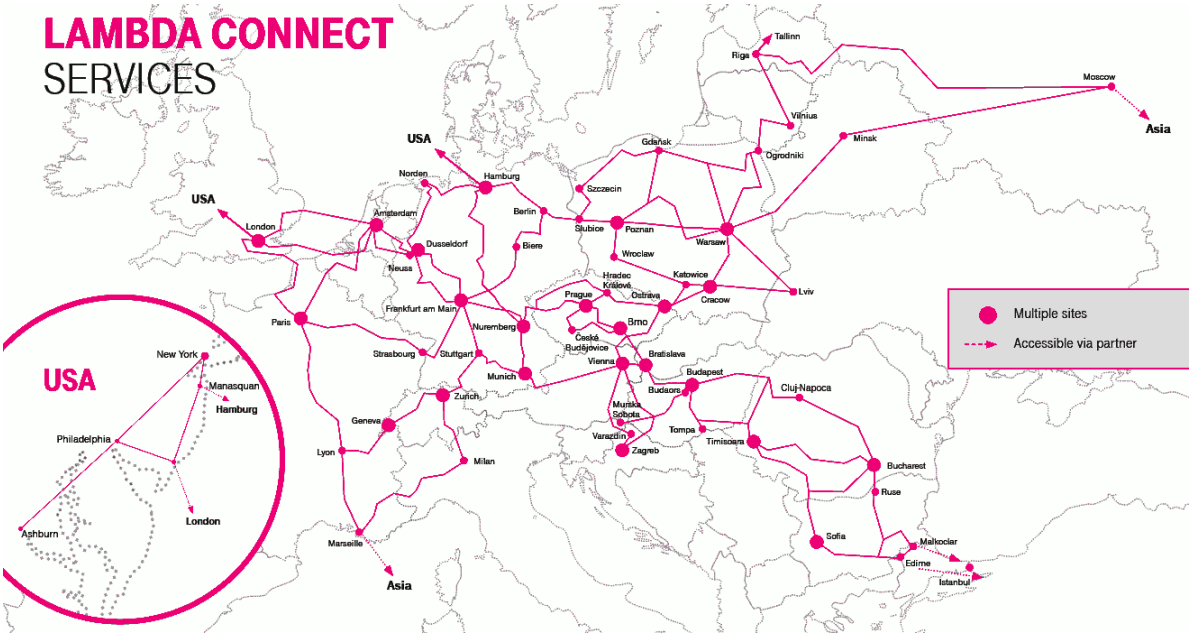


Abbildung 4.3: **Deutsche Telekom Wavelength Services**, Quelle: DTAG

DE-CIX Mit 2.146 angeschlossenen Autonomen Systemen und einer Gesamtkapazität von 68.1 Tbps über alle Standorte hinweg gehört der DE-CIX zu den führenden Anbietern von unabhängigen Internet Exchange Points. Allein über das Public Peering in Frankfurt sind ca. 750 Kunden direkt (und kostenneutral) in der Switching-Plattform erreichbar, der kombinierte Customer Cone dieser Route Server Teilnehmer entspricht mit knapp 30.000 Autonomen Systemen nahezu der Hälfte des globalen Internets. Weitere 18 DE-CIX-eigene Plattformen in Europa, Asien und den USA sind über direkte Schicht-1-Verbindungen erreichbar. Partnerprogramme erlauben zudem eine Fernteilnahme an unabhängigen IXPs (Remote Peering). Die Schaltung von Wellenlängen und MPLS-Verbindungen zur DE-CIX-Infrastruktur ist an unzähligen Standorten auf allen fünf Kontinenten wie in folgendem Schaubild ersichtlich möglich (Abb. 4.4).

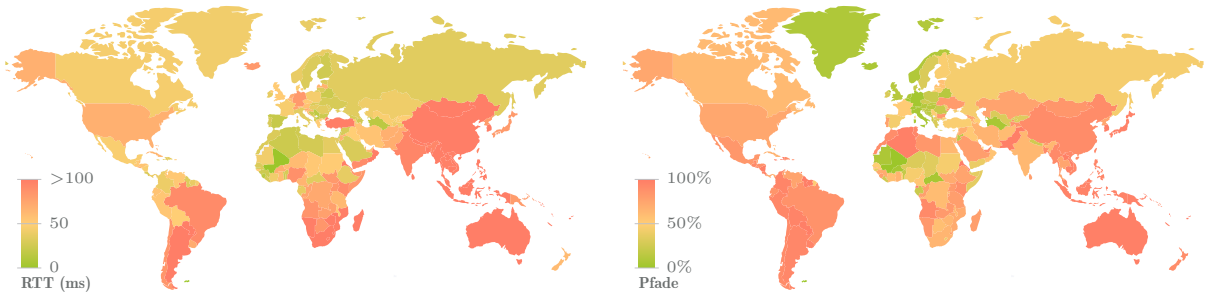
Abbildung 4.4: **DE-CIX Enabled Sites**, Quelle: DE-CIX

4.1.2.2 Weltweite Kabelabhängigkeit

Mit der eingangs beschriebenen Methodik zur Kabelerkennung wurden aus Sicht der Messstandorte DTAG und DE-CIX insgesamt 2.042 Kabel in 202 Autonomen Systemen identifiziert. Darüber sind 73,6% aller weltweiten Autonomen Systeme bzw. 69,2% des global gerouteten IPv4-Addressraumes erreichbar. Für IPv6 wurden aufgrund einer generell geringeren Zahl an Messzielen, und somit weniger IP-Verbindungen mit der geforderten Mindestanzahl an Messungen, nur 180 Kabel in 38 ASen erkannt. Die Internet-weite Kabelerreichbarkeit fällt hierüber mit 50,5% aller ASe und 50,2% aller Netzbereiche ebenfalls etwas niedriger aus, davon abgesehen sind die Ergebnisse jedoch vergleichbar. Die folgenden Analysen beschränken sich aufgrund der besseren Datenlage auf IPv4, sind infolge der Unabhängigkeit von Schicht 1 und Schicht 3 jedoch prinzipiell auf IPv6 übertragbar. Alle Ergebnisse lassen sich auch über die interaktive Projekt-Webseite abrufen.

Um weltweite Kabelabhängigkeiten der deutschen Internet-Infrastruktur zu bestimmen, werden verschiedene Metriken der messbasierten Kabelanalyse geographisch ausgewertet. Zunächst erfolgt eine Darstellung der Durchschnittslatenz aller identifizierten Kabel je Zielland als generelles Maß für die internationale Dienstgüte in Deutschland. Weiterhin wird der länderbezogene Anteil von Kabelverbindungen im Routing zu Autonomen Systemen dargestellt, um bestehende Abhängigkeiten zu quantifizieren. Schließlich erfolgt anhand der Anzahl identifizierter Kabel eine Bewertung der Redundanz der deutschen Internet-Anbindung an andere Länder. Alle Fragestellungen werden zur besseren Vergleichbarkeit separat aus Sicht der DTAG- und DE-CIX-Infrastruktur betrachtet.

Internationale Dienstgüte Neben einer Einschätzung der Dienstqualität in Bezug auf verschiedene Zielregionen dienen Auswertungen von durchschnittlichen Kabellatenzen zunächst auch einer Plausibilisierung der vorliegenden Daten. So würde bspw. die zu erwartende Umlaufzeit einer Messung von Deutschland in die USA bei einer einfachen Kabelstrecke von ca. 7.000 km laut der vorangehenden Berechnungsformel etwa 70 ms betragen, was am Standort DTAG auch den Ergebnissen (69 ms) entspricht (Abb. 4.5).



(a) Durchschnittslatenz (b) Pfadmessungen über Kabel

Abbildung 4.5: **Internationale Dienstgüte**, DTAG

In Einzelfällen kann die Durchschnittslatenz von dem aus der geographischen Distanz zu erwartenden Wert abweichen. Dies liegt zum Teil in indirekt verlegten Landkabeln, die Metropolen oder geographischen Merkmalen folgen, begründet. Auch die Durchschnittsbildung für Länder mit großer Ausdehnung, bspw. Russland mit einer Ost-West-Ausdehnung von rund 9.000 km, führt zwangsläufig zu einer vereinfachten Bewertung. Letztlich tragen auch Artefakte durch die rudimentäre IP-Präfix-basierte Länderzuordnung der Messziele zu Abweichungen bei. Dies zeigt sich insbesondere für Deutschland mit einer Durchschnittslatenz von 83 ms, die sich aus dem Einsatz deutscher IP-Adressen – vielfach durch die Deutsche Telekom – im außereuropäischen Ausland ergeben. Gleichzeitig fällt der hier betrachtete Anteil an IP-Pfadmessungen mit erkannten Kabelverbindungen für Deutschland mit 3,8% sehr gering aus. Dieser Umstand muss bei einer Einschätzung von Kabeldienstgüten naturgemäß berücksichtigt werden (Abb. 4.5). Da der Fokus dieses Kapitels auf internationalen Langstreckenkabeln liegt, was sich auch durch die Wahl einer minimalen Umlaufzeit von 10 ms ($\approx$1.000 km Wegstrecke) in der Kabelerkennung widerspiegelt, werden im Folgenden überwiegend außereuropäische Fragestellungen betrachtet. Hier liefern die Ergebnisse einen belastbaren Einblick in länderbezogene Dienstqualitäten.

Die höchsten Kabelanteile auf den vermessenen Pfaden ergeben sich mit stets mehr als 90% für die Südhalbkugel und Süd-/Ostasien. Gleichzeitig liegen die Durchschnittslatenzen erwartungsgemäß über 90 ms – der limitierende Faktor ist hier die physikalische Schranke der Lichtgeschwindigkeit. Besonders performant angebunden sind hingegen Osteuropa und Russland bei einem Anteil an Langstreckenkabeln von etwa 20–40% sowie Nordafrika und der Nahe Osten mit deutlich höheren Kabelanteilen von 60–90%. Auffällig ist eine überhaus hohe Umlaufzeit von 114 ms in die Türkei, hier kann auf eine unterdurchschnittlich ausgebaute Anbindung geschlossen werden. Ebenfalls auffallend ist ein vergleichsweise hoher Anteil an Kabelverbindungen zu 52% aller französischen Netzbereiche in Verbindung mit einer hohen Durchschnittslatenz von 46 ms, was sich im Gegensatz zu anderen europäischen Ländern möglicherweise durch die zentralisierte, über Paris verlaufende Streckenführung nationaler Kabelverbindungen erklären lässt (Abb. 4.1).

Bemerkensweit ist ein deutlicher Anstieg der durchschnittlichen Kabellatenzen an der Grenze von Indien, China und der Mongolei zu deren nordwestlich gelegenen Nachbarländern. Bei genauerer Betrachtung der Landkabel in dieser Region (Abb. 4.6) zeigt sich, dass aufgrund geographischer und politischer Gegebenheiten keine direkten Landverbindungen in Richtung Europa (und Deutschland) existieren. Besonders auffällig ist eine Abschottung zwischen Pakistan und Indien, die keinerlei direkten Verkehrsaustausch ermöglicht. Somit sind die betroffenen Länder zum überwiegenden Teil über den längeren Seeweg angebunden, was sich in den Durchschnittslatenzen eindrucksvoll widerspiegelt.

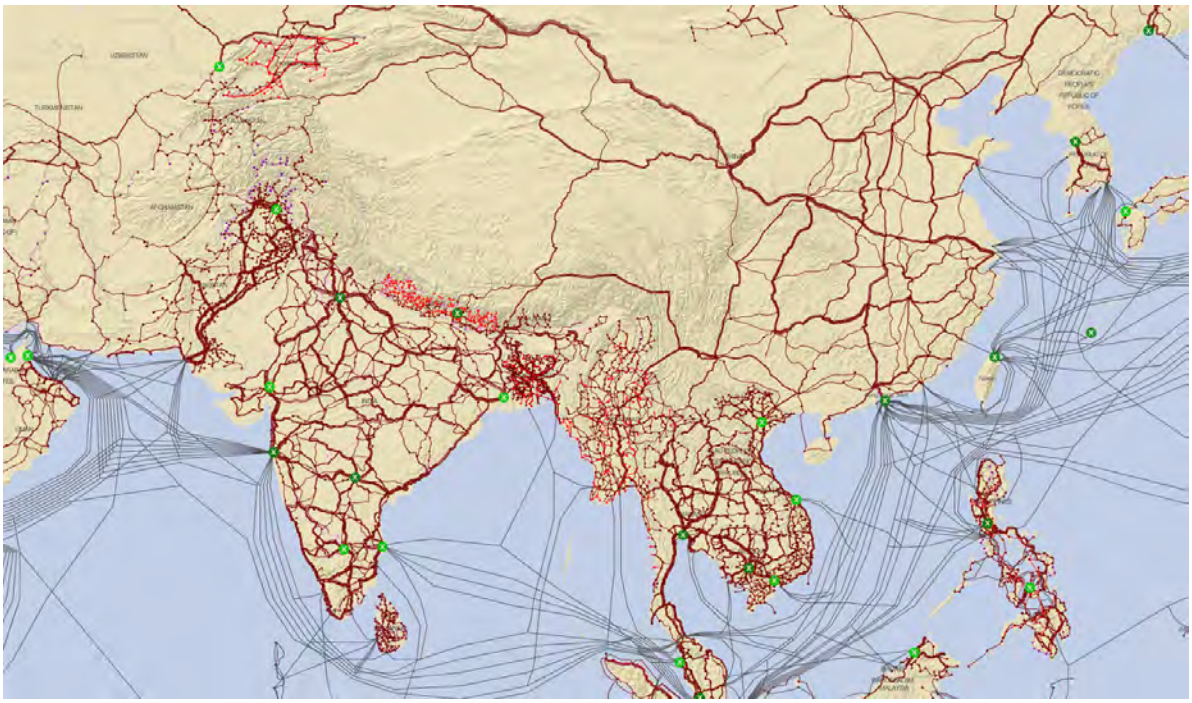
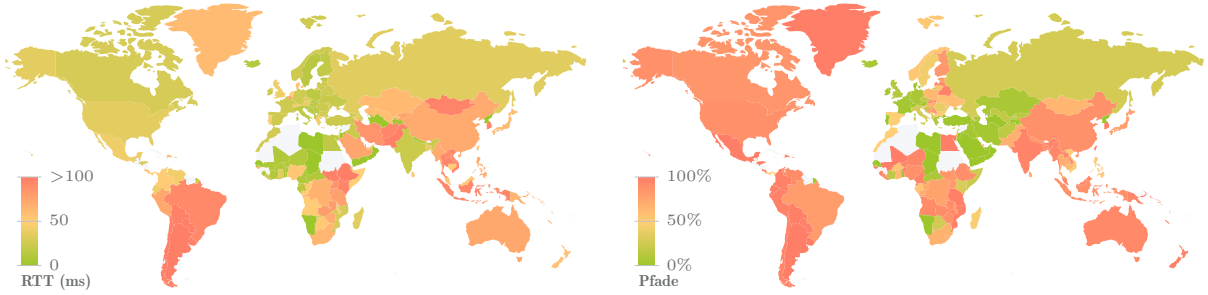


Abbildung 4.6: **Asiatische Kabelverbindungen**, Quelle: ITU [2]

Aufgrund der großteils europäischen Bedeutung des DE-CIX und einer geringeren Zahl an Messungen ergeben sich für dessen Durchschnittslatenzen zunächst weniger deutliche Ergebnisse (Abb. 4.7). Geringe Umlaufzeiten auch für weiter entfernte Netzbereiche können hier erneut in Artefakten der IP-Präfix-basierten Zuordnung von Messzielen zu Ländern begründet liegen. Zudem sind am DE-CIX zahlreiche internationale ISPs vor Ort präsent, die dort in der Regel auf ihr Land registrierte Netzbereiche verwenden, woraus sich bspw. eine Durchschnittslatenz von 36 ms für die USA ergibt. Demnach ist hier in höherem Maße mit Abweichungen zwischen der administrativen und physischen Verortung zu rechnen. Auch Remote Peering Anbindungen auf Schicht 2 tragen verstärkt dazu bei.

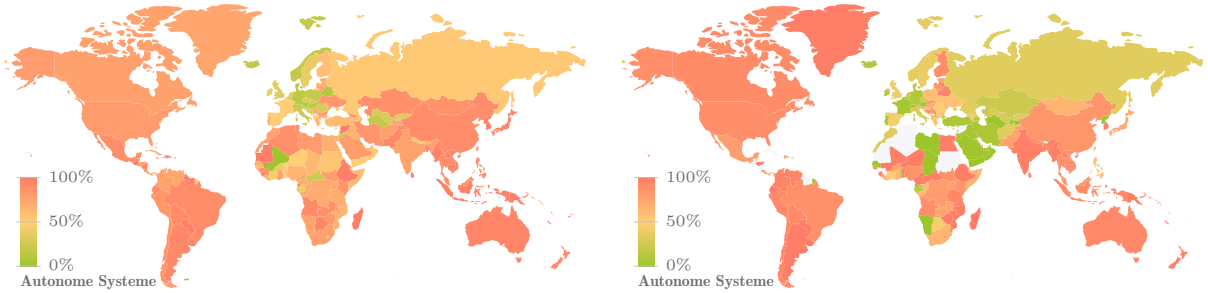


(a) Durchschnittslatenz (b) Pfadmessungen über Kabel

Abbildung 4.7: **Internationale Dienstgüte**, DE-CIX

Die Zahl der erkannten Kabelverbindungen liegt am DE-CIX mit 333 deutlich niedriger als bei der Deutschen Telekom mit 1.827 Kabeln (Schnittmenge: 215). Dennoch lassen sich auch hier weitgehend vergleichbare Aussagen über die internationale Anbindung Deutschlands ableiten. Bemerkenswert ist das große Einzugsgebiet des DE-CIX mit einem Radius von ca. 5.000 km, das aufgrund der Vielzahl regionaler IXP-Teilnehmer und deren engmaschigen Metronetzen kaum (anfälligere) Langstreckenkabel erfordert.

Kabelabhängigkeiten Die Abhängigkeit des deutschen Internets von internationalen Kabelverbindungen lässt sich anhand einer länderbezogenen Analyse des prozentualen Anteils aller weltweiten Autonomen Systeme, die über Langstreckenkabel an Deutschland angebunden sind, bewerten (Abb. 4.8). Dabei ist allerdings zu beachten, dass entsprechende Netzbereiche nicht zwangsläufig ausschließlich per Kabel zu erreichen sind. Ausweichverbindungen über Satellit oder enger vermaschte Kurzstreckennetze sind bei Störungen fallabhängig möglich. Zudem sind geographisch verteilt operierende Netzbetreiber von Kabelausfällen meist nur teilweise betroffen. Nichtsdestotrotz geben die Ergebnisse quantitative Einblicke in die international vorherrschenden Kabelabhängigkeiten.



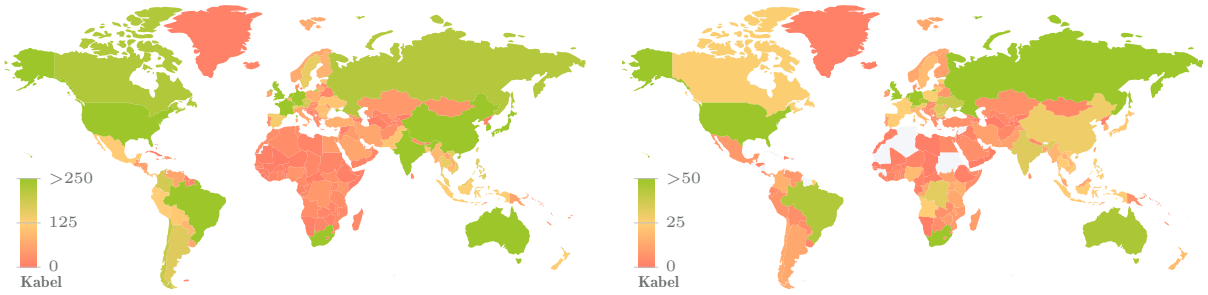
(a) DTAG (b) DE-CIX

Abbildung 4.8: **Kabelabhängigkeiten**

Erwartungsgemäß ergibt sich für alle Kontinente außer Europa eine hohe Abhängigkeit von Langstreckenkabeln. Für nahezu alle außereuropäischen Länder liegt der Anteil kabelabhängiger Netzbetreiber bei 80–90%, lediglich in Afrika zeigt sich aufgrund der geringen Zahl aktiver Autonomer Systeme ein mehr heterogenes Bild. Der unmittelbare Einzugsbereich des DE-CIX mit vielen über Kurzstreckenverbindungen angeschlossener ISPs ist auch in dieser Analyse größer als bei der Deutschen Telekom, wo höhere Kabelabhängigkeiten an den Grenzen von Europa vorherrschen. Für beide Perspektiven auffallend ist eine deutlich geringere Abhängigkeit russischer Autonomer Systeme von Langstreckenkabeln mit 54% bzw. 34%. Aufgrund dessen großer geographischer Ausdehnung sind die Ergebnisse allerdings nicht pauschal zu bewerten, eine Unterteilung von Russland in dessen europäischen und asiatischen Teil wäre für zukünftige Analysen zweckmäßig. Zusammenfassend ergibt die Analyse ein zu erwartendes Bild – nahezu alle Netzbetreiber in geographisch weit entfernten Regionen sind über Kabelverbindungen an Deutschland angeschlossen. Für Mittelstreckenverbindungen wird diese Abhängigkeit am DE-CIX jedoch abgemildert.

Redundanz Aufgrund der erwartbaren Abhängigkeit außereuropäischer Netzbetreiber von internationalen Kabelverbindungen ist deren redundante Auslegung von besonderem Interesse. Für eine länderbezogene Bewertung von Kabelredundanzen kann die absolute Zahl aller identifizierten Kabelverbindungen herangezogen werden (Abb. 4.9). Dabei ist allerdings zu beachten, dass die messbasierte Kabelanalyse zwar belastbare Hinweise auf Langstreckenkabel liefert, damit jedoch noch keine Aussagen über konkrete physische Kabel möglich sind. Insbesondere können mehrere unterschiedliche IP-Verbindungen in Schicht 3 über dasselbe Kabel in Schicht 1 realisiert sein, wodurch die Zahl redundanter Kabel potentiell überschätzt wird. Messungen über mehrere eingehende Interfaces einzelner Router, und somit auch mehrere lastausgleichende IP-Verbindungen zwischen zwei Routern, können diesen Effekt noch verstärken. In den Analysen des nächsten Abschnitts

wird diesem Umstand durch entsprechende Aggregierungsverfahren Rechnung getragen, an dieser Stelle wird der Fokus jedoch auf Redundanzen in Schicht 3 gelegt. Die Ergebnisse zeigen demnach, über wie viele unterschiedliche IP-Verbindungen mit Kabelbezug einzelne Länder zu erreichen sind, was im Wesentlichen einem übergeordneten Maß der Toleranz eines Landes gegenüber Router-Ausfällen an Anlandungspunkten entspricht.



(a) DTAG (b) DE-CIX

Abbildung 4.9: **Redundanz**

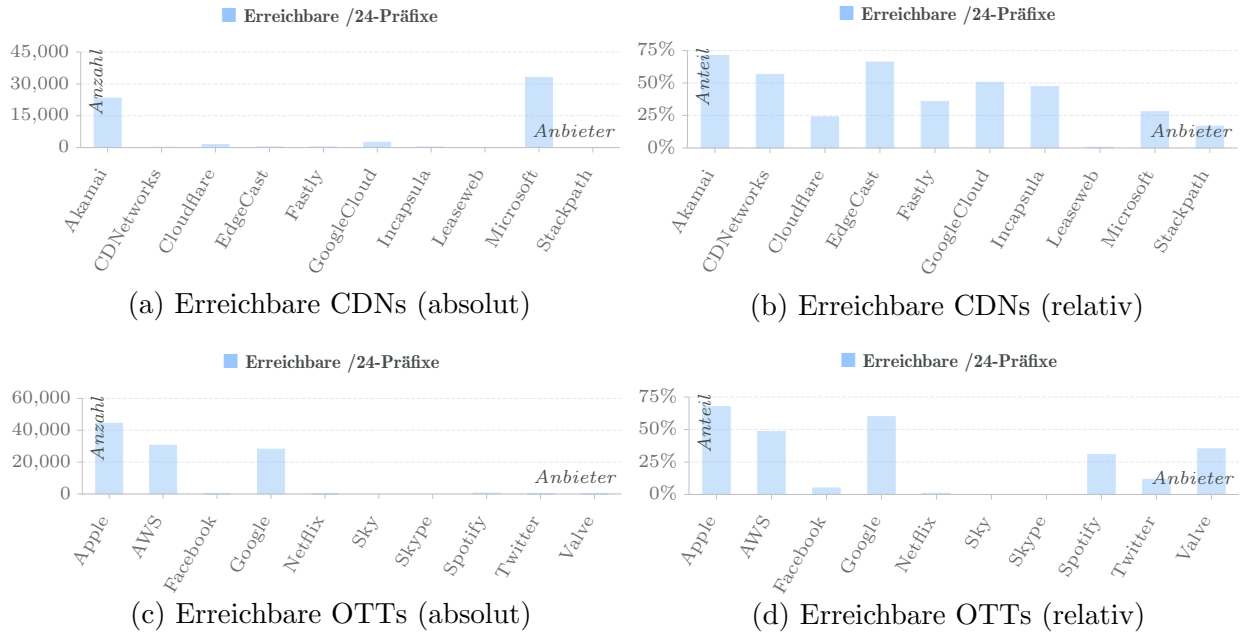
Die mit Abstand größte Zahl an redundanten Kabelverbindungen (1.208) ergibt sich aus Sicht der Deutschen Telekom für die USA. Aber auch China (420), Brasilien (305), Australien (304), Südafrika (285), Indien (258) und Japan (252) verfügen über ein hohes Maß an Redundanz. Diese Verteilung scheint plausibel, da in den genannten Staaten zahlreiche Anlandungspunkte für Seekabel zu finden sind. Auffällig hingegen ist eine vergleichsweise geringe Zahl an Verbindungen nach Süd- und Osteuropa, wobei hier analog zu den vorangehenden Auswertungen Kurzstreckenkabel außer Betracht bleiben. Insbesondere jedoch nach Afrika sind kaum nennenswerte Alternativ-Routen zu beobachten, was sich auch durch wiederkehrende landesweite Internet-Ausfälle in afrikanischen Ländern im Zusammenhang mit Kabelbeschädigungen zeigt (siehe Abschnitt 2.1.2.4). Eine zu Afrika vergleichbare Situation ergibt sich auch für den Nahen und Mittleren Osten sowie in geringerem Umfang für Teile Südamerikas. Aus Sicht des DE-CIX sind dabei – abgesehen von generell niedrigen Absolutzahlen – keine wesentlichen Abweichungen festzustellen, lediglich Asien ist der Erwartung entsprechend anteilig weniger redundant über den deutschen IXP zu erreichen. Allgemein zeichnet sich ab, dass zu wirtschaftlich oder politisch bedeutsamen Ländern, die in hohem Maße von Kabelverbindungen abhängen, auch überdurchschnittlich viele redundante Verbindungen identifiziert werden können. Für Entwicklungsländer hingegen besteht offenkundig Handlungsbedarf.

4.1.3 Kritische Kabelverbindungen

Aus den vorangehend als Langstreckenkabel identifizierten IP-Verbindungen lassen sich auch Aussagen über kritische Kabelbetreiber ableiten. Dazu werden IP-Links über eine IP-Präfix-basierte Zuordnung auf Autonome Systeme bzw. AS-Links abgebildet. Mehrere unterschiedliche IP-Verbindungen können somit zum selben AS-Link zugeordnet und die jeweils darüber erreichbaren Netzbereiche aggregiert werden. Dieses Vorgehen liefert zunächst eine weitere Abstraktion von physischen Kabeln, reduziert jedoch gleichzeitig die vorangehend diskutierten Messartefakte in Bezug auf mehrere Router-Interfaces und lastausgleichende Router-Pfade. Im Ergebnis lassen sich – auch unter Einbezug von Netzplänen und öffentlichen Seekabelinformationen – die wichtigsten ISPs bzw. ISP-Verbindungen

für den Transit in verschiedene Zielregionen identifizieren und zudem die darüber erreichbaren Dienstanbieter analysieren. Hierdurch wird eine individuelle Betrachtung der wichtigsten internationalen Content Delivery Networks (CDN) und Over-The-Top-Anbieter (OTT) möglich, die naturgemäß auch für Deutschland von großer Bedeutung sind. Im Fallbeispiel TAT-14 werden schließlich DNS-Daten zugrundeliegender IP-Messungen herangezogen, um ein detailliertes Routing-Bild des transatlantischen Seekabels anzufertigen. Alle nachfolgenden Analysen werden für eine kombinierte Sicht der DTAG- und DE-CIX-Infrastruktur durchgeführt, um eine möglichst umfassende Datengrundlage herzustellen. Weitere Einzelergebnisse lassen sich über die interaktive Projekt-Webseite abrufen.

Mögliche Auswirkungen eines Ausfalls von kritischen Kabelverbindungen können anhand der Zahl der darüber erreichbaren IP-Präfixe und Autonomen Systeme abgeschätzt werden. Auch wenn einzelne Kabelausfälle nicht zwangsläufig zur Nichterreichbarkeit entsprechender Netzbereiche führen, so ist bei Umleitungen über Ausweichkabel aufgrund von Überlast und längeren Kabelstrecken nichtsdestotrotz eine Verringerung der Dienstqualität zu erwarten. Für eine praxisnahe Einschätzung der Relevanz von Kabelverbindungen sowie möglicher Konsequenzen eines Ausfalls können darüber hinaus auch die über Kabel erreichbaren Netzbereiche ausgewählter CDNs und OTTs analysiert werden (Abb. 4.10).



(a) Erreichbare CDNs (absolut)

(b) Erreichbare CDNs (relativ)

(c) Erreichbare OTTs (absolut)

(d) Erreichbare OTTs (relativ)

Abbildung 4.10: **Kabelabhängigkeiten populärer Netzdienste**

In obigen Diagrammen ersichtlich sind die weltweit über alle identifizierten Kabelverbindungen erreichbaren IP-Präfixe für die zehn populärsten CDN- und OTT-Anbieter sowie deren relativer Anteil bezogen auf deren jeweilige Netzgröße. Als Maßstab wurde für eine bessere Vergleichbarkeit die aggregierte Größe aller Netzbereiche, gemessen in /24-Netzwerken, zugrunde gelegt. Dabei zeigt sich, dass das CDN von Akamai von Deutschland aus zu 71% über Kabelverbindungen erreichbar ist, ähnlich zum OTT-Angebot von Apple mit 67%. Die durchschnittliche Kabelabhängigkeit aller CDN/OTT-Anbieter liegt mit 39% bzw. 25% ebenfalls unerwartet hoch, insbesondere im Hinblick auf die zunehmende Verbreitung von IP Anycast [57]. Content-Caches, die von unabhängigen ISPs in deren eigener Netzinfrastruktur betrieben werden, bleiben dabei zwar aufgrund der fehlenden Zuordnungsmöglichkeit zu Netzbereichen von CDNs und OTTs außer Betracht. Die

Synchronisierung dieser lokal gespiegelten Inhalte mit zentral bzw. kontinental verwalteten Speichersystemen der Anbieter wäre jedoch von – in der Regel länger anhaltenden – Kabelausfällen analog zu obigen Ergebnissen betroffen. Alle nachfolgenden Analysen werden dementsprechend regionsbezogen, d.h. separat nach Kontinenten durchgeführt und zugehörige CDN/OTT-Analysen dabei auf Anbieter-spezifische Netzinfrastrukturen des jeweiligen Kontinents eingeschränkt. Aufgrund der deutlichen Unterschiede in den Netzgrößen einzelner Anbieter werden im Folgenden nur mehr relative Anteile betrachtet.

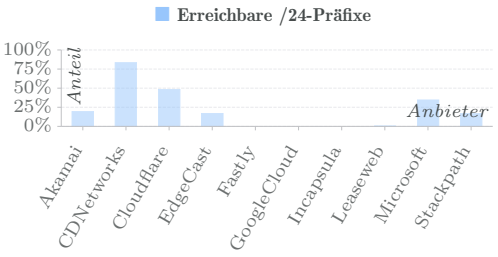
4.1.3.1 Unabhängige Kabelbetreiber

Zur Bestimmung von unabhängigen Kabelbetreibern werden all diejenigen Kabelverbindungen ausgewertet, für die beide zugehörigen IP-Adressen der zugrundeliegenden IP-Verbindungen im gleichen Autonomen System liegen. In diesen Fällen ist davon auszugehen, dass der jeweilige Netzbetreiber Infrastruktur an beiden Enden eines Kabels betreibt, d.h. selbst für den Transport verantwortlich ist. Allerdings ist anzumerken, dass im Falle von Point-to-Point-Verbindungen zwischen ISPs meist IP-Adressen des einen ISPs an den jeweils anderen verliehen werden. Nicht jede IP-Verbindung mit gleichen ASen beschreibt demnach zwangsläufig eine AS-interne Verbindung, so dass in Einzelfällen Kabelpartner nicht in Erscheinung treten. Auch trifft diese Definition keine Aussage über die Besitzverhältnisse eines physisch durchquerten Kabels, es kann sich sowohl um ein exklusiv genutztes eigenes Kabel als auch um angemietete Kapazität in Kabeln eines Drittanbieters handeln. Ebenso ist die Einschaltung eines in Schicht 3 nicht sichtbaren Kabelanbieters möglich. Ungeachtet dieser Einschränkungen kommt ein Ausfall in der Infrastruktur des jeweils betrachteten ISPs stets einem Ausfall des entsprechenden Kabels gleich.

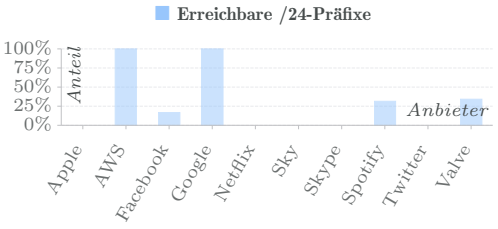
Europa Im Folgenden werden die zehn wichtigsten Transit-ISPs für die kabelgebundene Weiterleitung innerhalb Europas zusammen mit den darüber erreichbaren europäischen Autonomen Systemen und /24-Netzwerken aufgelistet. Die Gegenüberstellung wird ergänzt durch die über Kabel erreichbaren CDN- und OTT-Netzbereiche in Europa im Verhältnis zur jeweiligen gesamteuropäischen Netzgröße der Anbieter (Abb. 4.11).

Transit-ISP	Land	ASe	/24-Netze	Latenz
DE-CIX AS6695	DE	4.071	97.473	50 ms
DTAG AS3320	DE	2.931	213.730	93 ms
RETN AS9002	UA	2.650	43.802	26 ms
Seabone AS6762	IT	1.213	87.919	81 ms
Telia AS1299	SE	798	24.043	53 ms
MegaFon AS31133	RU	787	14.811	43 ms
NTT AS2914	JP	739	12.710	80 ms
Cogent AS174	US	615	36.486	17 ms
Hurricane AS6939	US	593	7.867	48 ms
Level3 AS3356	US	566	56.057	74 ms

(a) Kabelerreichbarkeiten nach Transit-ISP



(b) Erreichbare CDNs



(c) Erreichbare OTTs

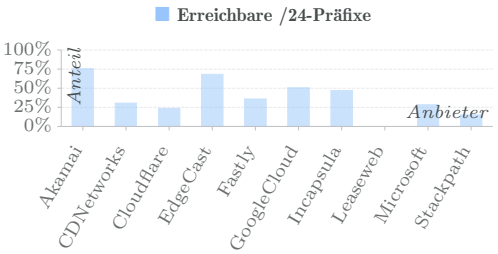
Abbildung 4.11: **Unabhängige Kabelbetreiber**, Europa

Wie eingangs bereits erwähnt bleiben in der vorliegenden Analyse Kurzstreckenverbindungen und Metronetze in Europa aufgrund der kurzen, für die vorliegende Kabelerkennung ungeeigneten Latenzen außer Betracht. Dennoch zeigt sich, dass unmittelbar über die Infrastruktur der Deutschen Telekom etwa 11% bzw. des DE-CIX etwa 15% der insgesamt 27.865 in Europa gerouteten Autonomen Systeme per Langstreckenkabel erreichbar sind, was sich auch in deren paneuropäischen Netzplänen widerspiegelt (siehe Abb. 4.3 und Abb. 4.4). Vom ukrainischen Anbieter RETN werden weiterhin zahlreiche Landkabelverbindungen nach Osteuropa und Russland unterhalten. Seabone, das Backbone-Netz von Telecom Italia Sparkle, ist ebenfalls stark vertreten, die verbleibenden ASe in Europa werden zumeist über die Infrastruktur internationaler Tier1-ISPs angebunden. Für etwas mehr als die Hälfte der betrachteten CDNs und OTTs sind deren europäische Netzbereiche in großen Teilen per Langstreckenkabel zu erreichen. Dies trifft mit einer Abhängigkeit von 100% insbesondere für die OTTs Amazon AWS und Google sowie in etwas geringerem Maße zu 83% auch für CDNetworks zu. Die verbleibenden Anbieter unterliegen in Europa nur einer geringeren oder vernachlässigbaren Abhängigkeit von Langstreckenkabeln.

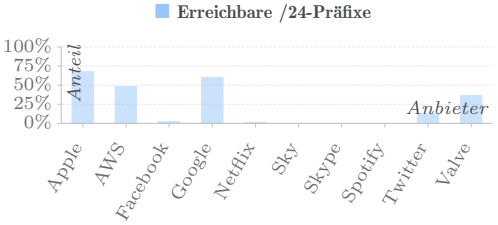
Nordamerika Für die Verkehrsweiterleitung nach Nordamerika (Abb. 4.12) ist aus Sicht der deutschen Netzinfrastruktur die Deutsche Telekom bzw. dessen TAT-14 Kabel maßgeblich, hierüber sind 46% der 19.166 nordamerikanischen Autonomen Systeme erreichbar. Nichtsdestotrotz tragen auch alle namhaften, überwiegend US-amerikanischen Tier1-ISPs zur transatlantischen Kommunikation bei. Hier sind insbesondere Hurricane (16%) mit angemieteter Kapazität über das AEC-1 Kabel von Irland nach New York sowie NTT (15%) über ein – trotz Zuhilfenahme von DNS-Daten – nicht näher bestimmbares Kabel anzuführen. Hingegen sind über die angemieteten Kabelverbindungen des DE-CIX zu dessen Standort in New York nur eine unwesentliche Zahl an Netzbetreibern zu erreichen. Auffallend sind sehr geringe Latenzen beim Infrastrukturbetreiber Zayo (12 ms) und dem US-Telekommunikationsmarktführer Comcast (16 ms), hier ist zweifelsohne von Landkabeln innerhalb den USA auszugehen. Erwartungsgemäß sind alle CDNs bis auf den niederländischen Anbieter Leaseweb von transatlantischen Kabelverbindungen abhängig – allen voran Akamai, Verizon EdgeCast und GoogleCloud zu über 50%. Bei den OTTs zeigt sich nur für Apple, Google und Amazon AWS eine ausgeprägte US-Fokussierung.

Transit-ISP	**Land**	**ASe**	**/24-Netze**	**Latenz**
DTAG AS3320	DE	8.776	1.901.584	94 ms
Hurricane AS6939	US	3.149	204.201	47 ms
NTT AS2914	JP	2.893	291.770	80 ms
Telia AS1299	SE	1.930	296.752	53 ms
Zayo AS6461	US	1.575	115.804	12 ms
Level3 AS3356	US	1.446	78.132	91 ms
GTT AS3257	US	1.131	70.650	84 ms
Cogent AS174	US	1.114	33.521	22 ms
Comcast AS7922	US	619	79.202	16 ms
DE-CIX AS6695	DE	242	4.462	58 ms

(a) Kabelerreichbarkeiten nach Transit-ISP



(b) Erreichbare CDNs



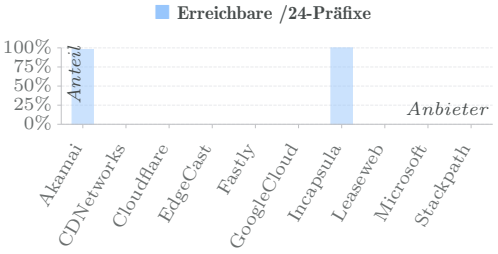
(c) Erreichbare OTTs

Abbildung 4.12: **Unabhängige Kabelbetreiber**, Nordamerika

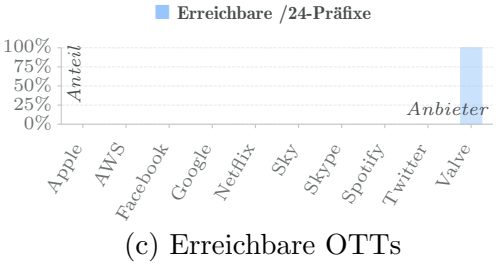
Südamerika Für die direkte Kommunikation mit Südamerika steht aus deutscher Sicht das Atlantis-2 Seekabel von Spanien und Portugal nach Brasilien und Argentinien mit einer Länge von 8.500 km zur Verfügung. Weitere Hinweise auf die Bedeutsamkeit dieses Seekabels geben wirtschaftliche Beteiligungen von Deutscher Telekom und Telefonica, deren damit verbundene hohe Weiterleitungsanteile zu 36% bzw. 19% aller 9.883 südamerikanischen Netzbetreiber sowie vergleichsweise niedrige Durchschnittslatenzen (Abb. 4.13). Erhebliche Kommunikationsströme verlaufen allerdings auch indirekt über Nordamerika, insbesondere in unerwartet hohem Maße über die Infrastruktur des DE-CIX (29%). Dies lässt sich durch Remote Peerings über New York erklären – durch den kürzlich etablierten Direktzugang zu Seaborn Seekabeln nach Südamerika[3] ist zukünftig mit einer weiteren Zunahme des Weiterleitungsanteils über den DE-CIX zu rechnen. Für Seabone (29%) und Level3 (20%) legen die Ergebnisse aufgrund hoher Latenzen Ende-zu-Ende-Verbindungen über deren eigene US-Infrastruktur nahe, wohingegen weitere Tier1-ISPs nur abschnittsweise von Europa nach Nordamerika oder von Nord- nach Südamerika zur Weiterleitung beitragen. Insbesondere scheint Cogent aufgrund sehr niedriger Latenzen trotz eigener Seekabelkapazitäten nach Brasilien von Deutschland aus nur für den Transport zwischen New York und Florida genutzt zu werden. Ein Ausfall der erkannten Kabelverbindungen hätte Konsequenzen für alle südamerikanischen Netzbereiche von Akamai – was allerdings nur 44 von dessen 32.769 weltweiten /24-Netzwerken entspricht. Ebenso unbedeutend wären Totalausfälle für Incapsula und Valve mit einem bzw. zwei /24-Netzwerken in Südamerika. Die verbleibenden CDNs und OTTs zeigen keinerlei südamerikanische Abhängigkeit.

Transit-ISP	Land	ASe	/24-Netze	Latenz
DTAG AS3320	DE	3.573	235.432	92 ms
DE-CIX AS6695	DE	2.846	27.807	97 ms
Seabone AS6762	IT	2.814	107.383	123 ms
Level3 AS3549	US	1.951	18.303	175 ms
Telefonica AS12956	ES	1.838	135.007	68 ms
Cogent AS174	US	1.526	25.679	25 ms
NTT AS2914	JP	1.010	65.182	81 ms
GTT AS3257	US	798	14.387	90 ms
GlobeNet AS52320	CO	774	8.834	36 ms
Telia AS1299	SE	758	68.830	41 ms

(a) Kabelerreichbarkeiten nach Transit-ISP



(b) Erreichbare CDNs



(c) Erreichbare OTTs

Abbildung 4.13: **Unabhängige Kabelbetreiber**, Südamerika

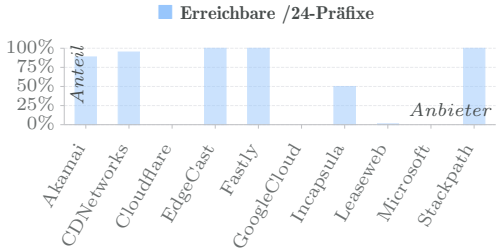
Asien Konnektivität nach Asien wird sowohl in westlicher Richtung über die USA als auch in östlicher Richtung über den Nahen Osten sichergestellt. Ein signifikanter Teil von 33% der insgesamt 9.390 asiatischen Netzbetreiber ist über die DE-CIX Plattform zu erreichen (Abb. 4.14), in mehr als der Hälfte aller Fälle mit Hilfe des indischen ISPs Bharti Airtel über Marseille und das Rote Meer. Hierfür sind verschiedene Kabel im Einsatz,

[3] https://www.de-cix.net/en/about-de-cix/news/de-cix-partners-with-seaborn-flexible-access-to-multiple-de-cix-locations

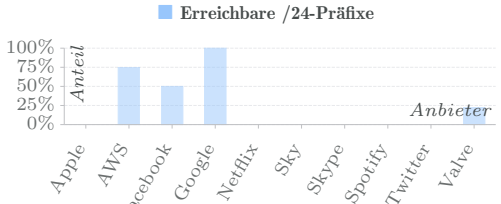
darunter SEACOM, MENA und SEA-ME-WE-4. Auch Seabone trägt zur Anbindung von 26% aller asiatischen Autonomen Systeme über das SEA-ME-WE Kabelsystem bei, an dem der italienische Anbieter ebenso wie Bharti Airtel wirtschaftlich beteiligt sind. Telia nutzt mehrere Kabel über Marseille nach Singapore und Hong Kong, auch ein Landkabel über Russland ist hier im Einsatz. NTT hingegen leitet Verkehre für 32% der ASe zum größten Teil über die USA und Japan, während Verbindungen über das Mittelmeer nach Asien einer DNS-basierten Analyse zufolge kaum genutzt werden. Die Deutsche Telekom ist für die Weiterleitung nach Asien von geringerer Bedeutung (18%) und stellt über das TAT-14 Kabel lediglich eine Teilstrecke bis Palo Alto an der Westküste der USA zur Verfügung. Erstmalig unter den zehn wichtigsten Transitanbietern tritt für die Weiterleitung nach Asien der indische Tier1-ISP Tata (13%) in Erscheinung. Die einzigen Content-Anbieter mit einer nennenswerten Menge an asiatischen Netzbereichen sind Akamai mit 282 und CDNetworks mit 61 /24-Netzwerken. Diese sind zu 88% bzw. 95% über Langstreckenkabel zu erreichen. Hohe Kabelabhängigkeiten für die verbleibenden Anbieter beziehen sich dagegen auf einen vernachlässigbar kleinen Teil asiatischer Netzbereiche, so dass Kabelausfälle aus Sicht von Deutschland hier kaum ins Gewicht fallen würden.

Transit-ISP	Land	ASe	/24-Netze	Latenz
DE-CIX AS6695	DE	3.117	139.166	68 ms
NTT AS2914	JP	3.005	675.171	79 ms
Seabone AS6762	IT	2.391	125.246	61 ms
Telia AS1299	SE	1.985	344.947	58 ms
DTAG AS3320	DE	1.733	445.699	95 ms
Hurricane AS6939	US	1.712	62.448	48 ms
Tata AS6453	IN	1.216	31.150	80 ms
PCCW AS3491	HK	608	62.711	232 ms
GTT AS3257	US	505	29.042	97 ms
Vodafone AS1273	GB	413	21.804	78 ms

(a) Kabelerreichbarkeiten nach Transit-ISP



(b) Erreichbare CDNs



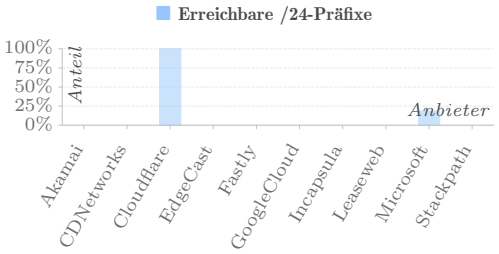
(c) Erreichbare OTTs

Abbildung 4.14: **Unabhängige Kabelbetreiber**, Asien

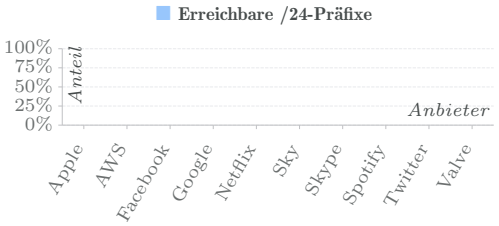
Afrika Bei der Weiterleitung nach Afrika treten keine Transitanbieter in besonderem Maße hervor (Abb. 4.15). Auffallend ist jedoch die Präsenz von multinationalen afrikanischen Gemeinschaftsprojekten wie dem SEACOM-Kabelsystem oder der West Indian Ocean Cable Company mit 15% bzw. 9% Anteil am Routing zu den 1.415 afrikanischen Autonomen Systemen. Demgegenüber treten international bedeutsame Tier1-ISPs wie Telia, Level3 und GTT nicht unter den zehn wichtigsten Transitanbietern für Verbindungen nach Afrika in Erscheinung. Auch Cogent scheint aufgrund einer niedrigen Durchschnittslatenz nur für europäische Streckenabschnitte relevant. Aus Sicht der wichtigsten CDNs betreiben lediglich Cloudflare und Microsoft eigene in Afrika registrierte Netzbereiche (4 bzw. 512 /24-Netzwerke). Letztere sind jedoch nur zu 18% über Kabelverbindungen angebunden, die verbleibenden Netze werden daher vermutlich innerhalb von Europa verwendet. OTT-Anbieter mit eigenen afrikanischen Netzbereichen sind nicht zu verzeichnen.

Transit-ISP	Land	ASe	/24-Netze	Latenz
Seabone AS6762	IT	469	110.417	53 ms
DTAG AS3320	DE	343	71.528	95 ms
DE-CIX AS6695	DE	313	38.732	29 ms
Hurricane AS6939	US	294	19.409	48 ms
NTT AS2914	JP	237	24.510	80 ms
SEACOM AS37100	MU	215	19.633	116 ms
Liquid AS30844	GB	184	21.284	124 ms
WIOCC AS37662	MU	131	6.528	64 ms
Tata AS6453	IN	112	19.449	90 ms
Cogent AS174	US	90	36.730	16 ms

(a) Kabelerreichbarkeiten nach Transit-ISP



(b) Erreichbare CDNs



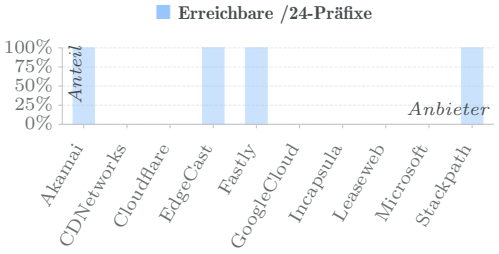
(c) Erreichbare OTTs

Abbildung 4.15: **Unabhängige Kabelbetreiber**, Afrika

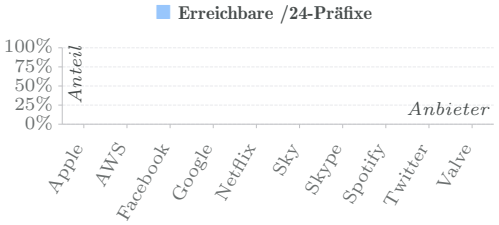
Ozeanien Die mit Abstand meisten Verbindungen nach Ozeanien werden von Hurricane unterhalten (Abb. 4.16). Über diesen Transitanbieter sind 72% der 1.593 australischen Autonomen Systeme erreichbar. Dabei finden sich Kabelverbindungen von London nach New York, Verbindungen innerhalb der USA, sowie von San Jose nach Australien. Für die Teilstrecke von Europa nach Nordamerika wird vermutlich das Seekabel AEC-1 durchquert, ab San Jose kommen mehrere Kabel in Betracht. Bei Telia (49%) finden sich sowohl Kabelverbindungen innerhalb der USA von Ashburn nach Las Vegas als auch von dort weiterführende Verbindungen nach Singapur. Der australische ISP Vocus (45%) stellt angemietete Kapazitäten auf den Kabeln von Telstra, Southern Cross Cable Network und Hawaiki bereit, Telstra tritt allerdings auch eigenständig im Routing nach Australien in Erscheinung. Die Deutsche Telekom (39%) hingegen bietet lediglich Verbindungen über TAT-14 bis hin zur Westküste der USA. CDNs operieren in vernachlässigbar geringem Maße mit australischen IP-Präfixen, OTTs zeigen keinerlei Kabelabhängigkeiten.

Transit-ISP	Land	ASe	/24-Netze	Latenz
Hurricane AS6939	US	1.146	45.616	49 ms
Telia AS1299	SE	733	28.992	56 ms
Vocus AS4826	AU	719	20.799	135 ms
DTAG AS3320	DE	614	88.637	94 ms
NTT AS2914	UP	338	22.022	81 ms
Telstra AS4637	HK	254	59.565	161 ms
Superloop AS38195	AU	229	4.345	64 ms
Singtel AS7473	SG	184	12.422	149 ms
Cogent AS174	US	123	1.829	16 ms
Telstra AS1221	HK	92	21.770	12 ms

(a) Kabelerreichbarkeiten nach Transit-ISP



(b) Erreichbare CDNs



(c) Erreichbare OTTs

Abbildung 4.16: **Unabhängige Kabelbetreiber**, Ozeanien

4.1.3.2 Kritische Kabelpartner und Konsortien

Im vorangehenden Abschnitt wurden unabhängige Kabelbetreiber individuell nach deren Bedeutung für die Erreichbarkeit einzelner Kontinente untersucht. Erwartungsgemäß ist diese Bedeutsamkeit in hohem Maße abhängig von den Quellen und Zielen spezifischer Kommunikationsflüsse. Im Folgenden werden die bisher gewonnenen Einzelergebnisse nun zusammengetragen und daraus eine weltweite Einschätzung kritischer Kabelpartner und Konsortien abgeleitet. Mit dieser Analyse sollen insbesondere auch charakteristische Unterschiede der beiden wichtigsten Säulen der deutschen Internet-Infrastruktur, der Deutschen Telekom und des Internet Exchange Points DE-CIX, herausgearbeitet werden.

In den nachfolgenden Tabellen werden die über Kabelverbindungen erreichbaren weltweiten Autonomen Systeme und /24-Netzwerke für die zehn an der Weiterleitung meistbeteiligten Transit-ISPs zusammengefasst. Zudem wird der prozentuale Anteil der kabelabhängigen ASe global und nach Kontinenten gegenübergestellt. Diese Erreichbarkeitsanteile sind nicht kumulativ, da mehrere Transit-ISPs gemeinschaftlich an der Weiterleitung zu einzelnen Kontinenten beteiligt sein können oder konsortial im Betrieb spezifischer Kabelstrecken auftreten. Ebenfalls von Interesse ist die Anzahl der IP-Links mit Kabelbezug, die für den jeweiligen Transit-ISP aggregiert bewertet wurden. Diese geben einerseits ein Maß der Redundanz gegenüber einzelnen Router- oder Verbindungsausfällen an, andererseits lässt sich aus den vorhandenen Redundanzen auch die relative Wichtigkeit entsprechender Kontinentalverbindungen ableiten: je mehr individuelle IP-Links von Transitanbietern dafür vorgehalten werden, desto größer ist die Bedeutung für deren Netz. Schließlich wird über alle betrachteten CDNs und OTTs hinweg auch das jeweilige Maximum der Kabelerreichbarkeiten angegeben. Daraus werden weltweite Konsequenzen für Endanwender bei Wegfall einzelner Kabelpartner bzw. Störungen im Netz der Transit-ISPs ersichtlich.

Deutsche Telekom Aus Sicht der Deutschen Telekom sind 67% (46.476) aller weltweiten Autonomen Systeme per Kabel erreichbar, bei 25% (17.308) ist die Deutsche Telekom unmittelbar mit eigenen Kabelverbindungen an der Weiterleitung beteiligt. Für die interkontinentale Kommunikation zeigt sich eine breit angelegte Zusammenarbeit mit mehreren namhaften Tier1-ISPs (Abb. 4.17).

Transit-ISP	Land	ASe	/24-Netze	Links	Global	Europa	N.Amerika	S.Amerika	Asien	Afrika	Ozeanien	CDN	OTT
DTAG AS3320	DE	17.308	2.956.610	**39**	25%	10%	45%	36%	18%	24%	38%	↑40%	↑48%
NTT AS2914	US	7.659	1.091.365	**64**	11%	2%	15%	10%	32%	16%	21%	↑43%	↑17%
Seabone AS6762	IT	6.960	436.992	**207**	10%	4%	1%	28%	25%	33%	1%	↑37%	↑6%
Hurricane AS6939	US	6.479	329.093	**42**	9%	1%	16%	2%	18%	8%	71%	↑2%	↑0%
Telia AS1299	EU	5.960	771.994	**129**	9%	2%	10%	7%	21%	5%	46%	↑22%	↑4%
Cogent AS174	US	3.527	149.064	**54**	5%	2%	5%	15%	2%	6%	7%	↑2%	↑0%
Level3 AS3356	US	2.841	202.584	**77**	4%	2%	7%	6%	2%	3%	0%	↑12%	↑5%
RETN AS9002	EU	2.768	51.047	**45**	4%	9%	0%	0%	1%	0%		↑0%	↑0%
GTT AS3257	DE	2.615	129.154	**107**	4%	0%	5%	8%	5%	2%	2%	↑6%	↑17%
Level3 AS3549	US	2.010	21.914	**51**	3%	0%	0%	19%	0%	0%	0%	↑0%	

Abbildung 4.17: **Kabelerreichbarkeiten nach Transit-ISP**, DTAG

Wie bereits festgestellt sind Langstreckenkabel innerhalb Europas aufgrund engmaschiger Metronetze von untergeordneter Bedeutung. Für das Routing nach Nordamerika ist das TAT-14 Kabel angesichts der konsortialen Beteiligung der Deutschen Telekom ausschlaggebend. Weitere Kabelbeteiligungen von NTT und Hurricane, insbesondere angemietete Kapazitäten im AEC-1 Kabel des unabhängigen Betreibers Aqua Comms, tragen ebenfalls zur transatlantischen Konnektivität bei. Unabhängige Seekabel anderer Tier1-ISPs, darunter Yellow (Level3), TGN-Atlantic (Tata) oder Apollo (Vodafone), treten hingegen kaum in Erscheinung. Auch OTT-betriebene Kabel wie Grace Hopper (Google) oder MAREA (Facebook) sind für die Erreichbarkeit internationaler Netzbetreiber kaum relevant, gleichwohl sind diese transatlantischen Kabel für den Datenaustausch innerhalb der OTT-Netze natürlicherweise von großer Bedeutung. Für Südamerika tritt überwiegend das auf direktem Weg verlegte Atlantis-2 Seekabel unter DTAG-Beteiligung hervor, zudem ist Seabone mit indirekten Kabelstrecken über die USA und den dort anlandenden Seekabeln South American Crossing und Seabras-1 am Routing beteiligt. Asien ist aus Sicht der Deutschen Telekom in größerem Umfang über unabhängige Tier1-ISPs angebunden, darunter NTT, Seabone und Telia. Hierbei kommen häufig Kabel des SEA-ME-WE Kabelsystems über das Mittelmeer und den Nahen Osten bis in den indischen Ozean zum Zuge. Da der Suezkanal nicht für Seekabel geeignet ist, weisen alle Kabelverbindungen entlang dieses Weges eine terrestrische Teilstrecke über Ägypten auf[4]. Nordafrika ist naturgemäß ebenfalls über dieses Kabelsystem erreichbar. Gleichzeitig existieren zahlreiche Alternativstrecken über den Atlantik, wie bspw. die Gemeinschaftsprojekte SAT-3/WASC oder ACE, aber auch das von Google betriebene Equiano Kabel sowie 2Africa unter Beteiligung von Facebook. Das Routing nach Ozeanien erfolgt meist über die USA, sowohl durch die Deutsche Telekom selbst als auch unter Zuhilfenahme weiterer Tier1-ISPs, und von dort in der Regel mit dem Southern Cross Kabelsystem über Hawaii. Aus Sicht populärer CDNs/OTTs sind neben der Deutschen Telekom insbesondere auch Seabone, NTT und Telia von größerer Bedeutung, deren Kabelkapazitäten in hohem Maße zur Erreichbarkeit wichtiger Dienste beitragen. NTT weist dabei eine vergleichsweise geringe Zahl an redundanten IP-Verbindungen gegenüber den anderen Routing-Partnern auf. Weitere Tier1-ISPs – und unmittelbare Konkurrenten der Deutschen Telekom – wie GTT, Cogent und Level3 sind insgesamt kaum von Bedeutung, lediglich für Verbindungen von Nordnach Südamerika leisten die beiden letztgenannten einen nennenswerten Beitrag.

Einschätzung: Für Deutschland sind die unmittelbaren Kabelbeteiligungen der Deutschen Telekom von großer Bedeutung, denn diese leisten einen wichtigen Beitrag zur Unabhängigkeit von internationalen Transitanbietern. Ähnlich bedeutsam für die weltweite Konnektivität ist für DTAG-Kunden lediglich die Kooperation mit Seabone, der Transitsparte von Telecom Italia Sparkle. Dennoch ist durch breit angelegte Tier1-Kooperationen eine Aufrechterhaltung der internationalen Verbindungen auch bei gravierenden Kabelausfällen im Netz der Deutschen Telekom oder dem Netz anderer Partner sichergestellt.

DE-CIX Über den DE-CIX sind 27% (18.438) aller weltweiten Autonomen Systeme per Kabel erreichbar. Dabei ist jedoch anzumerken, dass über das Public Peering des Internet Exchange Point grundsätzlich nicht das gesamte Internet zu erreichen ist, sondern lediglich 44% (29.229) aller global gerouteten ASe. Hieraus ergibt sich ein mit der Deutschen Telekom vergleichbarer Kabelanteil von 63% (Abb. 4.18).

[4] `https://www.submarinenetworks.com/en/services/research/submarine-cables-crossing-egypt-and-cost`

Transit-ISP	Land	ASe	/24-Netze	Links	Global	Europa	N.Amerika	S.Amerika	Asien	Afrika	Ozeanien	CDN	OTT
DE-CIX AS6695	DE	10.479	308.245	**105**	15%	14%	1%	28%	33%	22%	3%	↑3%	↑2%
Hurricane AS6939	US	6.783	350.484	**42**	10%	2%	16%	2%	18%	20%	71%	↑2%	↑0%
Vocus AS4826	AU	749	20.847	**2**	1%	0%	0%		0%	0%	41%	↑1%	↑0%
GlobeNet AS52320	CO	641	7.622	**7**	1%	0%	0%	6%				↑2%	
AngolaC. AS37468	AO	495	8.235	**24**	1%	0%	0%	4%		4%		↑0%	
Seabras AS13786	US	431	3.240	**2**	1%	0%	0%	4%				↑0%	
IP-Conv. AS23930	PH	311	24.278	**2**	0%	0%	0%		3%			↑0%	↑0%
CAT Tel. AS4651	TH	244	10.587	**4**	0%	0%	0%		2%	0%	0%		↑0%
Liquid AS30844	GB	200	19.571	**8**	0%	0%	0%		0%	12%		↑0%	↑0%
TransTel. AS20485	RU	161	3.915	**8**	0%	0%	0%		0%			↑0%	

Abbildung 4.18: **Kabelerreichbarkeiten nach Transit-ISP**, DE-CIX

Aufgrund der heterogenen Natur des DE-CIX in Frankfurt mit über 750 direkt angebundenen Autonomen Systemen treten einzelne Transit-ISPs kaum hervor. Lediglich über Hurricane – als einziger Tier1-ISP auch Teilnehmer des Public Peerings – ist eine größere Zahl an Kabelverbindungen nach Afrika und Ozeanien zu verzeichnen. Für letztgenannte Region ist dementsprechend auch dessen australischer Kunde Vocus in größerem Maße sichtbar. Im Vergleich zur Deutschen Telekom liegt der Anteil an Kabeln im Routing für Europa etwas höher, da insbesondere zahlreiche osteuropäische ISPs am Internet Exchange Point präsent sind. Kabelstrecken nach Nordamerika hingegen werden fast ausschließlich über Hurricane eingebracht. Auffallend hoch ist der Anteil an Langstreckenkabeln in den Netzbereichen des DE-CIX nach Südamerika, Asien und Afrika. Dies lässt auf dort ansässige ISPs mit eigenen Points of Presence in Frankfurt schließen, weist aber auch auf einen zunehmenden Einsatz von Remote Peering Verbindungen über Drittanbieter und unabhängige Kabelbetreiber hin. Als wichtigster Vertreter entsprechender ISPs stellt Liquid Telecom angemietete Kabelverbindungen nach Afrika bereit, betreibt aber auch ein eigenes Landkabel von Ägypten bis Südafrika. Infolge der großen Diversität der IXP-Teilnehmer sind konkrete physische Kabel in der bestehenden Datenlage meist nicht zu erkennen. Dennoch ergeben sich allein aus der Vielzahl der Teilnehmer große Redundanzen gegenüber Kabelausfällen, während für einzelne ISPs – abgesehen von wenigen Ausnahmen – kaum redundanten Verbindungen festzustellen sind. Aus Sicht von CDNs/OTTs zeigen sich nur geringe Kabelabhängigkeiten. Dies bedeutet jedoch keineswegs fehlende Erreichbarkeit: vielmehr ist davon auszugehen, dass alle namhaften Content-Anbieter lokale Caches am IXP betreiben, die keinem direkten Einfluss von Langstreckenkabeln ausgesetzt sind.

Einschätzung: Die internationale Infrastruktur des DE-CIX stellt eine bedeutende Ergänzung zum Netz der Deutschen Telekom dar. Netzbetreiber, die Verbindungen zu beiden Infrastrukturen unterhalten, sind sowohl hinsichtlich Redundanz als auch Performanz bestens gerüstet – insbesondere CDNs und OTTs werden am DE-CIX unmittelbar erreicht. Die offene Peering Policy von Hurricane ist ebenso von Vorteil, sollte jedoch nicht als dauerhafte Gegebenheit angenommen werden. Aufgrund der zunehmend verteilten Natur des IXPs ist jedoch mit steigenden Langstreckennachteilen durch Remote Peering zu rechnen.

4.1.3.3 Fallbeispiel TAT-14

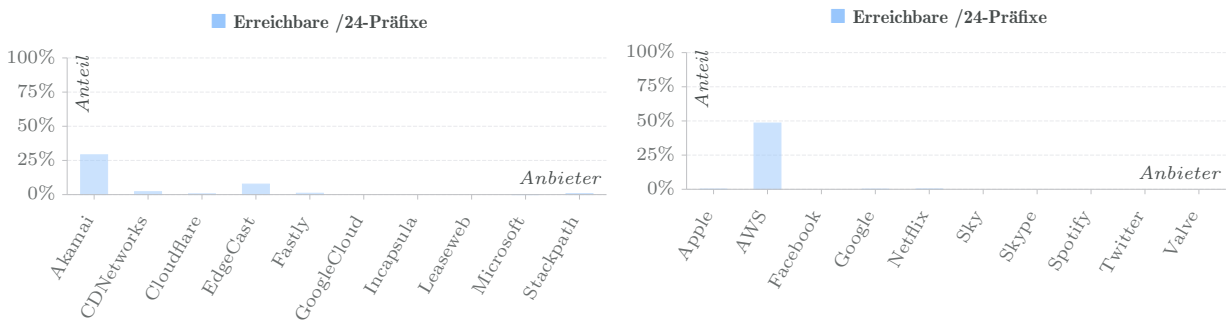
Um von Internet-weit erfassten IP-Verbindungen auf konkrete physische Kabelverbindungen schließen zu können, wird im Folgenden ein konstruktives Verfahren anhand des Fallbeispiels TAT-14 erarbeitet. Die dabei gewonnenen Daten und Erkenntnisse liegen ebenfalls den Betrachtungen eines fiktiven Kabelausfalls in Abschnitt 3.2 zugrunde.

Das transatlantische Seekabel TAT-14 wird unter konsortialer Beteiligung der Deutschen Telekom betrieben. Dementsprechend erfolgt zunächst eine statistische Analyse aller aus deren deutscher Infrastruktur heraus vermessenen IP-Links, die als Kabelverbindung eingestuft wurden und an der Weiterleitung zu Messzielen in Nordamerika beteiligt sind. Für die häufigsten IP-Adresspaare im Netzbereich der Deutschen Telekom treten hierbei vier DNS-Namen in Erscheinung, die die Kürzel `NYC` und `WAS` beinhalten. Diese Namensgebung weist auf Router mit Bezug zu New York City bzw. Washington hin, was sich auf die TAT-14 Anlandungspunkte Manasquan südlich von New York und Tuckerton östlich von Washington abbilden lässt. Um für weiterführende Analysen sicherzustellen, dass alle damit in Verbindung stehenden IP-Links berücksichtigt werden, werden weitere IP-Adressen durch manuelle Abfrage von A-Records für die vier identifzierten DNS-Namen bestimmt. Daraus ergeben sich die folgenden 174 IP-Adressen mit unmittelbarem Bezug zu Routern an den beiden US-amerikanischen Anlandungspunkten des TAT-14 Kabels:

- `nyc-sb5-i.NYC.US.NET.DTAG.DE` 69 IP-Addressen
- `nyc-sb6-i.NYC.US.NET.DTAG.DE` 36 IP-Addressen
- `was-sa2-i.WAS.US.NET.DTAG.DE` 40 IP-Addressen
- `was-sa3-i.WAS.US.NET.DTAG.DE` 29 IP-Addressen

Anhand der Umlaufzeiten aller zugehörigen IP-Links lässt sich zweifelsfrei feststellen, dass obige IP-Adressen stets am Ende des Kabels, d.h. in den USA, in Erscheinung treten. Für Router am deutschen Anlandungspunkt in Norden, Ostfriesland wurden zwar keine DNS-Namen vergeben, einer manuellen Recherche zufolge werden dort jedoch ebensfalls je zwei redundante Router für Verbindungen in beide Richtungen des ringförmigen Kabels, d.h. nach New York und Washington, betrieben. Für IPv6 konnten keine IP-Links mit Bezug zu TAT-14 bestimmt werden, hier dominieren Kabelverbindungen über Hurricane von London nach New York sowie über NTT von Frankfurt nach Ashburn und Newark.

Alle mit Hilfe der identifizierten IP-Adressen auffindbaren IP-Verbindungen können aus Sicht der Deutschen Telekom als vollständige Repräsentation des TAT-14 Kabels zusammengefasst und aggregiert bewertet werden. Insgesamt sind über diese jeweils zweifach redundanten Router-Verbindungen nach New York und Washington 7.821 Autonome Systeme und 58.769 IP-Präfixe erreichbar, anteilig betrachtet etwa 11,6% bzw. 7,3% aller global gerouteten Netzbereiche. In der Summe entspricht dies etwa einem /3,3-Netzwerk oder 15% des gesamten im Internet erreichbaren IP-Addressraumes. Erwartungsgemäß liegen diese Netzbereiche zum überwiegenden Teil in den USA, allerdings sind auch 578 der 7.342 brasilianischen Autonomen Systeme über das TAT-14 Kabel erreichbar. Dies steht im Einklang zu vorangehenden Ergebnissen, aus denen eine Weiterleitung nach Südamerika in Teilen über die USA hervorgeht. In Bezug auf populäre CDNs und OTTs zeigt die Auswertung der zugrundeliegenden IP-Verbindungen, dass 29% aller IP-Adressen von Akamai sowie 48% aller IP-Adressen von Amazon AWS über das Seekabel zu erreichen sind. Zudem werden 7% der IP-Adressen von Verizon EdgeCast sowie kleinere Netzbereiche von CDNetworks, Cloudflare und Fastly darüber geroutet (Abb. 4.19).



(a) Erreichbare CDNs (b) Erreichbare OTTs

Abbildung 4.19: **Kabelabhängigkeiten populärer Netzdienste**, TAT-14 Kabel

Vergleichbare Analyseversuche wurden auch für das Seekabel SEA-MA-WE-3, das von Europa über Atlantik und Mittelmeer nach Asien und Australien verläuft, durchgeführt. Da die Deutsche Telekom hier jedoch nicht an beiden Enden des Kabels agiert, sondern Verkehre vom Anlandungspunkt in Norden, Deutschland zum Teil direkt an benachbarte Autonome Systeme der weiteren – mit 38 äußerst zahlreichen – Anlandungspunkte übergibt, ist eine eindeutige Kabelzuordnung einzelner IP-Verbindungen nicht immer möglich. Auch eine Abgrenzung von anderen Kabeln des SEA-MA-WE Kabelsystems sowie weiterer parallel dazu verlaufender Kabel stellt aufgrund gemeinsamer Anlandungspunkte und unzureichender DNS-Daten größere Herausforderungen dar. Nichtsdestotrotz ist das erarbeitete Vorgehen im Grundsatz für eine umfassende Routing-Bewertung von europäischen und weltweiten See- und Landkabeln geeignet. Hierfür wären allerdings weitere Grundlagenarbeiten zur Router-Erkennung und ferner eine maschinelle Einbindung von geographischen Kabeldaten vonnöten. Dies übersteigt den Umfang der vorliegenden Studie und muss zukünftigen Arbeiten vorbehalten bleiben. Dennoch zeigen weiterführende, auch über die interaktive Projekt-Webseite abrufbare Ergebnisse zur fiktiven Betrachtung des Kabelausfalls in Abschnitt 3.2 vielversprechende Anknüpfungsmöglichkeiten.

Aktuelle Entwicklung Das TAT-14 Kabel wurde nach 19-jähriger Betriebszeit am 15. Dezember 2020 offiziell stillgelegt. Bis Ende 2021 erfolgt ein vollständiger Rückbau, um wertvolle Bestandteile des Kabels einer Wiederverwendung zuzuführen. Die Außerbetriebsetzung von TAT-14 zeigt sich auch anhand einer nach den obigen Vorgaben erneut durchgeführten DNS-Auswertung. Von den bisher 174 IP-Adressen der vier Kabel-Router wurden 48 IP-Adressen deaktiviert und 22 IP-Adressen neu in Betrieb genommen:

- `nyc-sb5-i.NYC.US.NET.DTAG.DE` 69 → 64 IP-Adressen (+11 | –16)
- `nyc-sb6-i.NYC.US.NET.DTAG.DE` 36 → 31 IP-Adressen (+4 | –9)
- `was-sa2-i.WAS.US.NET.DTAG.DE` 40 → 25 IP-Adressen (+1 | –16)
- `was-sa3-i.WAS.US.NET.DTAG.DE` 29 → 28 IP-Adressen (+6 | –7)

Bei genauerer Betrachtung ergibt sich, dass die Router nach wie vor in gleichem Maße an der Weiterleitung nach Nordamerika beteiligt sind. Über 80% des entsprechenden Messverkehrs wird nun allerdings über andere Interfaces geleitet als bisher. Dies weist darauf hin, dass die Deutsche Telekom zwar auf ein anderes Kabel ausweicht, die Router an den US-amerikanischen Anlandungspunkten als Teil der „Hauptverkehrsader“ jedoch weiterbetreibt. Da keine neuen Beteiligungen der Deutschen Telekom an transatlantischen Seekabeln bekannt wurden, ist hier von angemieteten Kapazitäten auszugehen. Mit der Stilllegung des TAT-14 Kabels geht somit auch ein gewisser Verlust der Unabhängigkeit des Wirtschaftsstandortes Deutschland von internationalen Kabelbetreibern einher.

4.2 Verbesserung der Widerstandsfähigkeit

Im Rahmen der vorangehenden Analysen wurden internationale Kabelabhängigkeiten datengestützt identifiziert und hinsichtlich ihrer Bedeutung für die deutsche Internet-Infrastruktur bewertet. Im Folgenden werden die gewonnenen Erkenntnisse zusammengeführt und reale Kabelbeschädigungen des Vorfallskatalogs (siehe Abschnitt 2.1.2.4) in diesem Kontext erneut betrachtet. Eine Übersicht über relevante Forschungsarbeiten, die im Zusammenhang zu internationalen Kabelverbindungen stehen, schließt das Kapitel ab.

4.2.1 Empirische Erkenntnisse

Die Deutsche Telekom und der Internet Exchange Point DE-CIX stellen zweifelsohne die wichtigsten beiden Eckpfeiler der deutschen Internet-Infrastruktur dar. Interessanterweise verfügen beide Plattformen jedoch über gänzlich verschiedene Anbindungscharakteristiken. Mit 600 bzw. 750 Kunden liegen die Anbieter zwar in derselben Größenordnung, unterscheiden sich aber in ihrer auf kostenpflichtigen Transit bzw. kostenneutrales Peering fokussierten Dienstleistung. Diese ungleiche Ausrichtung äußert sich bereits darin, dass fast 150 Netzbetreiber gleichzeitig als Kunde beider Anbieter auftreten – mit steigender Tendenz. Aber auch hinsichtlich kritischer Kabelabhängigkeiten, Redundanzen und Erreichbarkeiten populärer CDNs und OTTs ergeben sich bedeutende Unterschiede.

Zunächst ist festzuhalten, dass die mit der vorgestellten Messmethodik identifizierten Kabelabhängigkeiten weltweiter Netzbereiche bei Ausfällen nicht zwangsläufig zu Unerreichbarkeiten führen, da meist auf redundante Kabelstrecken ausgewichen werden kann. In vielen Fällen würden dennoch Störungen als Folge von unzureichend ausgelegten Ausweichkabeln auftreten, die den zusätzlichen Verkehr nicht vollständig aufnehmen können. Da aus deutscher Perspektive über zwei Drittel der globalen Internet-Teilnehmer per Langstreckenkabel zu erreichen sind, ist das Risiko für Dienststörungen entsprechend hoch. Entgegen der Erwartung sind auch die Netzbereiche nahezu aller populären Content-Dienste größerenteils – im Maximum mit 67–71% – über Kabel angebunden, auch wenn der Durchschnitt über alle betrachteten CDNs und OTTs mit 39% bzw. 25% im eigenen Interesse der Anbieter geringer ausfällt. Ein wesentlicher Teil dieser stark frequentierten Netzwerke ist auf die USA registriert, allerdings sind „out-of-region“-Einsätze in anderen Teilen der Welt gängige Praxis. Somit ergibt sich für populäre Netzbereiche auch keine unmittelbare Korrelation zwischen Registrierungsländer und den dorthin beobachtbaren Kabelverbindungen. Analog dazu werden die in Europa registrierten Netzbereiche keineswegs nur regional und damit unabhängig von Langstreckenkabeln eingesetzt.

Weitere Ergebnisse der Kabelanalyse zeugen von einer hohen Redundanz für wirtschaftlich oder politisch bedeutsame Länder. Jedoch zeigt sich auch, dass abgelegene und strukturell schwächere Regionen über deutlich weniger redundante Kabelverbindungen verfügen und in gleichem Maße anfälliger für Kabelausfälle sind. Dies betrifft in erster Linie den afrikanischen Kontinent, aber auch größere Teile von Asien und Südamerika. Im Netz der Deutschen Telekom ergeben sich redundante Kabelstrecken durch konzerneigene Kabelbeteiligungen sowie durch Kooperationen mit wenigen international operierenden Tier1-ISPs. Am DE-CIX ist die Bedeutung einzelner ISPs deutlich geringer, hier resultieren Redundanzen vorrangig durch die Heterogenität der zahlreichen IXP-Teilnehmer aus

allen Regionen der Welt. Deutschland und Europa nehmen aufgrund einer hohen Flächennutzung und der damit verbundenen geringen Abhängigkeit von Langstreckenkabeln eine besondere Stellung ein: infolge des äußerst hohen Vermaschungsgrades ist die Eintrittserwartung gravierender innereuropäischer Kabelstörungen vergleichsweise gering.

Die Kabelbeteiligungen der Deutschen Telekom sind von großer Bedeutung für die Unabhängigkeit der deutschen Internet-Infrastruktur. Hierunter zählen insbesondere die transatlantischen Seekabel TAT-14 (mittlerweile stillgelegt) und Atlantis-2 sowie das SEA-ME-WE-3 Kabel über das Mittelmeer nach Asien. Bei Ausfall eines dieser Kabel kann jedoch jederzeit auf ausgedehnte Peering-Verbindungen zu allen Tier1-ISPs – und somit unmittelbar auf deren eigene Langstreckenkabel – ausgewichen werden. Je nach Schwere der Störung bzw. Zahl der betroffenen Endkunden können Verkehrsumleitungen allerdings zu Überlastsituationen im Netz der Peering-Partner führen. Ungeachtet dessen sind Tier1-Verbindungen regionsabhängig auch im störungsfreien Betrieb unentbehrlich, insbesondere Kabelstrecken von NTT und Telia nach Asien sowie von Hurricane und Telia nach Australien. Gleiches gilt für den ukrainischen Transitanbieter RETN und dessen Landkabel nach Osteuropa und Russland. Hingegen sind weitere prominente Tier1-ISPs, wie Cogent, Level3 und GTT, in Bezug auf kritische Kabelabhängigkeiten weniger bedeutsam und tragen nur abschnittsweise zur Weiterleitung nach Nord- oder Südamerika bei.

Über die GlobePEER-Plattform des DE-CIX stehen (angemietete) Kabelkapazitäten für alle IXP-Teilnehmer zur Verfügung. Dies gilt im Besonderen für Verbindungen zwischen den weltweiten Standorten des DE-CIX, wodurch MPLS-Tunnel in die USA sowie nach Russland, Indien und Singapur geschaltet werden können. Durch eine Partnerschaft mit dem Seekabelbetreiber Seaborn wurde kürzlich auch der Grundstein für Verbindungen nach Südamerika gelegt. Darüber hinaus steht in den anbieterneutralen Rechenzentren des DE-CIX eine Vielzahl von unabhängigen Transportpartnern für die Weiterleitung in alle Regionen der Welt bereit. Ungeachtet dessen kann allein über das Public Peering des DE-CIX in Frankfurt bereits nahezu die Hälfte des globalen Internets kostenneutral erreicht werden. Hurricane, und in geringerem Maße auch der indische ISP Bharti, nehmen eine Sonderstellung als Tier1-ISPs im Public Peering ein. Zudem bedrängt Hurricane den Markt am IXP mit kostenlosem IPv6-Transit. Die hohe Diversität der ca. 750 Teilnehmer ermöglicht Weiterleitungen über zahlreiche unterschiedliche Kabelverbindungen und trägt damit wesentlich zur redundanten Internet-Anbindung Deutschlands – vor allem für die Nordhalbkugel – bei. Nicht zu vernachlässigen sind jedoch suboptimale Interkontinentalpfade, die aus dem zunehmenden Einsatz von Remote Peering resultieren können.

Die vorgestellte Methodik zur Bewertung kritischer Kabelbetreiber eignet sich grundsätzlich auch für die Untersuchung von konkreten physischen Kabeln. Ein expliziter Analyseansatz wurde hierzu am Fallbeispiel des TAT-14 Seekabels vorgestellt. Anhand dieser Studie konnte gezeigt werden, dass sich Redundanz auch für einzelne Kabelverbindungen herstellen lässt. Die Ausfallsicherheit der TAT-14 Infrastruktur wird dabei durch mehrere Anlandungspunkte und Router wesentlich erhöht. Störungen auf Kabelstrecken können so zwar nicht ausgeschlossen werden, durch die ringförmige Verlegung von TAT-14 zwischen Nordamerika und Europa ist jedoch zusätzliche Redundanz vorhanden. Mit der Stilllegung des TAT-14 Kabels Ende 2020 konnten im Rahmen der Fallstudie auch damit einhergehende Routing-Änderungen im Netz der Deutschen Telekom untersucht werden.

Limitierungen der angewandten Methodik bestehen in Bezug auf innereuropäische Kurzstreckenkabel und Metronetze, die aufgrund äußerst niedriger Latenzen kaum von

Patch- bzw. Switch-Verbindungen zu unterscheiden sind. In zukünftigen Arbeiten ließen sich hierzu topologische und geographische Gesichtspunkte mit berücksichtigen. Weitere Anknüpfungspunkte ergeben sich aus steten kurz- und längerfristigen Änderungen in der Routing-Landschaft, die einer kontinuierlichen Beobachtung bedürfen – sowohl im Hinblick auf nationale Transitanbieter als auch bedeutsame CDNs und OTTs. Zudem erscheint eine tiefergehende Analyse der Infrastruktur direkter Nachbarländer hinsichtlich deren Anlandungspunkte für kritische Seekabel zweckmäßig. Auch mögliche Konsequenzen einer dauerhaften Stilllegung von Kabelstrecken – wie am Fallbeispiel TAT-14 aufgezeigt – sollten untersucht werden. Generell besteht die Gefahr, dass sich Verkehre durch infrastrukturelle Änderungen zu Ungunsten der deutschen Internet-Infrastruktur verlagern.

4.2.2 Reale Kabelbeschädigungen

Anhand der Auswertung von realen Internet-Vorfällen (siehe Abschnitt 2.1.2.4) wurde deutlich, dass physische Kabelbeschädigungen infolge unvermeidlicher Umwelteinflüsse und insbesondere durch menschliche Einwirkungen – wie Bauarbeiten, Fischerei oder Sabotage – die häufigsten Ursachen für den Ausfall von Langstreckenkabeln darstellen. Während die Hintergründe in der Regel zwar öffentlich bekannt werden, lassen sich konkrete Auswirkungen auf die Internet-Infrastruktur meist nur anekdotisch nachvollziehen. Mit Hilfe der vorgestellten Analysemethodik wurde jedoch aufgezeigt, dass eine unzureichende Informationslage bei Kabelstörungen anhand von messbasierten Beobachtungen wesentlich verbessert werden kann. Um in angepasster Weise auf Ausfälle zu reagieren, könnten entsprechende Messdaten zukünftig dauerhaft erhoben und nutzbar gemacht werden.

Die Ergebnisse der fallbezogenen Betrachtungen legen nahe, dass wirtschaftlich schwache und abgelegene Regionen in besonderem Maße durch Kabelbeschädigungen gefährdet sind, da sich Netzinfrastrukturen in weitläufigen Gebieten nicht vollständig überwachen und nur mit hohem Kostenaufwand vor äußeren Einflüssen schützen lassen. Die datengestützte Analyse weltweiter Kabelverbindungen zeigt zudem, dass gerade diese Regionen wesentlich geringere Kabelredundanzen aufweisen und Störungen somit noch wahrscheinlicher werden. Gleichzeitig drohen durch singuläre Ausfallpunkte auch Totalausfälle in der Internet-Anbindung ganzer Landstriche. Diese Umstände spiegeln sich im Vorfallskatalog unmittelbar wider: nahezu alle betrachteten Ausfälle mit gravierenden Auswirkungen fanden in Entwicklungsländern statt. In Anbetracht der meist langwierigen Reparaturarbeiten sind diese Länder demnach einem hohen infrastrukturellen Risiko ausgesetzt, wodurch sich dort wie gezeigt auch kaum weltweit populäre Dienste ansiedeln. Handlungsdruck für hochentwickelte Industrienationen kann daher nur durch politische Bemühungen entstehen, wie das Beispiel der „digitalen Seidenstraße“ [5] Chinas eindrucksvoll demonstriert.

Folgenschwere Internet-Störungen sind für Europa und insbesondere auch für Deutschland nicht zu erwarten. Die Deutsche Telekom und der Internet Exchange Point DE-CIX ergänzen sich in idealer Weise und tragen unabhängig voneinander zur Resilienz der deutschen Internet-Infrastruktur bei. Auch ein hoher Vermaschungsgrad als Folge der zahllosen Kurzstreckenverbindungen und Metronetze trägt wesentlich zur Robustheit des Internets in Europa bei. Mit kleineren Kabelbeschädigungen und damit einhergehend regionalen Ausfällen ist nichtsdestotrotz zu rechnen. Aber auch ernstzunehmende Kabelstörungen

[5] https://www.gtai.de/gtai-de/trade/specials/special/china/china-hegt-expansive-plaene-fuer-die-digitale-seidenstrasse-586502

mit weitreichenderen Auswirkungen auf Deutschland und Europa sind belegt. So kam es allein für das in der vorangehenden Fallstudie betrachtete TAT-14 Seekabel, das unter Beteiligung der Deutschen Telekom transatlantische Konnektivität herstellt, zu drei voneinander unabhängigen Ausfällen. Mehrere technische Defekte in den Jahren 2003 [6] und 2008 [7] zogen Verbindungsprobleme in die USA nach sich, auch ein Software-Problem des Konsortialpartners Telia im Jahr 2014 [8] führte zu merklichen Beeinträchtigungen.

Die im Vorfallskatalog betrachteten Kabelausfälle zogen bisher überwiegend Probleme im Internet-Backbone nach sich. Durch die zunehmende Wichtigkeit von CDN- und OTT-Diensten – und dem voranschreitenden Aufbau neuer Langstreckenkabel durch die Anbieter selbst – werden Abhängigkeiten von Kabelverbindungen zukünftig weiter zunehmen und Redundanzen zwangsläufig abnehmen. Aktuell vorherrschende Trends hinsichtlich lokaler Content-Caches können dieser Entwicklung nur bedingt entgegenwirken, da deren Synchronisierung bei längerfristigen Kabelausfällen ebenfalls beeinträchtigt wird und Anbieter-interne Kommunikationsstörungen auch gravierende Konsequenzen nach sich ziehen können. Der in Abschnitt 2.2.5 untersuchte Totalausfall des verteilten CDNs von Cloudflare [I13] macht die mit zentralen Steuersystemen verbundenen Risiken deutlich.

4.2.3 Wissenschaftliche Arbeiten

Auf dem Gebiet internationaler Kabelverbindungen existieren vielfältige weiterführende Forschungsarbeiten, die relevant für eine Verbesserung der Widerstandsfähigkeit der deutschen Internet-Landschaft sind. Diese Arbeiten untergliedern sich in praxisbezogene Ausfallstudien, verbesserte Infrastrukturen sowie Mitigationsstrategien bei Störungen.

Empirische Ausfallstudien Zahlreiche verwandte Arbeiten tragen anhand empirisch gewonnener Erkenntnisse zu einem besseren Verständnis von Kabelverbindungen und den damit verbundenen Ausfallrisiken in der Internet-Infrastruktur bei. So stellt [58] ein Modell zur empirischen Bewertung der Widerstandsfähigkeit transozeanischer Seekabel basierend auf Nachfrage, Kapazitäten und Flussinformationen anhand fiktiver Störungen vor. In [59] wird der Einfluss von Katastrophen auf die Leistungsfähigkeit des Internets am Beispiel eines realen Ausfalls erforscht. Basierend auf Erkenntnissen über das große Erdbeben in Japan im Jahr 2011 werden in [60] Folgeschäden für die Telekommunikationsinfrastruktur aufgezeigt und zukünftige Gegenmaßnahmen diskutiert. Anstelle von Ausfällen in bestehenden Kabelverbindungen untersucht [61] mittels aktiver IP-Pfadmessungen negative Auswirkungen auf Netzdienste beim Aufbau eines neuen Seekabels im Südatlantik.

Risiko-minimierte Kabelverlegung Neben Studien zu konkreten Ausfällen existiert auch eine Vielzahl von Arbeiten in Bezug auf eine möglichst ausfallsichere Kabelverlegung. In [62, 63] werden Methoden untersucht, um die Robustheit von Unterseekabeln gegenüber Umwelteinflüssen und menschlichen Einwirkungen zu erhöhen. Weiterführende Planungsstrategien werden in [64, 65] erarbeitet, um bei der Verlegung von Seekabeln das Kosten/Nutzenverhältnis mit Blick auf die Widerstandsfähigkeit gegenüber Erdbeben zu optimieren. Mit ERBON [66] wird ein Modell vorgeschlagen, mit dessen Hilfe die Auswirkungen von Erdbeben auf optische Kabel bewertet werden können. Ergänzend hierzu lässt

[6] https://groups.google.com/g/alt.internet.providers.uk.aaisp/c/tSLawRAmVzU
[7] https://heise.de/-192266
[8] https://www.capacitymedia.com/articles/3343798

sich mittels SZANR [67] abwägen, ob eine Verlegung bestehender Seekabelkomponenten in seismisch weniger aktive Regionen sinnvoll ist, um deren Widerstandsfähigkeit zu erhöhen. In [68] werden erweiterte Planungsstrategien für die Verlegung von Langstreckenkabeln untersucht, die neben Ausfallrisiken selbst auch das Risiko für Verlegefahrzeuge minimieren sollen, gleichzeitig aber weitere Rahmenbedingungen für Kabelverbindungen wie Kosten und Leistung einbeziehen. Zuletzt werden in [69] bestehende Arbeiten zur Verlegung von Seekabeln unter expliziter Berücksichtigung von Kabelverzweigungen weiterentwickelt.

Ausfalltolerantes Backbone-Design Anstelle von Prävention wird in [70] diskutiert, wie Netzwerke und Cloud-Infrastrukturen kurzfristig auf vorhersehbare Katastrophen und kaskadierende Ausfälle vorbereitet werden können, um ausreichend Ressourcen für die Aufrechterhaltung des Betriebs sicherzustellen. Darüber hinaus existiert mit RECODIS [71, 72] ein Programm, das die Internet-Anbindung von Endnutzern im Katastrophenfall aufrechterhalten und Auswirkungen auf umliegende Gebiete minimieren soll. In [73] wird ein Modell vorgestellt, das basierend auf Erdbebenwahrscheinlichkeiten den Aufbau von zusätzlichen Verbindungen empfiehlt, um die Auswirkungen von Erdbebenschäden auf das Gesamtnetz zu minimieren. Eine Aufarbeitung bestehender Arbeiten zum Thema Schutz, Wiederherstellung und Auswirkung von Katastrophen für optische Kabelverbindungen [74] unterstreicht Herausforderungen in Bezug auf deren Resilienz.

Data Evacuation Maßnahmen Neben dem Schutz von Infrastrukturen beschäftigen sich mehrere Arbeiten auch mit konkreten Maßnahmen, die Datenverlust im Ernstfall verhindern und somit die Verfügbarkeit von Netzdiensten sicherstellen sollen. Eine Heuristik zur schnellen Evakuierung großer Datenmengen in sichere Gebiete unmittelbar vor Eintritt einer vorhersehbaren Katastrophe wird in [75] vorgestellt. Auch [76] beschreibt eine Strategie für Notfall-Backups über vernetzte Datenzentren, durch die auf bevorstehende Ausfälle reagiert werden kann. Um Daten während einer Katastrophe zu evakuieren, wird in [77] ein reaktiver Ansatz konzipiert, der die Internet-Anbindung abgeschnittener Gebiete über Satellit aufrechterhält. Ergänzend dazu zeigen [78, 79] auf, wie Datenzentren im Nachgang von Katastrophen schnell wieder in Betrieb genommen werden können.

Reaktive Umleitungen In [80] wird ein heuristischer Routing-Algorithmus vorgestellt, der geographische Epizentren von Ausfällen in der Verkehrsweiterleitung meidet und so die Konnektivität von nicht unmittelbar betroffenen Netzbereichen sicherstellt. Weitere Umleitungsstrategien, die Überlastsituationen auf alternativen Routen verhindern sollen, werden in [81] untersucht. Mit [82] erfolgt ferner eine Analyse der Ausbreitungsmuster von Ausfällen, um Wiederanlaufphasen für Energie- und Wasserversorgungen unter bewusstem Einbezug von Abhängigkeiten zu kritischen Netzinfrastrukturen zu verbessern.

Zusammenfassend lässt sich festhalten, dass in der jüngeren Forschung zahlreiche, auch auf Wirtschaftlichkeit bedachte Methoden für den Aufbau von ausfalltoleranten Kabelinfrastrukturen zur Verfügung stehen, die bei der Verlegung zukünftiger See- und Landkabel berücksichtigt werden können. Um Störungen in bereits bestehenden Kabelsystemen abzumildern, kommen für kritische Netzwerke auch Notfalllösungen, wie die Bereitstellung von Satellitenverbindungen, in Betracht. Für nicht unmittelbar betroffene Netzbetreiber lassen sich zudem Routing-Notfallstrategien vorbereiten, die eine kurzfristige Umleitung um beeinträchtigte Netzwerke ermöglichen. Aufgrund der zunehmenden Verbreitung von Cloud-Infrastrukturen liegt das größte Schutzpotential jedoch in einer Spiegelung – oder nötigenfalls reaktiven Relokation – von kritischen Daten und Diensten.

4.3 Zusammenfassung

Mit den Arbeiten in diesem Kapitel wurde der Grundstein für eine messgestützte Analyse internationaler Kabelverbindungen gelegt. Anhand des erarbeiteten Verfahrens lassen sich Dienstgüten abschätzen, globale Abhängigkeiten bestimmen und Kabelredundanzen bewerten. Mit Hilfe geeignet positionierte Messstandorte konnten konkrete Einblicke in die Diversität der deutschen Internet-Landschaft gewonnen werden. Dabei wurde insbesondere zwischen den wichtigsten Eckpfeilern der nationalen Kommunikationsinfrastruktur, der Deutschen Telekom und dem DE-CIX, differenziert. Aus deren technisch wie ökonomisch gegensätzlicher Ausrichtung ergeben sich vorteilhafte Synergien für den Internet-Standort Deutschland bzgl. Dienstgüte und Ausfallsicherheit. Dennoch nehmen infrastrukturelle Risiken infolge grundlegender Veränderungen des weltweiten Internet-Marktes zu.

Anhand der messbasierten Analysen wurden mehr als 2.000 Kabelabschnitte erkannt, über die von Deutschland aus 74% aller weltweiten Netzbetreiber und 69% der globalen Netzbereiche zu erreichen sind. Weiterhin konnten Betreiber besonders wichtiger Kabelverbindungen identifiziert und Abhängigkeiten nach Weltregion quantifiziert werden. Im Rahmen der Analysen zeigten sich unerwartet hohe Kabelanteile für populäre Content Delivery Networks und Over-The-Top-Anbieter. Zudem wurde anhand einer Fallstudie über das TAT-14 Seekabel deutlich, dass diese – mittlerweile stillgelegte – transatlantische Verbindung mit eigenem Anlandungspunkt in Deutschland einen wertvollen Beitrag zur Unabhängigkeit der deutschen Internet-Infrastruktur leistete. Kritische Kabelverbindungen, von Konsortien mit dutzenden Mitgliedern betrieben, werden der aktuellen Marktsituation jedoch kaum mehr gerecht. Der Trend neuer Kabelprojekte [9] weist auf Kleinstkooperationen mit dominierenden Content-Anbietern. Die Sicherstellung weltweiter Konnektivität hingegen tritt zunehmend hinter die prioritäre Bereitstellung kommerzieller Masseninhalte zurück. Dies wird insbesondere für Entwicklungsländer immer mehr zum Problem, wo generell kaum redundante Kabelverbindungen vorhanden sind und somit Totalausfälle noch wahrscheinlicher werden. Ungeachtet dieser Verschiebungen in tradierten Konsortialmodellen arbeitet die Wissenschaft kontinuierlich an ausfallsichereren Kabelverbindungen. Fundiertes Wissen um häufige Störfälle und deren Ursachen ermöglicht risikoärmere Kabelstrecken und speist die Entwicklung vielfältiger Mitigationsmaßnahmen. Nicht zuletzt im Hinblick auf große Reparaturaufwände und Folgeschäden treten Wirtschaftlichkeit und Robustheit – auch für bestehende Kabelverbindungen – vermehrt in den Vordergrund.

Einschätzung: Zwar ist zu erwarten, dass durch zukünftigen Kabelausbau und wissenschaftliche Fortschritte die Robustheit der deutschen Internet-Landschaft nicht abnimmt. Gleichzeitig steigt jedoch deren Schutzbedarf infolge kontinuierlich wachsender Anforderungen an Bandbreiten und Verfügbarkeit sowie der Diversifizierung der Kabelbetreiber. Alternativen wie das Starlink Satellitennetzwerk werden den Bedarf an ausfallsicheren Kabelverbindungen zumindest mittelfristig nicht wesentlich mindern, weshalb Schutz und Überwachung von bestehenden Kabelverbindungen sowohl physisch als auch mit Hilfe von messgestützten Analysen wichtige Bausteine für eine robuste Internet-Infrastruktur bleiben werden. Die technischen Voraussetzungen dazu sind auch unter Berücksichtigung von Aspekten der Wirtschaftlichkeit durchaus vorhanden. Entscheidungen über deren konsequenten Einsatz sollten nichtsdestotrotz politisch flankiert werden – bspw. im Rahmen von regulatorischen Maßnahmen oder staatlichen Kabelbeteiligungen.

[9] https://www.submarinenetworks.com/en/insights/old-cables-don-t-die-but-do-they-just-fade-away

Kapitel 5
Änderungen in der Internet-Infrastruktur

5.1 Übersicht: Begrifflichkeiten, Grundprinzipien und Trends

Der Begriff *Internet-Infrastruktur* bezeichnete ursprünglich die Routing-Infrastruktur, die das Weiterleiten von Daten über Grenzen von autonomen Systemen hinweg ermöglicht. Über die letzten 10 bis 15 Jahren hat sich dieser Begriff erweitert und schließt Kerndienste, die von den meisten Anwendungen oberhalb des Internets genutzt werden, ein. Jari Arko, ehemaliger Chair der IETF, definiert die Internet-Infrastruktur als „die Elemente der technischen Infrastruktur, die notwendig sind, um Anwendungen oberhalb dieser Schicht zu ermöglichen.“ [83] Demnach sind Anwendungen selber nicht Teil der Internet-Infrastruktur, aber „Paket-Forwarding, Routing, Namensauflösung genauso wie Zertifizierungsstellen; alle Elemente, die eine HTTPS-Verbindung Ende-zu-Ende zwischen Hosts ermöglichen“ [83].

Das Internet ist seit seinen Anfängen ein dezentrales System, welches durch seine Offenheit Heterogenität nicht nur bezüglich der eingesetzten Technologien, sondern auch bezüglich des Betriebs der Infrastruktur fördert. Tatsächlich besteht aber eine Wechselwirkung zwischen dem Grad an Heterogenität der Betreiber und der langfristigen Innovationsskraft der Internet-Infrastruktur. Eine Änderung hin zu einer konsolidierten Infrastruktur, die von einigen wenigen Betreibern dominiert wird, verhindert langfristig die Entwicklung neuer Dienste, die breites Gemeinwohl erzeugen können, da zum einen die Konkurrenzsituation verringert wird, zum anderen der Martkeintritt für nicht etablierte Firmen schwieriger ist.

In den letzten 15 Jahren fand eine ursprünglich schleichende, nun zunehmend offensive Konsolidierung der Internet-Infrastruktur statt. Dies betrifft insbesondere Dienste, die erst später zur Internet-Infrastruktur gezählt wurden, wie die Namensauflösung, Zertifizierungsstellen und Content Delivery.

Abb. 5.1 zeigt für einen Internet-Austauschpunkt beispielhaft die Auswirkungen aufgrund von Konsolidierungen der Dienstleister für die Verteilung von populären Inhalten. Dargestellt ist das Verkehrsvolumen des DE-CIX am Standort Frankfurt, wobei zwischen dem mittleren Datenaufkommen (gelb) und der Peak-Datenrate (rot) unterschieden wird. Das Verkehrsaufkommen ist in den letzten Jahren deutlich gestiegen, insbesondere im Jahr 2020 hat die Zunahme von Home Office u.ä. durch die Corona-Pandemie zu erheblich höheren Peak-Datenraten geführt. Dennoch ist es auffällig, dass die Datenraten innerhalb eines Jahres erheblich schwanken. Im Jahr 2020 hängen die Verkehrsschwankungen

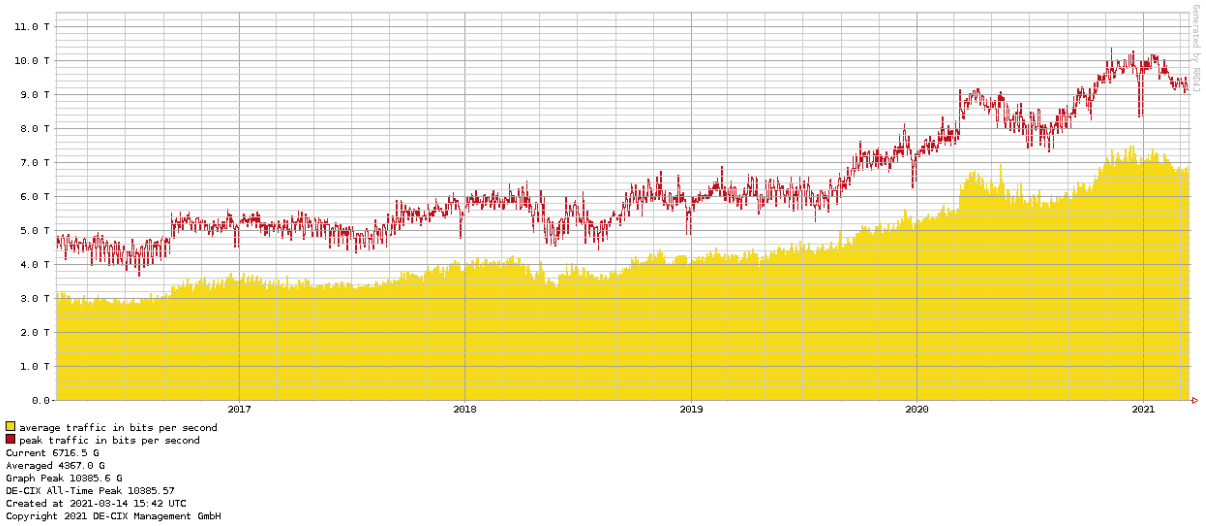


Abbildung 5.1: Verkehrsaufkommen der letzten 5 Jahre am DE-CIX (Quelle: DE-CIX Webseite). Abfall der Peak-Datenrate um ca. 1 Tbit/s von Januar zu Februar 2021.

vermutlich mit den pandemiebedingten Einschränkungen und Lockerungen zusammen. Von Januar zu Februar 2021 sinkt die Peak-Datenrate aber um ca. 1 Tbit/s, obgleich die äußeren Randbedingungen unverändert sind. Hierfür gibt es zwei Möglichkeiten. (*i*) Viele Internet-Dienstleister am DE-CIX entscheiden sich gegen ein Routing über Frankfurt. (*ii*) Ein einzelner Dienstleister verändert sein Routing. Fall (*i*) würde ein diverses Internet widerspiegeln, wie es den Grundprinzipien, die den Entwurf von Internet-Protokollen antreiben, entspricht [84]. Fall (*ii*) würde ein Anzeichen von Konsolidierung bedeuten, da ein einzelner Akteure erheblichen Einfluss auf einen wichtigen internationalen Internet-Austauschpunkt hat. Wichtig ist, in dieser Diskussion auch nicht-technische Argumente zu berücksichtigen. Verkehrsvolumen werden oft als Marketing-Instrument von Internet-Austauschpunkten genutzt, um die eigene Bedeutung zu unterstreichen: Bei einem hohen Datenvolumen ermöglicht der Austauschpunkt viel Internet-Verkehr, insofern ist er relevant. In diesem konkreten Fall vermuten wir nach Rücksprache mit Internet-Betreibern Fall (*ii*), voraussichtlich durch die Änderungen im Routing eines großen Content Delivery Networks, das Mitglied am DE-CIX ist.

5.1.1 Gründe für die Beförderung von Konsolidierung

> „Many members of the Internet community would argue that there is no architecture, but only a tradition, which was not written down for the first 25 years (or at least not by the IAB). However, in very general terms, the community believes that the goal is connectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network.“
>
> — Brian E. Carpenter (Ed.) [84]

Die Standardisierungsaktivitäten in der IETF sind grundsätzlich getrieben von dem Gedanken, Konnektivität in einem heterogenen Netz unterschiedlicher Akteuere zu ermög-

lichen. Die Kernprotokolle im Internet sind derart entworfen, dass sie Konsolidierungen nicht befördern, aber auch nicht inhärent verhindern.

Nicht technische Lösungen haben in den letzten Jahren Konsolidierungs- und Zentralisierungsbestrebungen befördert, sondern Geschäftsinteressen. Umgekehrt wirken Geschäftsinteressen auch in die Standardisierung von technischen Lösungen, z.B. durch das Engagement von Firmenvertretern in der IETF. Sie können so bedingten Einfluss auf Lösungen nehmen, um Konsolierungen zu erleichtern.

Als Beispiel können QUIC und DNS über HTTPS dienen. QUIC, ursprünglich *QUIC UDP Interconnect*, war ein von Google entworfenes Transport-Protokoll, das die Web-Kommunikation beschleunigen und privatsphären-freundlich gestalten sollte. Obgleich es seit vielen Jahren einen Deployment-Rückstau von neuen Transportprotokollen gab, hat sich QUIC zeitnah verbreitet, da Google sowohl die Server-Infrastruktur (Suchmaschinen und YouTube) als auch die Clients (Google Chrome) kontrolliert. Neben Leistungsverbesserungen gegenüber TCP/HTTP sorgt QUIC aber auch für eine Verschleierung von Meta-Informationen, wodurch mehr Informationen gegenüber Internet Service Providern verborgen werden und die Rolle von Anwendungsprovidern gestärkt wird. Trotz der Möglichkeit einer unmittelbar hohen Verbreitung hat Google QUIC in der IETF zur Diskussion gestellt, worauf die QUIC-Arbeitsgruppe gegründet wurde. Das dort definierte QUIC-Protokoll weist erhebliche Abweichungen zu Google QUIC auf. Dies zeigt zweierlei: Es gibt ein bestehendes (und erprobtes) Umfeld, um Innovationen gemeinschaftlich erfolgreich zu bearbeiten. Hätte Google hingegen QUIC nicht zur Diskussion gestellt, wäre das Protokoll weniger innovativ im Vergleich zum jetzigen Standard.

DNS über HTTPS (DoH) ist ein weiteres Beispiel, in dem Geschäftsinteressen, technische Lösungen und gesellschaftliche Perspektiven wechselwirken und Änderungen der Internet-Infrastruktur zur Folge haben. Nach den Überwachungsenthüllungen durch Edward Snowden hat die IETF vermehrt Protokolle gefördert, die Überwachungen erschweren. DoH stellt die Geheimhaltung zwischen DNS Client und Recursive Resolver sicher. Gleichzeitig verändert der Einsatz des Protokolls aber die Hoheit darüber, welchen Resolver ein Client verwendet, da DoH die Nutzung von Recursive Resolvern von Webdienstleistern befördert und die bisher üblichen Recursive Resolver der jeweiligen Internet-Zugangsanbieter weniger Einsatz finden. DoH wird maßgeblich von Mozilla forciert.

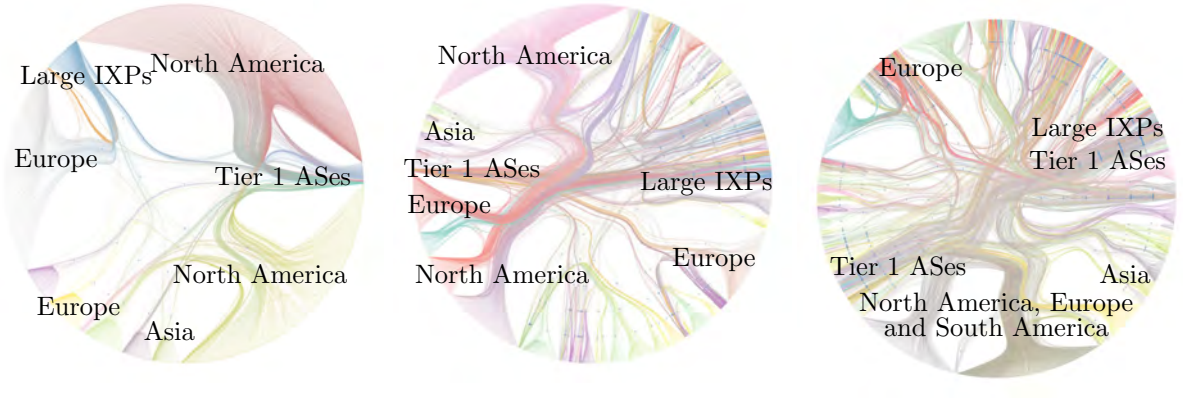
DoH und QUIC zeigen, dass technische Lösungen missbraucht werden können, um die eigenen Geschäftsinteressen zu befördern, obgleich die Lösungen den grundlegenden Internet-Prinzipien folgen.

Dem gegenüber befördern ökonomische Konsolidierungen technologische Konsolidierungen in jedem Fall. Je weniger Akteure es innerhalb eines Marktes gibt, desto weniger wichtig sind Aspekte der Interoperabilität. Mangelende Interoperabilität erleichtert Konsolidierungen bzw. Abhängigkeiten. Das Beispiel QUIC zeigt aber auch, dass Firmen mit Vormachtstellung im Internet-Anwendungsmarkt weiterhin den Weg einer offenen, interoperablen Internet-Infrastruktur gehen.

5.1.2 Strukturelle Entwicklungstrends im Internet Routing

Eine interessante Sicht auf grundlegende Entwicklungstrends lässt sich aus der Betrachtung der Internet Routing-Strukturen gewinnen. Beschränkte, regionale Inseln mit spärlicher Vermaschung zeigen ein stark diversifiziertes, dezentrales Internet unabhängiger Provider. Einzelne Autonome Systeme, die global eine große Zahl von regionalen Clustern verbinden – etwa Tier-1 ASes – zeigen ein funktionskritisches, in der Routing-Hierarchie herausgestelltes Rückgrat. Dahingegend sind eine starke Vermaschung zwischen regional und strukturell heterogenen ASes ein Indikator für robuste, föderale Strukturen. Solche Strukturen weisen geringe hierarchische Abhängigkeiten auf.

Um die Entwicklung der Routing-Strukturen sichtbar zu machen, analysieren wir die AS-Relationsdaten von CAIDA [85] aus den letzten 20 Jahren. Diese Datensätze beinhalten die Routing-Beziehungen zwischen allen erfassbaren Autonomen Systemen. Die Beziehungen sind klassifiziert nach Customer-to-Provider (C2P) und Peer-to-Peer (P2P). Im Routing und damit in der Erreichbarkeit besitzen diese Beziehungen unterschiedliche Bedeutungen: Während Provider ihren Kunden in der Regel eine vollständige Erreichbarkeit im Internet Routing gewähren, indem sie die vollständige BGP Routing-Tabelle weiterleiten, werden in P2P-Beziehungen lediglich die Präfixe der eigenen Kunden ausgetauscht; es entstehen also regional verkürzte Wege, aber keine vollständige Dienstversorgung im Internet.



(a) 2000 (b) 2010 (c) 2020

Abbildung 5.2: Ringvisualisierung hierarchischer Blockstrukturen im Internet Routing während der letzten zwei Dekaden

Wir untersuchen die Gesamtheit aller Routing-Beziehungen mithilfe hierarchischer Blockstrukturen [86]. Hierbei werden zunächst die Autonomen Systeme nach ihren direkten Beziehungen in Cluster gruppiert und Cluster wiederum nach ihren Beziehungen hierarchisiert.

Die Entwicklung der Routing-Strukturen im Internet der vergangenen 20 Jahre wird in Abbildung 5.2 als stochastische hierarchische Blockstruktur [86] im Ring visualisiert. In diesen Graphen werden alle Autonomen Systeme in ihren zusammenhängenden, farblich markierten Clustern auf einem Ring angeordnet sowie Cluster ähnlicher Routing-

Zusammenhänge in Teilgruppen arrangiert. Ihre Peering-Links werden als verbindende Linien gezeichnet, so dass sich ein Bild der minimierten Wege im Internet ergibt.

Deutlich sichtbar wird, wie Strukturen über die zwei Dekaden zusammengewachsen sind, u.a. durch den Ausbau von IXPs. Während es im Jahr 2000 sehr klare Gruppenbildungen nordamerikanischer, europäischer und asiatischer Autonomer Systeme gab, und die internationalen Strukturen im Wesentlichen von den Tier-1 ASes und einer kleinen Gruppe großer IXPs vornehmlich in Europa gebildet wurden, haben sich diese klaren Trennungen im Jahr 2020 weitgehend aufgelöst. Große IXPs sind mehrfach auch international entstanden und clustern mit den Tier-1 Providern. Südamerika hat eine umfangreiche Provider-Infrastruktur entwickelt, die einerseits regional mit großen IXPs, andererseits international mit nordamerikanischen und europäischen Providern verknüpft ist. Zusätzlich sichtbar werden viele kleine Gruppen von heterogen peerenden Providern, welche die zunehmende Präsenz Autonomer Systeme am Internet Rand widerspiegeln.

Betrachten wir die Cluster-Entwicklung der letzten zehn Jahre genauer, so sehen wir in Tabelle 5.1, dass die Zahl der ISP Cluster kontinuierlich zunimmt, die durchschnittliche Größe der Cluster aber abnimmt. Diese Entwicklung hat in den letzten fünf Jahren besonders zugenommen. Eine genauere Differenzierung nach Routing-Beziehungen zeigt aber, dass dieses Gesamtbild die Summe von zwei gegenläufigen Effekten ist.

Jahr	Anzahl ASes	Anzahl Cluster	mittlere Cluster-Größe [# ASes]
2010	33486	162	206,70
2015	46172	230	200,74
2020	68289	444	153,80

Tabelle 5.1: Clusterentwicklung bei Betrachtung aller Routing-Beziehungen

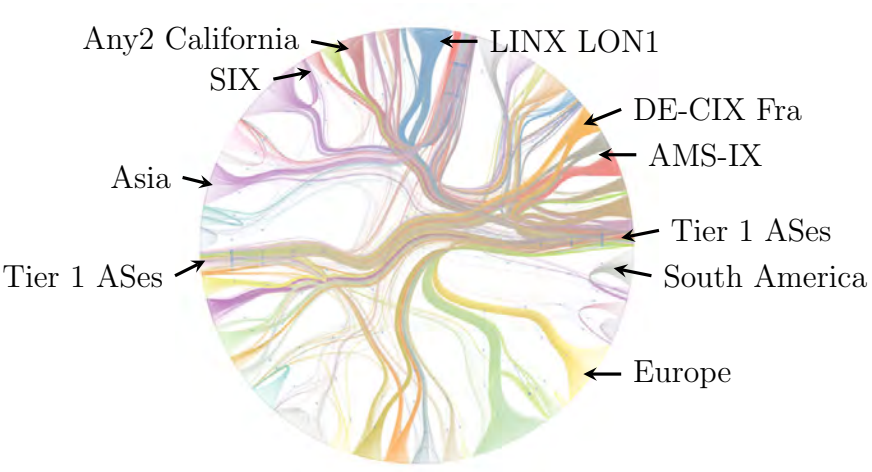
Die Tabellen 5.2 und 5.3 schlüsseln diese Cluster-Bildungen weiter nach Peering-Beziehungen auf. Für die C2P-Relationen sehen wir in Tabelle 5.2 eine Trendumkehr seit 2015: Die Cluster wachsen sehr stark, zeugen also von einem Kundenwachstum, während gleichzeitig die Anzahl der (Provider-)Cluster abnimmt. Dies kann als klarer Konsolidierungstrend gedeutet werden.

Jahr	Anzahl ASes	Anzahl Cluster	mittlere Cluster-Größe [# ASes]
2010	33381	107	311.97
2015	45962	142	323.67
2020	68004	135	503.73

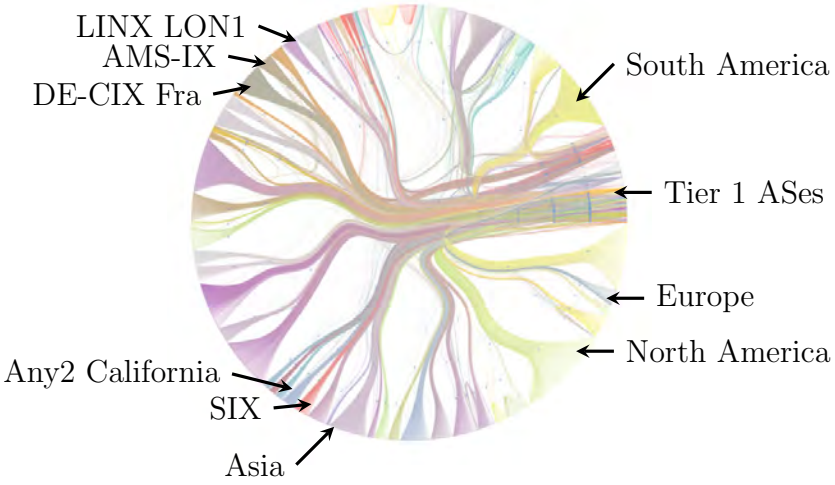
Tabelle 5.2: Clusterentwicklung bei Betrachtung der C2P-Beziehungen

Jahr	Anzahl ASes	Anzahl Cluster	mittlere Cluster-Größe [# ASes]
2010	3736	103	36.27
2015	6906	135	51.15
2020	13319	277	48.08

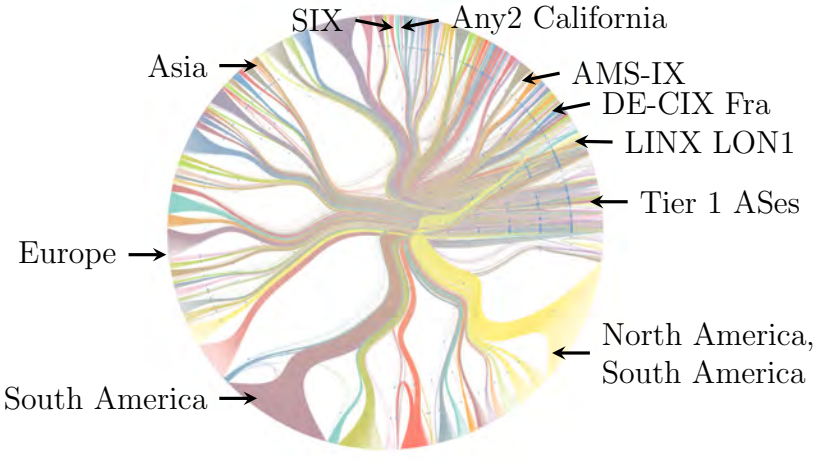
Tabelle 5.3: Clusterentwicklung bei Betrachtung der P2P-Beziehungen



(a) 2010



(b) 2015



(c) 2020

Abbildung 5.3: Hierarchische Blockstruktur der P2P-Verbindungen im Lauf der letzten Dekade
(CAIDA AS-Relationship Daten)

Ein gegenläufiges Bild zeigen die P2P-Relationen in Tabelle 5.3: Die relativ kleinen Cluster bleiben in ihrer Größe weitgehend stabil, die Clusteranzahl verdoppelt sich hingegen in den letzten fünf Jahren. Diese Verdopplung entspricht ungefähr der Zunahme von Autonomen Systemen im Internet, so dass diese Statistiken also als organisches Wachstum des Internets bei struktureller Stabilität interpretiert werden können. Insbesondere stehen diese Beobachtungen dem – in Europa gängigen – Eindruck entgegen, dass P2P-Beziehungen sich vor allem an wenigen monopolartigen, stark wachsenden IXPs entwickeln.

Betrachten wir die Entwicklung der P2P-Beziehungen noch einmal in der Ringvisualisierung (vgl. Abbildung 5.3), so sind vergleichsweise stabile, selbstähnliche Strukturen zu erkennen. Regionale Cluster wachsen in der Anzahl und Teilnehmerdichte, wohingegen die großen europäischen IXPs relativ in der Größe abnehmen; dies ist für den Londoner LINX besonders auffällig.

5.1.3 DNS over HTTP (DoH) und DNS over TLS (DoT)

Domainnamen (oder kurz Namen) sind elementar für die meisten Internet-Dienste, da Anwender selten direkt IP-Adressen in ihren Anwendungen benutzen. Das Domain Name System (DNS) bildet Namen auf IP-Adressen ab und gehört deswegen zu den wichtigsten Diensten im Internet. Da Namen fast immer der Einstiegspunkt für die Kommunikation sind, haben sie nicht nur technische, sondern auch wirtschaftliche und politische Relevanz.

Namen: Wirtschaftliche Relevanz Die Relevanz von Namen für die erfolgreiche Umsetzung von Geschäftsinteressen ist in Abb. 5.4 illustriert [87]. Die linke y-Achse zeigt die Entwicklung der registrierten Domainnamen über die Zeit, ausgehend von den Anfängen des Internet. Die rechte y-Achse stellt die Anzahl der Namensstreitigkeiten dar, welche durch die World Intellectual Property Organization (WIPO) verhandelt wurden. Ein erheblicher Anstieg ist während der `.com`-Phase zu beobachten, während etablierte und neue Firmen anfingen, den Digitalmarkt zu erschließen. Damit einhergehend wurde ein wichtiges nicht-technisches Problem stärker offenbart: Wer ist legitimiert, einen bestimmten Namen im DNS zu registrieren? Dritte haben Namen von bekannten Firmen, Organisationen etc. reserviert, um besonders hohe Klickzahlen auf Webseiten zu erzielen, Schadsoftware zu verteilen o.ä. Um dem zu begegnen wurden – ähnlich zu Markenstreitigkeiten – Schlichtungsverfahren zur Auflösung von Namensstreitigkeit von der ICANN entwickelt. Die Grundgebühren für die Durchführung solcher Schlichtungsverfahren sind moderat. Sie liegen zwischen 1500 USD und 5000 USD[1] und können damit auch von kleineren Firmen aufgebracht werden.

Namen: Politische Relevanz Da Namen als Indirektion zwischen Anwendungsdienst und IP-Endpunkt fungieren, kann die Unterdrückung (oder Fälschung) der Namensauflösung die Kommunikation generell unterbinden (oder umlenken). Entsprechend wird das DNS auch genutzt, um Zensur umzusetzen. Begünstigend kommt hinzu, dass Namen im Alltag oft so gewählt werden, dass sie sprechend sind. Sie verraten damit viel über den Nutzer bzw. mögliche Intentionen des Nutzers. Die Beobachtung der angefragten Namen ist deswegen für viele Parteien von Interesse.

[1] `https://www.wipo.int/amc/en/domains/fees/index.html`

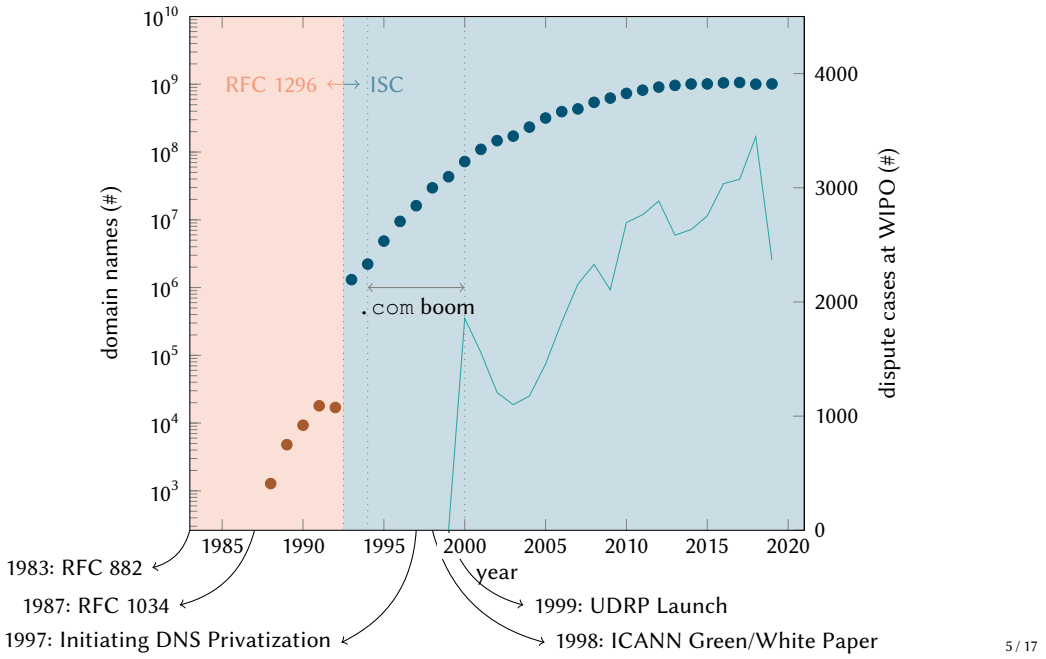


Abbildung 5.4: Wachstum der Namen im DNS (gepunktet) im Vergleich zu Domainnamen-Streitigkeiten (Linie) aufgrund der Uniform Domain-Name Dispute-Resolution Policy (UDRP) registriert bei der World Intellectual Property Organization (WIPO) (Quelle: Tehrani *et al.* 2019)

Die über lange Zeit vorherrschende Umsetzung von DNS-Anfragen sah derart aus, dass der Endkunde für die Auflösung von Namen den rekursiven DNS-Server seines Netzzugangsproviders nutzt. Dies hat drei Vorteile:

1. Mit jedem Netzzugang wird ein anderer DNS-Server gewählt, wodurch es automatisch zu keiner zugangsübergreifenden Ballung auf einzelne DNS-Server kommt.
2. Das damit notwendige dynamische Auffinden des aktuell passenden rekursiven Servers wird vereinfacht, da die *Service Discovery*, d.h. welcher DNS-Server soll gewählt werden, lokal stattfindet.
3. Es gibt bereits eine minimale Vertrauensbeziehung zwischen Kunden und Netzzugangsprovider und damit auch zwischen Kunden und DNS-Server.

In den vergangenen fünf Jahren gab es zunehmend Bestrebungen, DNS-Anfragen auf dem Weg zwischen Stub-Resolver und rekursiven DNS-Server zu verschlüsseln, so dass die angefragten Namen für mögliche Angreifer auf dem Weg nicht sichtbar sein sollen. Die zwei bekanntesten Ansätze zur Umsetzung dieses Ziels sind *DNS over TLS (DoT)* und *DNS over HTTPS (DoH)*. Um Datenlecks zu verhindern, gibt es aber auch andere Ansätze, wie z.B. *Query Name Minimisation*.

Query Name Minimisation Im traditionellen DNS-Auflösungsprozess weiss jeder zwischenliegende (rekursive und iterative) DNS-Server um den vollständigen, angefragten Namen. Query Name Minimisation verringert die offenbarten Informationen, indem jedem iterativen autoritativen DNS-Server nur die DNS-Labels seiner Zone übermittelt

werden. Die Root-Server erfahren dadurch nur die angefragte Top-Level-Domain. Top-Level-Domain Server erfahren nur die angefragte Second-Level-Domain usw.

Einige öffentliche DNS-Resolver wie der Google DNS Resolver nutzen Query Name Minimisation nur für die ersten drei Ebenen des DNS-Domainnamens [88]. Folglich verbirgt der rekursive Server den vollen Namen sowohl für die Root-Server als auch die Top- und Second-Level-Server, offenbart aber alle weiteren Details solchen Servern, die weiter tiefer in der DNS-Hierarchie verortet sind. Kritische Stimmen mögen vermuten, dass ein solches Vorgehen weniger den Endnutzern dient, als dass es die Informationsdiskrepanz zwischen TLD-Servern und Third-Level-Servern etc. erhöht [88].

Unterschied DoT und DoH *DNS over TLS (DoT)* baut eine TLS-Verbindung zwischen Stub-Resolver und rekursiven DNS Server auf. Hierfür ist ein dedizierter Transportport vorgesehen. Durch den Aufbau einer TLS-Verbindung sind zwar DNS-Anfragen vor dem Mitlesen oder Manipulationen geschützt, lassen sich aber nicht mehr mit einer Round-Trip-Zeit auflösen. Viele sehen nur wenig Erfolgschancen für DoT. Es ersetzt DNS über UDP. Viele Browser-Hersteller unterstützen DoT aber nicht. Entsprechend muss es im Betriebssystem verankert werden. Das Hauptargument gegen eine Nutzung von DoT besteht darin, dass DoT aufgrund eines dedizierten Transportports von anderen Internet-Diensten unterscheidbar ist, wodurch das Filtern von DoT vereinfacht wird.

DNS over HTTPS (DoH) setzt ebenfalls auf TCP und TLS auf. Im Gegensatz zu DoT werden DoH-Nachrichten aber zusätzlich in HTTP eingebettet und der entsprechende Standard-Transportport ist analog zu HTTPS TCP/443. Damit ist DoH-Verkehr für einen externen Beobachter von HTTPS-Verkehr nicht einfach unterscheidbar. Das gilt insbesondere dann, wenn unter der gleichen IP-Adresse (bzw. IP-Präfix bzw. autonomen System) vorrangig Web-Verkehr angeboten wird. DNS- und Anwendungsverkehr verschwimmen hierbei also deutlich stärker.

Verschiebung der Informationshoheit DoH wird vorrangig von zwei Gruppen vorangetrieben: Browser-Herstellern und CDNs. Einerseits bieten die DNS-Änderungen diesen Anbietern die Möglichkeit, neue, für ihre Geschäfte relevanten Daten zu erlangen. Andererseits verfügen diese Firmen über eine umfangreiche Infrastruktur, um die Dienste zuverlässig und skalierbar anzubieten. Auch wenn die ursprüngliche Motivation, d.h. die Verschleierung der angefragten Namen vor weiteren Internet-Akteuren zu befürworten ist, sind die Triebkräfte der größeren, konsolidierenden Firmen kritisch zu sehen. Die aktuellen Implementierungen verschieben primär die Informationshoheit. Viele Browser haben per Default die gleichen DoH-Server vorkonfiguriert. Nutzer können diese nur umständlich ändern. Anstatt dass ISPs über ihre rekursiven DNS-Resolver Einsicht in die angefragten Namen erhalten, lernen nun Browser-Hersteller und CDNs oder OTTs diese Informationen. Das ist insofern bedenklich, als die Geschäftsmodelle von CDNs und OTTs primär auf der Gewinnung von Daten basieren. Dies ist im Gegensatz zu ISPs: Die Auswertung einzelner Namen ist für ISPs nur bedingt relevant. Generelle Verkehrsflüsse können ISPs immer analysieren; CDNs und OTTs hingegen nicht. Durch die DNS-Zusatzdaten sind aber CDNs und OTTs auf einmal in der Lage Verkehrsflüsse auch für Content-Elemente unabhängig ihrer eigenen Kunden zu modellieren. Dies könnte es ihnen z.B. erlauben, eine informierte Kundenakquise bzw. -charakterisierung durchzuführen.

Auswirkungen von DoH auf die Netzneutralität im Kontext von CDNs Neben dem

Problem der veränderten Informationshoheit bestehen Bedenken, dass sich aktuelle DoH-Anbieter in einem Interessenkonflikt befinden und Prinzipien der Netzneutralität unterwandern [89]. Cloudflare beispielsweise ist sowohl DoH-Anbieter, als auch Anbieter von CDN-Dienstleistungen. Ein Endgerät, das die Web-Inhalte von einem anderen CDN abruft (z.B. Akamai), für die Namensauflösung aber den Cloudflare-DoH-Dienst nutzt, könnte als Antwort auf eine DNS-Anfrage einen IP-Endpunkt außerhalb des eigenen ISPs erhalten, obgleich CDN-Caches innerhalb des ISPs vorhanden sind. Entsprechend würde zum einen die Latenz beim Abrufen der Web-Inhalte des (konkurrierenden) CDN höher als nötig sein, zum anderen würde der Abruf der Webinhalte Transitkosten für den ISP und das CDN erzeugen, da die Inhalte nicht von einem lokalen Cache bereitgestellt werden. Der DoH-Anbieter würde also die Kunden der Konkurrenz und ihre Zugangsprovider benachteiligen.

Die Verletzung der Netzneutralität im Rahmen von DoH wurde in der Praxis beobachtet [89]. Die damit verbundenen Messergebnisse sollten aber vorsichtig bewertet werden, da die Messungen nicht trivial sind und eine seriöse Bewertung Details über den Messaufbau verlangt. Auch ohne explizite Verletzung der Netzneutralität durch den DoH-Provider kann es bei der Nutzung von DoH in dem skizzierten Fall zu nachteiligen Leistungswerten im Vergleich zu DNS-Anfragen über den DNS-Reolsver des ISPs kommen. Jeder rekursive DNS-Server (vom ISP oder vom DoH-Anbieter) fragt iterativ den autoritativen DNS-Server an. Im Fall von CDN-Inhalten entscheidet der autoritative DNS-Server anhand der IP-Absenderadresse der DNS-Anfrage, welche IP-Adresse in der DNS-Antwort verwendet wird. Die Absenderadresse ist immer die des rekursiven DNS-Servers. Der rekursive DNS-Server des ISPs ist topologisch dichter am Stub-Resolver (also Endnutzer) im Vergleich zu einem beliebigen rekursiven DoH-Server. Dadurch wird bei der Nutzung des DNS-Servers des ISPs der Resolver des Endnutzers als Antwort eher einen Content Cache aus dem eigenen Netz erhalten.

Um den IP-Präfix des DNS Stub-Resolvers in der DNS-Anfrage zu kodieren, muss der rekursive DNS-Server das `EDNS Client Subnet` setzen. Das Nutzen dieses Feldes ist nicht verpflichtend. Der Coudflare DoH-Server setzt es explizit nicht und verweist auf den Schutz der Privatsphäre für die Endnutzer – wohl wissend, dass die autoritativen DNS-Server konkurrierender CDNs damit keine Möglichkeit haben, den optimalen CDN-Cache zu ermitteln. Umgekehrt benötigt Cloudflare für die eigenen Webinhalten kein `EDNS Client Subnet`, da sich die Stub Resolver direkt an den Cloudflare DoH-Dienst wenden. Weitere Apskekte der Netzneutralität werden in Abschnitt 6.2.4 diskutiert.

Gedanken zu einem besseren Ökosystem Idealerweise gibt es für jeden Nutzer eine erhebliche Diversifizierung in den genutzten rekursiven DNS-Resolvern, die unabhängig von ISPs oder größeren Content-Netzen ist. Eine drastische Option wäre, dass jeder Stub Resolver gleichzeitig als iterativer Resolver fungiert. Solche Ansätze werden in der IETF diskutiert. Auch wenn die Idee aufgrund umfangreicher Hardware-Ressourcen im Endgerätebereich denkbar ist, ist sie nicht in allen Szenarien geeignet. Insbesondere Low-end-IoT-Geräten würden entsprechende Speicherkapazitäten fehlen.

Weiterhin wurden Möglichkeiten des *Resolverless-DNS* vorgeschlagen. Hierbei werden DNS-Antworten proaktiv, d.h. ohne explizite Anfrage, von einem DoH-Server an den Client übermittelt. Mittels HTTP Push wäre das möglich.

Eine weitere Alternative wäre, dass ein Stub Resolver abhängig vom *Content* unterschiedliche rekursive DNS-Resolver benutzt. Die Privatsphäre würde dann nicht weiter verletzt werden, wenn der DNS-Server unter Kontrolle des Content-Anbieters wäre. Dies ließe sich prinzipiell in einem URL-Schema kodieren, z.B. `https://youtube.com/dns=google.com`. Offen bliebe, wie die IP-Adresse des DoH-Servers aufgelöst wird. Hierfür könnte statt eines Namens eine IP-Adresse verwendet werden. Solch erzeugte URLs wären aber nur praktikabel, wenn sich der Endnutzer die Webseiten über eine Suchmaschine erschließt.

Viel wichtiger scheint aber ein generelles Bewusstsein in der Bevölkerung für den Missbrauch und die Verletzung der Privatsphäre durch DNS zu sein. Aktuelle Technologien wie DoH erlauben prinzipiell eine flexible Nutzung von DNS-Resolvern. Es mangelt aber an entsprechenden Konfigurationsschnittstellen, so dass der Endnutzer einfach Gebrauch davon machen kann. Wenn ein Endnutzer seinen Webbrowser so konfigurieren könnte, dass er einzelne Webseite (oder Namenspräfixen) bestimmten DoH-Server zuordnen könnte, wäre eine praktische Verbesserung zum Status Quo gegeben.

5.2 Content Distribution Networks

Content Distribution Networks (CDNs) implementieren einen skalierbaren Dienst für die effiziente Verteilung von Netzinhalten. Der usprüngliche Fokus lag auf Webinhalten. Heute verbreiten CDNs ein deutlich breiteres Spektrum an Daten, einschließlich Software-Updates. Das oberste Ziel ist immer die Verringerung von Latenzen, d.h. die Verzögerung von der Anfrage bis zur Zustellung der Daten. Dies wird durch Caches erreicht, welche möglichst nah an den Content-Konsumenten platziert werden.

Grundsätzlich gibt es zwei Arten, ein CDN zu betreiben: (1) Die CDN-Caches werden in potentiellen Zielnetzen platziert. Hiermit entfällt der Betrieb eigener umfangreicher Netzinfrastruktur. (2) Das CDN betreibt ein eigenes, geographisch verteiltes autonomes System, welches direkt mit den Endkundennetzen BGP-Verbindungen unterhält. Konnten CDNs ursprünglich diesen beiden Betriebsarten zugeordnet werden, nutzen große CDNs heute hybride Modelle, welche beide Arten implementieren. Des Weiteren haben sich in den letzten Jahren sogenannte Meta-CDNs gebildet, welche zwischen unterschiedlichen CDNs vermitteln.

5.2.1 Von dedizierten Transit zu eigenen Peering-Verbindungen

Der Betrieb eines großen Content-Netzwerks kann hohe finanzielle Aufwendungen zur Folge haben, wenn der Betreiber umfangreich Transit-Konnektivität bezahlen muss. Ein schneller Markteintritt kann für CDNs erfolgen, indem sie Peer-to-Peer-Konnektivität statt Transit-Konnektivität nutzen. Peer-to-Peer-Konnektivität ist an IXPs kostengünstig realisierbar. Ein 100 Gbps-Anschluss kostet z.B. am BCIX 2.600 EUR/Monat. Zusätzlich müssen Leitungen für die Anbindung an das eigene, interne Netz angemietet werden. Dennoch entsteht so eine deutlich höhere Autonomie bezüglich des Routings im Vergleich zu einer ausschließlichen Abhänigkeit von Upstream-Providern. IXPs waren einer der Kernfaktoren für den Erfolg von CDNs, umgekehrt haben große CDNs die Bedeutung von IXPs

erheblich erhöht, wodurch es zu einer Abflachung der Internet-Infrastruktur kam [2, 90].

CDNs mit sehr populären Inhalten haben im gesamten Internet-Ökosystem einen erheblichen Einfluss, da sie einen umfangreichen eingehenden Datenverkehr verursachen können. Als Beispiel sei ein DSL-Provider genannt und der Fall eines Betriebssystem-Updates auf Seiten der Endkunden, wodurch dieselbe Software für jeden einzelnen Endkunden (oft zeitgleich) über einen Transitlink des ISPs geladen wird. Dies kann schnell zu Überlastsituationen führen. ISPs haben demnach per se ein Interesse, die Content-Caches der CDNs innerhalb ihres eigenen Netzes zu platzieren, so dass der Verkehr nur einmal an den Netzgrenzen ausgetauscht wird. Tatsächlich gibt es oft Vereinbarungen zwischen CDNs und ISPs, die genau das den CDNs (oft kostenfrei) ermöglichen. Dies ist insofern kritisch, als dass CDNs somit automatisch kostenfrei globaler Internet-Transit bereitgestellt wird. CDNs nutzen diese Option, um Daten zwischen ihren Cache-Servern, welche in unterschiedlichen autonomen Systemen stehen, auszutauschen. Für Transit-ISPs stellt es eine Herausforderung dar, dies zu erkennen und ggf. zu unterbinden.

5.2.2 Wachstum von Cloud-Infrastrukturen

Cloud-Dienste haben seit mehr als 15 Jahren hohe Popularität erlangt. Die Gründe hierfür sind in zwei Punkten zu sehen. Zum einen können Hardware-Ressourcen dynamisch ausgelagert werden. Zum anderen bieten sie Entwicklern die Möglichkeit, dynamisch Ressourcen auf der Anwendungsebene zu allokieren. Jeder Cloud-Dienst bietet hochstehende Schnittstellen (z.B. über ein Web-Portal oder eine Python API), um die notwendige (Hardware-)Infrastruktur in Betrieb zu nehmen. Diese Abstraktion stellt einen Paradigmenwechsel dar. Anwendungsentwickler sind durch Cloud-Dienste in die Lage versetzt, ohne langwierige Interaktionen mit anderen IT-Abteilungen die für ihre Arbeit notwendigen Ressourcen eigenständig zu aktivieren.

Die größten Cloud-Anbieter werden als *Hyperscaler* bezeichner. Amazon Web Services (AWS) dominiert den Markt mit 32% Anteil im Jahr 2020, gefolgt von Microsoft Azure (18%) und Google (7%) sowie Alibaba (6%).[2] Mit ihrer Marktmacht dominieren sie auch die eingesetzten Technologien. Dies zeigt sich beispielhaft in der Integration von Anwendungen für das Internet der Dinge (IoT). Aufgrund der hohen Datenmengen, welche durch IoT-Sensoren gewonnen werden, werden Analysen der Daten häufig in Cloud-Infrastrukturen durchgeführt. Das *Constrained Application Protocol (CoAP)* [91] stellt das von der IETF standardisierte Protokoll dar, um die Maschinen-zu-Maschinen-Kommunikation zwischen IoT-Geräten und Cloud zu realisieren. Die meisten momentan im Einsatz befindlichen IoT-Cloud-Lösungen setzen aber auf MQTT [92] auf. MQTT ist ein offener Industriestandard. Ein Grund für die starke Verbreitung von MQTT liegt darin, dass AWS MQTT im Gegensatz zu CoAP von Hause unterstützt.

Insbesondere im Bereich des IoT erschließen etablierte low-tech Firmen (z.B. Heizungshersteller) auf Basis von IT neue Märkte, obgleich deren Kernkompetenz außerhalb von IT liegt. Sie nutzen bestehende Dienste ohne die Technologien im Detail zu hinterfragen oder mitzugestalten. Hier bedarf es langfristig eines Kulturwechsels, um weitere Konsolidierungen zu verhindern.

[2] Die Zahlen sind über unterschiedliche Quellen hinweg konsistent.

Die vollständig virtuelle, geopolitisch undurchsichtige Ablage der Daten wird kontinuierlich kritisiert. Um dieser Sorge zu begegnen, wird im Rahmen des Projekts *GAIA-X* eine europäische Dateninfrastruktur geschaffen, welche über offene Schnittstellen und Standards dezentrale Komponenten zu einem homogenen System vernetzt. Neben den Leitlinien von Neutralität, Offenheit und Transparenz wird dem Wunsche nach Datensouveränität auch dahingehend Rechnung getragen, als dass die Daten in Europa abgelegt werden.

5.2.3 Content-Pluralisierung außerhalb klassischer Cloud-Dienste

Die Konsolidierung großer Datenmengen auf einige wenige Cloud-Anbieter wird regelmäßig in der Fachgemeinschaft diskutiert. Grundsätzlich kann dem nur entgegengewirkt werden, indem die durch Clouds bereitgestellten Dienste Teil der Basis-Netzwerkprimitiven werden. Voraussetzung hierfür ist, dass Daten überall ablegbar und auffindbar sind.

Ein vielversprechendes neuartiges Konzept für die Pluralisierung von Cloud-ähnlichen Diensten sind sogenannte informations-zentrischen Netzwerke (kurz ICN). Die Kernidee dieser neuen Protokollfamilie liegt in einem namensbasierten „Hop-by-Hop"-Routing auf Inhalten (statt adressbasiertem Ende-zu-Ende-Zugriff) und einem ubiquitären Caching im Netzwerk. Durch die Verwendung eines namensbasierten Routings verringert sich nicht nur die Komplexität des Netzwerk-Stacks, sondern es werden inhaltsbezogene Differenzierungen und Optimierungen möglich. Darüber hinaus ermöglicht Caching innerhalb des Netzwerks, Kommunikationsausfälle zu überbrücken und Übertragungskapazitäten zu schonen.

Das Konzept des ubiquitären Caching setzt voraus, das Daten von jedem Knoten im Netzwerk zwischengespeichert werden können – ebenfalls eine Vorausstzung für die Pluarlisierung von Cloud-Diensten. Entsprechend muss jedes Content-Elemente verifizierbar und ggf. verschlüsselbar sein. Die damit verbundenen Fragen nach einer globalen Namensverwaltung und einem globalen Schlüssel-Management sind ein offenes Thema [93]. Um bestehende (technische und nicht-technische) Infrastukturen weiter zu nutzen, gibt es Vorschläge, die auf das heutige DNS-Ökosystem aufsetzen [87].

Eine vollständige Content- bzw. Cloud-Pluralisierung ließe sich in einem zukünftigen ICN-basierten Internet wie folgt vorstellen: Jede Komponente, die beim Weiterleiten der Daten auf der Netzwerkschicht involviert ist, speichert Daten soweit möglich zwischen. Dies würde z.B. DSL Home Gateways einschließen. Daten in einem Haushalt könnten so direkt aus der lokalen „Cloud" zugestellt werden. Jeder Endkunde könnte durch die Speicher-Provisionierung der eigenen Gateways festlegen, wieweit die Daten lokal vorrätig sind. Um die technischen Details muss sich der Endkunde nicht kümmern, da dies ein nativer Dienst auf der Netzwerkschicht – ähnlich wie sich Endkunden nicht explizit um den Bezug von IP-Adressen kümmern.

Bestehende Internet Service Provider könnten ebenfalls transparent CDN-basierte Dienste anbieten. Hierbei sind diejenigen im Vorteil, die bereits Möglichkeiten für Mini-Rechenzentren dicht am Endkunden haben. Die Deutsche Telekom ist ein solches Beispiel. Über die Verteilerkästen am Straßenrand, welche ursprünglich für die Anbindung von Haustelefonen installiert wurden, verfügt sie über ein dichtes Netz an geschützten Unterstellmöglichkeiten für zusätzliche, aktive Komponenten. Aufgrund der aktuell geringen

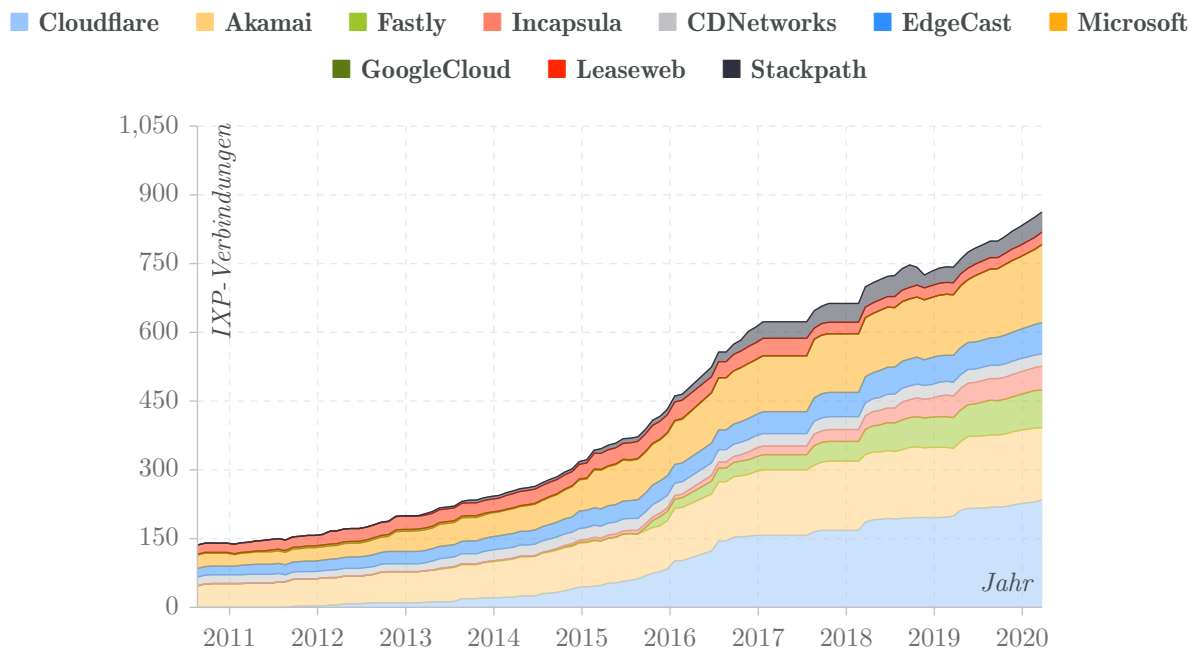


Abbildung 5.5: Entwicklung der IXP-Verbindungen ausgewählter CDN-Betreiber basierend auf Daten der PeeringDB

Packungsdichten von Medien mit hohem Speicheraufkommen könnte trotz geringem Platzbedarf eine umfangreiche Cache-Infrastruktur aufgebaut werden. Schon jetzt projektiert die Deutsche Telekom eine Neunutzung der vorhandenen Infrastruktur als bundesweites Ladennetz für Elektroautos (siehe `https://www.comfortcharge.de/`). Entsprechend werden die Kästen zukünfigt mit einer eigenen Stromversorgung und einer digitalen Messstelle ausgestattet werden. Leider ist nicht bekannt, dass das vorhandene Potential auch für eine modernere Internet-Infrastruktur genutzt wird. Anzuraten wäre es.

5.2.4 Historische Entwicklungen

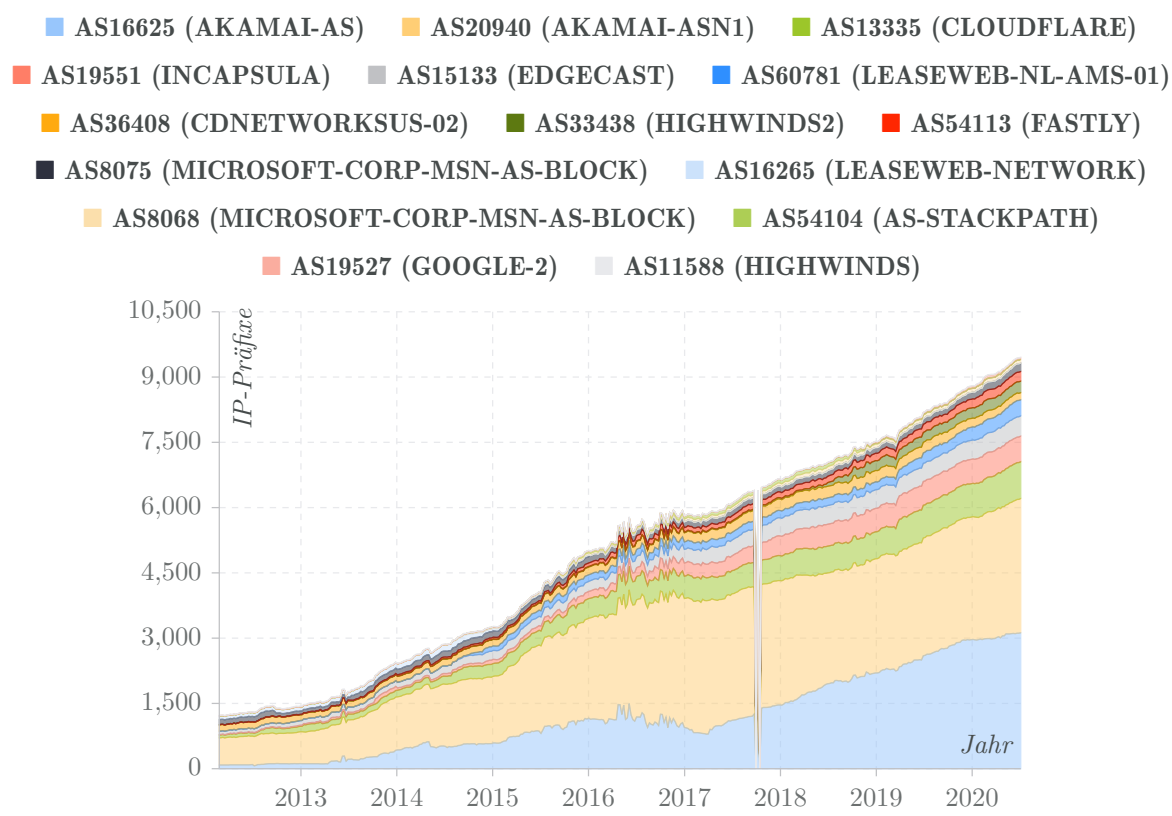
Im diesem Abschnitt betrachten wir einige historische Entwicklungen für die folgende populären CDNs: Akamai, CDNetworks, Cloudflare, EdgeCast, Fastly, GoogleCloud, Incapsula, Leaseweb, Microsoft und Stackpath.

Abb. 5.5 zeigt die Anzahl der IXP-Verbindungen pro CDN von 2011 bis 2020 basierend auf Daten der PeeringDB. In den Jahren 2011 bis 2014 ist die Anzahl der CDNs mit umfangreichen IXP-Verbindungen noch gering. Dies spiegelt den generellen CDN-Markt wider. Zu diesem Zeitpunkt gab es nur wenig etablierte CDNs. Akamai wurde bereits 1998 gegründet. Cloudflare hingegen erst 2009. Eine umfangreiche Nutzung des Cloudflare-Dienstes begann aber erst in den Jahren 2010 und 2011. Nach fünf Jahren Betrieb hat Cloudflare an 75 *Points of Presence (PoPs)* und 100 IXPs Daten ausgetauscht. Die Bedeutung von IXPs für CDNs wird auch darin sichtbar, dass IXP die Gründung von IXPs vorantreiben [94].

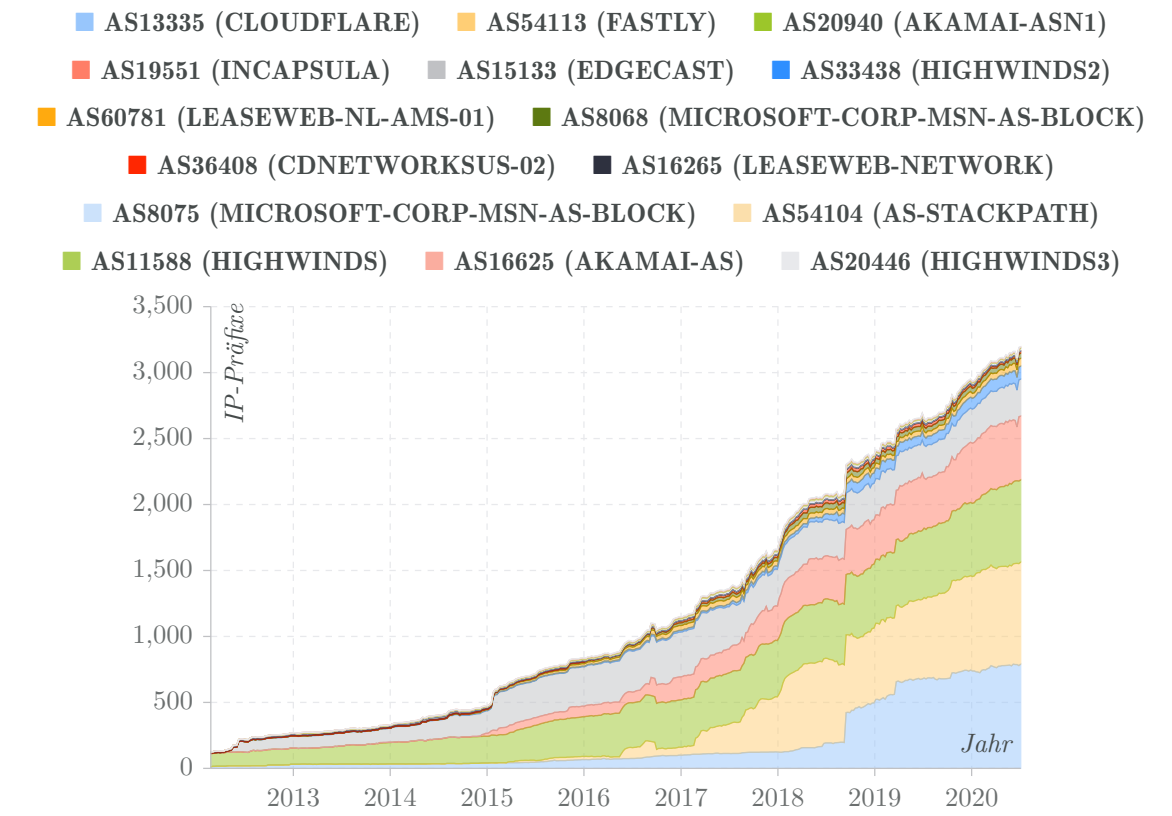
Insgesamt bauen CDNs kontinuierlich ihre Präsenz an IXPs aus, auch wenn die Wachstumsraten zwischen den CDNs unterschiedlich hoch sind. Dies hängt vermutlich auch damit zusammen, dass einige CDNs wie z.B. Cloudflare ihren Fokus auf große IXPs richten

und diese erschlossen wurden.

Die Wechselwirkung zwischen dem Infrastrukturausbau von CDNs und dem Bedarf nach Internet-Ressourcen, d.h. IP-Adressen zeigt Abb. 5.6. Die im globalen Routing sichtbaren IP-Präfixe von CDNs steigen kontinuierlich, um Anycast-Dienste, also standortbezogene Antworten, zu realisieren. Dabei steigt die Nutzung von IPv6 deutlich stärker im Vergleich zu IPv4 aufgrund der mangelnden freien Adressblöcke in IPv4. CDNs steuern auch maßgeblich die Verbreitung von IPv6-Verkehr. So ist in großen DSL-Netzwerken der Anteil des IPv6-Verkehrs signifikant (>50%), weil große CDNs IPv6 forcieren.



(a) IPv4



(b) IPv6

Abbildung 5.6: Entwicklung der im globalen Routing sichtbaren IP-Präfixe von ausgewählten CDN-Betreibern basierend auf Daten von RouteView Tier1-Peers

5.3 OTTs und Content-Anbieter

Over-the-top Content (OTT) Anbieter bezeichnen Firmen, die Endkunden über das Internet-Protokoll Audio- und Videoinhalte anbieten. Sie stellen eine Gegenbewegung zu ursprünglichen IPTV-Diensten dar, bei denen ISPs wie die Deutsche Telekom oder Vodafone die Filme selbst zur Verfügung stellen und somit zusätzlich zum eigentlichen Netzwerkzugang Einnahmen generieren. OTTs sind populär, weil sie nicht an einen spezifischen Netzzugang oder proprietäre Endgeräte gebunden sind. Der Kunde kann das Programm entweder direkt im Web-Browser oder über spezifische Abspiel-Software (*Apps, Player*) auf seinem Mobilgerät, Desktop etc. sehen – egal über welchen Netzzugang er gerade angebunden ist.

OTTs betreiben in der Regel eine eigene Content-Verteilinfrastruktur oder nutzen bestehende Content Delivery Netzwerke. IXPs sind hierbei wieder ein wichtiges Rückgrat (siehe Abbildung 5.7). OTTs beteiligen sich aber nicht am Ausbau der Netzzugänge zum Kunden. Entsprechend stellen OTTs für Eyeball-Provider folgende Probleme dar:

Wegfall von flexiblen Geschäftsmodellen OTTs haben einen für die ISPs lukrativen Zusatzdienst übernommen. Die Eyeball-ISPs fallen wieder in die wenig attraktive Rolle des reinen Datenvermittlers zurück, dessen Preismodell inhaltsunabhängig ist. Der Vorteil von Video-Diensten u.ä. liegt darin, dass sie ein deutlich flexibleres Preismodell im Vergleich zu klassischen Internet-Zugängen erlauben. So können Filme beispielsweise in unterschiedlichen Zusammensetzungen verkauft werden. Es besteht ein deulich größeres Verständnis dafür, dass mehr (oder hochwertigerer) Content, mehr kostet. Internet-Konnektivität hingegen wird als Basisdienst angesehen, für den wenige Kunden bereit sind, über das Grundmaß hinaus mehr zu bezahlen.

Datenraten und Infrastrukturausbau OTTs sind einer der großen Treiber für höhere Datenraten. Viele Endkunden wünschen sich hohe Auflösungen (Full HD, Ultra HD etc.), zumal die Endgeräte diese erlauben. Umgekehrt nutzen OTTs hohe Auflösungen als Marketing-Instrument, um die Qualität des eigenen Dienstes hervorzuheben. Das Problem für Eyeball-Provider besteht darin, dass die Bereitstellung von hochauflösenden Videos entkoppelt von dem Netzzugang der Endkunden ist: Der OTT-Anbieter stellt das hochauflösende Video bereit, der ISP muss den Netzzugang ausbauen, da sonst die Endkunden den Netzanbieter wechseln könnten. Das OTT-Netzwerk muss höhere Auflösungen mit Eyeball-Netzwerken auch nicht zwangsweise absprechen, da skalierbare Videokompressionsverfahren abhängig von der verfügbaren Datenrate die Auflösung dynamisch anpassen.

Die Bedeutung von Videoplattformen auf die Provisionierung der Internet-Infrastruktur zeigt sich auch darin, dass während des Corona-Krise große OTTs, wie z.B. YouTube, Netflix und Facebook ihre Datenraten explizit reduziert haben, um Überlast und Stausituationen zu verhindern.

Interessanterweise haben OTT-Plattformen in den letzten Jahren nicht nur einen konsolidierenden Einfluss auf die Internet-Infrastruktur, sondern auch auf das klassische Filmgeschäft. OTT-Anbieter vermarkten nicht nur Inhalte Dritter über Lizenzierungen, sondern produzieren eigene Inhalte. Sie sind Konkurrenz zu klassischen Filmproduzenten.[3]

[3]Aufgrund der Corona-Krise durften für die Academy Awards 2021 auch reine Streaming-Filme nominiert werden.

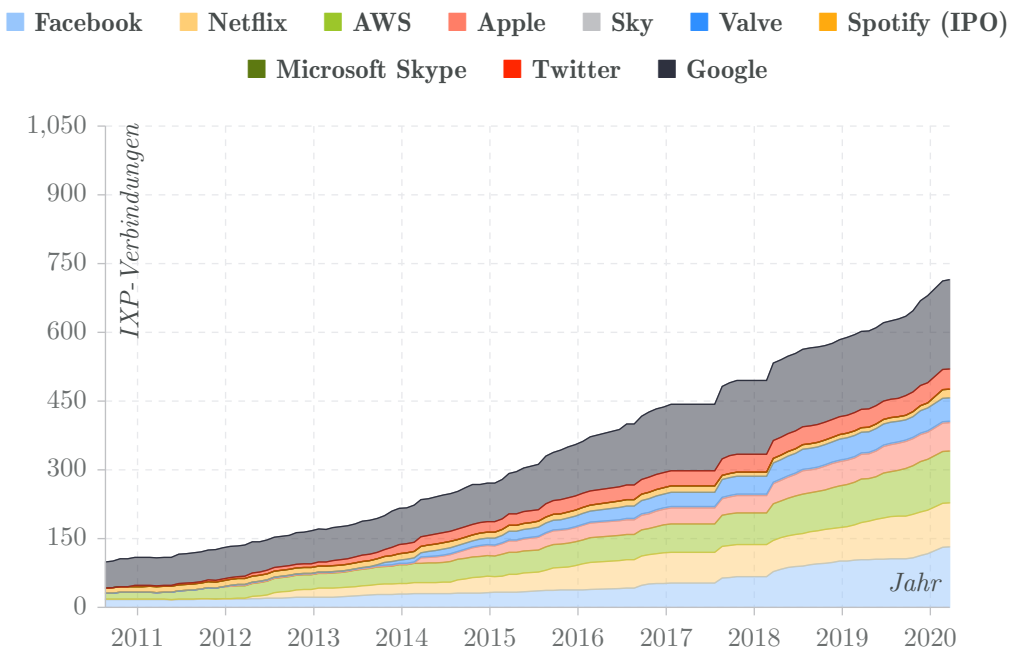


Abbildung 5.7: Entwicklung der IXP-Verbindungen ausgewählter OTTs basierend auf Daten der PeeringDB

Netflix und Amazon dominieren hierbei den Markt.

5.3.1 Fallstudie: Netflix

Netflix ist aktuell der größte Anbieter von kostenpflichtigen Videostreaming-Diensten. Die Infrastruktur von Netflix lässt sich im Kern wie folgt zusammenfassen:

1. Ursprünglich nutzte Netflix klassische CDNs wie Akamai und Limelight für die Content-Verteilung.

2. Im Jahr 2012 begann Netflix die Verteilung der Videos an die Endkunden auf sein eigenes CDN, *Open Connect*, umzustellen.

3. Im Gegensatz zu anderen Hypergiants wie Google und Facebook betreibt Netflix keine eigenen Rechenzentren, sondern nutzt Amazon Web Services, z.B. für die eigenen Webseiten sowie um Filme zu speichern und zu kodieren.

Der Wechsel von Dritt-CDNs zu einer ausschließlichen Verteilung über Open Connect hatte größere wirtschaftliche Folgen für die klassischen CDNs und illustriert die wirtschaftlichen Folgen von Konsolidierungen. Im Jahr 2011 betrug der Anteil an Einnahmen bei Limelight durch Netflix 11% [95].

Die Studie von Böttger et al. [96] analysiert die Netflix-Infrastruktur im Detail. Das Kernprinzip von Open Connect ist der Einsatz von Servern nahe am Edge durch die Nutzung von IXPs. Netflix betreibt deswegen kein eigenes umfangreiches Backbone-Netzwerk, sondern versucht Inhalte außerhalb von Spitzenzeiten auf ihre Server zu verteilen. Für ISPs, die viele Netflix-Kunden anbinden, bietet Netflix zwei Optionen an: (1) die Installation von Cache-Servern direkt im Netzwerk des ISPs und (2) direkte Peering-Links, d.h.

Private Network Interconnect. Die drei Mechanismen (IXP-Peering, externe Cache-Server, direktes Peering) erlauben Netflix signifikant Transit-Verkehr einzusparen; ungefähr 10% des gesamten Netflix-Datenverkehrs ist Transit-Verkehr.

Aktuell ist Netflix an 105 IXP-Standorten vertreten. Dabei wählt Netflix tendenziell solche IXPs, an denen viele Netzwerke vor Ort sind. Ähnlich verhält es sich mit den Netflix Servern. 50% der Netflix Server sind in den 500 größten ISP-Netzwerken im Einsatz. Die verbleibenden Server sind über mehrere tausend kleinere ISPs verteilt. Die Verteilinfrastruktur ist wie üblich vor allem konzentriert auf Nordamerika und Europa, aber auch erheblich in Südamerika (Brasilien). Der typische Weg, um Regionen zu erschließen, erfolgt oft über IXPs. Wenn eine kritische Kundenbasis gewonnen wurde, werden zusätzlich ISPs direkt eingebunden.

Zum Zeitpunkt der Studie von Böttger et al. [96] gab es einige Tier1 ISPs in den USA und Europa, die keine Netflix Server einsetzten. Der Grund hierfür können Marktinteressen sein. Große ISPs möchten ihren (Tier1) Status schützen und binden Netflix über Paid Peering an.[4] Aktuell wird z.B. Netflix weiterhin als Kunde der Deutschen Telekom im CAIDA AS Rank identifiziert, wodurch die Deutsche Telekom nach außen sichtbar einen der größten Content-Produzenten als Kunde führen kann.

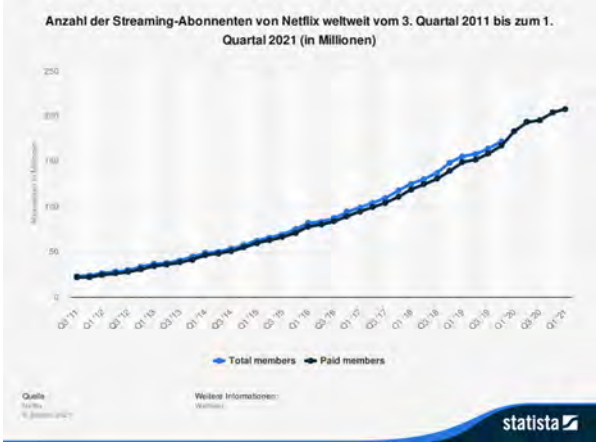
Das Vorgehen von Netflix ist kostengünstig und erlaubt eine hohe Agilität, da keine eigenen Rechenzentren gebaut und betrieben werden müssen. Umgekehrt macht sich Netflix durch dieses Vorgehen von Rechenzentrumsbetreibern abhängig. Dies ist insbesondere mit Blick auf mangelnde Rechenzentrumsflächen und steigenden Platzbedarf durch wachsende Server-Infrastruktur nachteilig. Dem kann aber durch innovatives Hardware Design begegnet werden.

5.3.2 Fallstudie: Disney+

Am 12. November 2019 nahm die Firma Disney ihren eigenen Video-Streaming-Dienst, Disney+, in den USA in Betrieb. In den darauffolgenden zwei Jahren wurden Länder in Europa und Asien erschlossen, da bestehende Rechte für das Streaming von Disney-Filmen erst auslaufen oder erworben werden mussten. Seit dem 24. März 2020 ist Disney+ in Deutschland, Österreich, Spanien, Italien, dem Vereinigten Königreich und der Schweiz verfügbar. Im März 2021 hatte Disney+ mehr als 100 Millionen Abonnenten weltweit und übertrifft damit ursprüngliche Wachstumsprognosen. Abbildung 5.8 zeigt das Wachstum der Abonnenten von Disney+ im Vergleich zu Netflix.

Die Einführung von Disney+ wurde von vielen als kritisch angesehen, da Disney+ von Disney produzierte Filme nunmehr exklusiv vertreibt. Bestehende Verträge mit beispielsweise Netflix wurden aufgelöst. Damit fragmentiert der Streaming-Markt für den Endkunden: Statt über einen Streaming-Dienst eine Vielzahl von Filmen unterschiedlicher Produzenten zu erhalten, muss der Kunde sich entweder für einen Produzenten oder für Abonnements unterschiedlicher Streaming-Dienste entscheiden. Diese Argumentation ist ambivalent, da bereits mit Netflix Eigenproduktionen oder Produktionen Dritter exklusiv über einen Streaming-Dienst, d.h. Netflix, vertrieben wurden. Die Vereinigung von

[4] Paid Peering ist kein Transit, da nur die eigenen IP-Präfixe und die der Kunden verteilt werden, einer der Teilnehmer dafür aber bezahlen muss.



(a) Anzahl der Abonnenten von Netflix weltweit vom 3. Quartal 2011 bis zum 1. Quartal 2021

(b) Anzahl der Abonnenten von Disney+ weltweit vom 1. Quartal 2020 bis zum 1. Quartal 2021

Abbildung 5.8: Wachstum der Streaming-Dienste Netflix und Disney+

Content-Produzent und Content-Anbieter ist nicht neu, und wurde durch das Internet erheblich verstärkt.

Technische Infrastruktur Im Gegensatz zu Netflix betreibt Disney+ für die Verteilung der Videoinhalte bisher kein eigenes CDN, sondern nutzt die Infrastrukturen von Akamai, Lumen, Limelight, Edgecast, CloudFront und Fastly. Es setzt damit auf Diversität. Multi-CDN-Szenarien sind insbesondere bei Live Streaming für eine hohe Dienstgünste entscheidend. Die Aufbereitung des Streamings und die Orchestrierung der CDNs erfolgt über Disney Streaming Services (ehemals BAMTech), die wiederum auf Amazon Web Services aufsetzen. Perspektivisch kann sich die Infrastruktur von Disney+ ändern:

> "Disney Streaming Services is evaluating partners for a future distribution network that will include commercial CDNs, Open Caches, and Disney cache appliances that will initially be deployed at IXPs.
>
> We are gathering information from potential partners who are interested in future peering and interconnect options. "
>
> — Disney Streaming (`https://www.peeringdb.com/net/15627`)

Auswirkungen auf das globale Verkehrsvolumen und Peering Die Einführung von Disney+ hat das globale Datenaufkommen nur bedingt verändert, da sich die Zahl der Filme, die ein Nutzer parallel anschaut, durch eine weitere Streaming-Plattform nicht erhöht. Der Einsatz unterschiedlicher CDNs verhindert zudem eine signifikante Konzentration von Datenlasten auf einzelne CDNs, wodurch auch einzelne CDNs keine erhöhte Relevanz erhalten. Große ISPs haben bereits sowohl zu allen populären CDNs als auch Netflix optimierte Datenübergänge, so dass sich das Peering-Ökosystem nicht erheblich ändern wird. Auch kleinere autonome Systeme dürften ihre Peering-Strategie bisher nicht anpassen müssen, da sie von den bestehenden Übergängen an den IXPs profitieren.

Zukünftig wird die Popularität von Streaming-Diensten weiter steigen. Auch das ist ein Effekt der Corona-Pandemie, da Nutzer aufgrund geschlossener Kinos stärker an den digitalen Konsum von Kinofilmen gewöhnt werden. Disney könnte diese Kulturänderung nutzen, um Filme zukünftig Filme exklusiv über Disney+ (statt parallel über Kinos) zu vertreiben. Ein solcher Vertriebsweg hätte den Vorteil, dass keine Drittfirmen, wie z.B. Verleiher, involviert werden müssen. Mit einer weiter steigenden Nutzerzahl kann davon ausgegangen werden, dass Disney das Geschäftsfeld des selbst betriebenen Online-Streamings als erfolgreich ansieht. Entsprechend könnte eine Abkehr von klassischen CDNs hin zu einer eigenen Infrastruktur zu beobachten sein. Ob dies passiert wird vorrangig eine Frage der einzusparenden Kosten sein. Am Beispiel Netflix sehen wir, dass bei einer ausreichenden Marktetablierung der Betrieb eines eigenen CDNs kostengünstiger sein kann.

Copyright-Verletzungen (Online Piracy) Die Fragmentierung des Streaming-Marktes ist per se kein Problem. Schwierig ist es, wenn Filme exklusiv an einzelne Streaming-Dienstleister gebunden werden. Um weiterhin ein breites Filmspektrum konsumieren zu können, müssten die Endkunden mehrere Streaming-Dienstleister nutzen, wozu sie in der Regel aus finanziellen Gründen nur ungern bereit sind. Diese für Endkunden ungünstige Fragmentierung könnte zukünftig erhöhte Copyright-Verletzungen zur Folge haben.

Des Weiteren kann vermutet werden, dass Tunnelmechanismen eine stärkere Verbreitung finden werden, da Streaming-Dienste oft örtlich gebunden sind. Laut eigenen Aussagen von Disney+ ist zwar der Großteil der Inhalte in allen Ländern verfügbar, aber es kann zu kleinere Abweichungen kommen. Im Februar 2020 gab es einen maximalen Unterschied von 66 Filmen und TV-Sendungen zwischen den Ländern Australien, Neuseeland, Kanada, Niederlanden und den USA. Disney+ Star ist eine neues Streaming-Angebot im Rahmen von Disney+, das bisher nur in eingeschränkten verfügbar ist. Selbst wenn sich langfristig Märkte verbreitern, wird es kurz- bis mittelfristig immer Inhaltsseparationen geben.

5.3.3 Fallstudie: Marea

Das Unterseekabel „Marea“ zwischen Nordamerika und Europa wurde von Facebook, Microsoft und Telxius, einem Unternehmen für Telekommunikationsinfrastruktur des spanischen Telefónica-Konzerns, gebaut. Der operative Betrieb wird von Telxius verantwortet. Das Unterseekabel umfasst ca. 6600 km, hat eine Gesamtkapazität von 200 Tbps und ging im Jahr 2018 in Betrieb. Das Kabel besteht aus acht Glasfaserpaaren. Hiervon gehören zwei Paare Microsoft, zwei Paare Facebook und vier Paare Telxius. Ein Glasfaserpaar hat Telxius an Amazon Web Services (AWS) im Rahmen einer IRU-Vereinbarung verkauft [97].[5] Die Anlandungspunkte sind Virigina Beach (USA) und Sopelana/Bilbao (Spanien). Der Anlandungspunkt in den USA ist strategisch, da hier die Unterseekabel BRUSA (ebenfalls Telxius) und Dunant (Google) ankommen und es eine Verbindung nach Ashburn[6] und Richmond gibt (siehe Abb. 5.9).

Marea illustriert gut das ambivalente Verständnis von Konsolidierungen im Kontext

[5]Bei IRU (Indefeasible Rights of Use) Vereinbarungen geht die verkaufte Infrastruktur üblichweise zwischen 20-30 Jahren an den Kunden über.

[6]Ahsburn zählt u.a. durch die Rechenzentren von Equinix zu den größten Internet-Austauschpunkten in den USA.

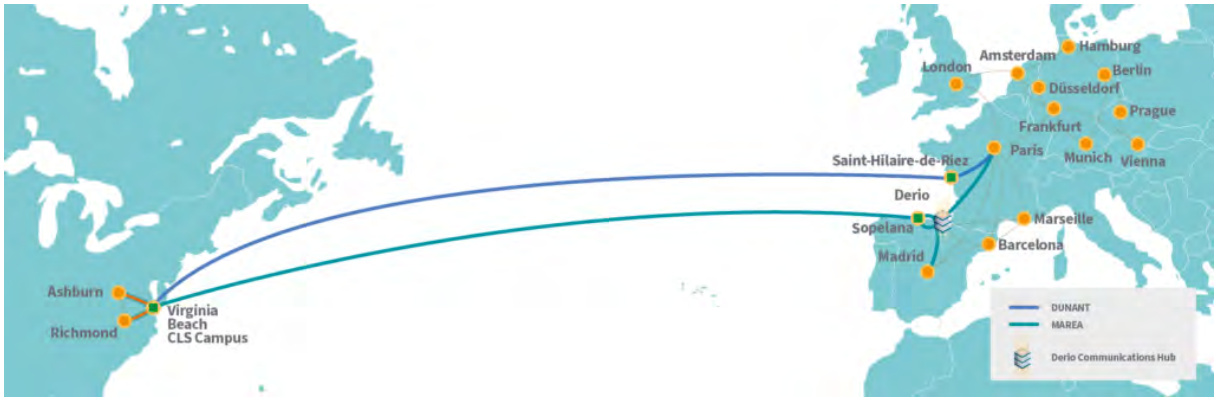


Abbildung 5.9: Die Unterseekabel Marea und Dunant verbinden strategische Anlandungspunkte in Nordamerika und Europa (Quelle: https://telxius.com/en/telxius-leads-the-transatlantic-subsea-market-with-dunant-and-marea-fully-in-service/).

der Unterseekabel. Aus Sicht von Facebook und Microsoft ist Marea eine Antwort auf die vorher existierende Konzentration von Anlandungspunkten in New York und New Jersey [98]. Beide Orte wurden durch den Orkan Sandy im Jahr 2012 stark beeinträchtigt, so dass es zu Internet-Ausfällen von mehreren Stunden zwischen den USA und Europa kam. Um die Verwundbarkeit der transatlantischen Infrastruktur zu verringern, haben sich die Betroffenen (Microsoft und Facebook) für den Bau des Kabels entschieden – unabhängig von klassischen Kabelbetreibern. Telxius ist dem Konsortium während der Planungsphase beigetreten. Im Gegensatz zu Microsoft und Facebook besteht die Expertise von Telxius im Bau und Betrieb solcher Kabel.

Telxius betreibt neben Marea auch BRUSA und die Anlandungsstelle für Dunant in Virginia Beach. Damit konzentrieren sich wichtige Unterseekabel zwischen Europa, Nord- und Südamerika auf Telxius.

5.3.4 Fallstudie: Google Fiber

Die Breitbandanbindung von Privathaushalten ist in den USA deutlich eingeschränkt (siehe Abschnitt 6.1.2). Um Netzinhalte mit hohen Datenraten und geringen Latenzen an die Endkunden zu übermitteln, hat Google im Jahr 2010 das Projekt „Google Fiber“ initiiert. Ursprünglich wurde der Dienst in der Metropolregion Kansas City aufgebaut und umfasst aktuell nach eigenen Aussagen 19 Städte in den USA. Google Fiber ist eine Tochterfirma von Alphabet.

Die Kosten für einen Endanschluss sind gering und transparent [99]. 1 Gigagbit-Anschluss kostet $70 pro Monat, 2 Gigagbit $100 pro Monat. Dennoch ist der Dienst weniger populär als ursprünglich vermutet, so dass der Ausbau von Google Fiber an mehreren Orten eingestellt wurde.

Google Fiber illustriert die Abhängigkeiten von Kommunen und Städten von IT-Unternehmen. Damit eine Region durch Google Fiber erschlossen wird, müssen sich Kommunen oder Städte dafür bewerben und infrastrukturelle Voraussetzungen schaffen. In einigen Fällen ist dies erfolgreich passiert, obwohl im Nachhinein der Ausbau von Goo-

(a) High-End-Geräte (b) Low-End (oder auch eingebettete) Geräte

Abbildung 5.10: Vergleich von Hardware-Ressourcen bei High- und Low-End-Geräten im IoT und exemplarische Betriebssysteme.

gle Fiber durch Alphabet aufgrund von wirtschaftlichen Defiziten eingestellt wurde. Die langfristige Entwicklung von Google Fiber bleibt offen.

5.4 Endgeräte und Internet-Edge mit dem Internet der Dinge (IoT)

Das Internet der Dinge (IoT) wird zukünftig die Internet-Infrastruktur vom Edge heraus verändern. Das IoT beschreibt die Vernetzung von intelligenten Gegenständen mit dem Internet. IoT-Geräte lassen sich grob in zwei Klassen unterteilen (vgl. Abb. 5.10). (1) High-End-Geräte bringen Hardware-Ressourcen mit, welche nicht weit von klassischen Desktop-Rechnern entfernt sind, aber einen deutlich geringere Packungsdichte (*Form Factor*) aufweisen. Klassische Vertreter sind der Raspberry Pi und Smartphones. (2) Low-End-Geräte (oder auch eingebettete Geräte) hingegen sind nicht nur in ihrer Größe erheblich kleiner, sondern bringen auch weniger Speicher- und Rechenkapazitäten mit. Insbesondere sind diese Geräte in der Regel batteriegetrieben und setzen eine hohe Energieeffizienz voraus. Umgekehrt ist das Einsatzgebiet von Low-End-Geräten vielfältiger, da sie deutlich preiswerter und leichter verbaubar sind.

5.4.1 Low-End-IoT-Geräte

Bei Low-End-IoT-Geräten wird bei der Hardware zwischen drei gängigen Klassen differenziert [100]. Geräte der Klasse 0 verfügen $\ll$10 kB RAM und $\ll$100 kB ROM und sind alleine nicht Internet-fähig. Sie werden in der Regel vorkonfiguriert, während des Betriebs – wenn überhaupt – nur sehr selten verändert und mittels Proxies o.ä. an das Internet angebunden. Geräte der Klasse 1 mit $\sim$10 kB und $\sim$100 kB ROM können weiterhin keinen klassischen TCP/IP Netzwerk-Stack betreiben. Protokolle wie HTTP oder TLS entfallen. Klasse 1 Geräte können aber auf das IoT zugeschnittene Protokolle wie z.B. CoAP oberhalb von UDP nutzen. Insbesondere sind solche Geräte in der Lage, eigenständig Si-

cherheitsprotokolle, z.B. DTLS, zu nutzen. Die Speicherressourcen der Klasse 2 Geräte mit ∼50 kB und ∼250 kB ROM erlauben in der Regel den Einsatz von Netzwerkprotokollen, wie sie auf Smartphones, Desktops oder Servern genutzt werden.

Klassische Beispiele für den Betrieb von IoT-Geräten sind u.a. die Gebäudeautomatisierung, intelligente Autos und Industrieanlagen. Der Markt der eingebetteten Geräte nimmt eine Schlüsselfunktion für den Erfolg des Internets der Dinge ein, wie eine umfangreiche Studie von McKinsey [101] belegt. Kombiniert man diese Prognose mit der Vorhersage großer Hersteller wie Intel und Cisco, dass in den nächsten fünf Jahren mehr als 50 Milliarden IoT-Geräte eingesetzt werden, dann ergeben sich für den zukünftigen Internet-Edge erhebliche Änderungen. Es werden deutlich mehr leistungsschwache Geräte über Gateway-Architekturen oder ressourcenfreundliche Protokolle eingebunden. Damit werden sich die Protokolle deutlich von dem herkömmlichen Internet-Protokollstapel unterscheiden.

5.4.2 Gefährdungspotential durch das IoT

Mit der Erweiterung des Edges durch IoT-Geräte entsteht auch ein neues Gefährdungspotential sowohl für die Internet-Infrastruktur (vgl. Abschnitt 5.5) als auch die Privatsphäre der Nutzer. Dabei sind nicht nur Consumer-Geräte betroffen. Vielen Herstellern und Betreibern von IoT-Geräten fehlt die IT-Expertise. Eine Studie aus dem Jahr 2020 hat gezeigt, dass proprietäre Industriesteuerprotokolle in der Regel unverschlüsselt funktionieren, die entsprechenden Geräte aber an das Internet angeschlossen werden, so dass Angreifer Passwörter im Klartext sehen oder mit den Geräten ohne Authentifizierung direkt kommunizieren können [102, 103]. Weiterhin ist bekannt, dass Hersteller von Consumer-IoT-Geräten, wie z.B. Fernsehern, abhängig vom Einsatzort der Geräte unterschiedliche Daten erheben [104].

5.5 Verteilte Denial-of-Service-Angriffe

Denial-of-Service-Angriffe (DoS-Angriffe) haben zum Ziel, die Ressourcen des Opfers zu überlasten. Die Art der Ressourcen ist vielfältig und kann z.B. Speicher- und CPU-Kapazitäten, aber auch Netzbandbreiten betreffen. Entscheidend ist, dass durch die Überlast der Ressourcen ein Internet-Dienst nicht mehr angeboten oder genutzt werden kann. Ebenfalls ist die Art des Opfers unterschiedlich. DoS-Angriffe zielen auf einzelne Nutzer, kleinere Firmen, globale Marktführer oder Netzinfrastrukturbetreiber ab. Es werden hierfür einzelne Endgeräte, Server-Farmen oder Netzübergänge attackiert. Dies erfolgt häufig durch die Erzeugung eines hohen Verkehrsvolumens, da somit die Netzkommunikation grundsätzlich gestört wird. Angreifer gehen hierbei meist verteilt vor, indem sie von unterschiedlichen Orten im Internet den Angriff ausführen, um die Schlagkraft zu erhöhen und die Rückverfolgung zu erschweren. Sogenannte Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) sind ein alltägliches Phänomen im Internet, zumal kleine DDoS-Angriffe kostengünstig und unproblematisch über Booter-Portale eingekauft werden können [105].

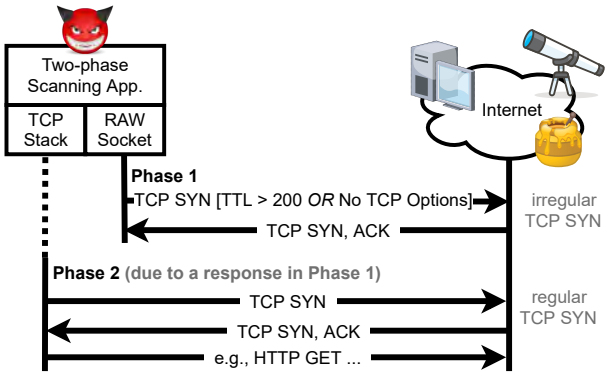


Abbildung 5.11: Zwei-Phasen Scanner.

5.5.1 Auswirkungen von Angriffen auf das Internet-Ökosystem

DDoS-Angriffe stellen eines der größten Probleme für Netzbetreiber dar, da sie Netzübgergänge ganzer Städte stören können [106]. Selbst wenn der Netzübergang selber nicht Ziel des Angriffs ist, sondern ein Endgerät, kann dieser als Kollateralschaden betroffen sein, da er durch die erzeugte, hohe Verkehrslast verstopft. DDoS-Angriffe zu erkennen bevor sie das Opfer erreichen, ist nicht trivial, da die erzeugten Daten wie normaler Internet-Verkehr erscheinen. Die Erkennung wird umso schwieriger, je verteilter der Angriff ist.

Neuartiges Vorgehen von Angreifern

Für die Durchführung von DDoS-Angriffen werden häufig Bot-Netze genutzt, die durch die Übernahme fremder Geräte aufgebaut werden. Um solch verwundbare Rechner zu identifizieren, scannen Angreifer das Internet, d.h. sie schicken spezifische Messpakete an alle verfügbaren IP-Adressen. Eine aktuelle Studie [107] zeigt, dass Angreifer deutlich informierter vorgehen als bisher vermutet.

Zwei-Phasen Scans Um den IP-Adressraum möglichst schnell zu durchsuchen, implementieren Angreifer sogenannte zwei Phasen-Scans [107]. In der ersten Phase wird geprüft, ob für eine bestimmte IP-Adresse ein bestimmter Transportport offen ist, d.h. ein entsprechender Server-Dienst (z.B. HTTP) läuft, um diesen in einem zweiten Schritt zu übernehmen. Die erste Phase wird derart implementiert, dass das Senden der Scan-Pakete möglichst wenig Zeit benötigt. Dafür bedienen sich Angreifer dem Konzept des zustandslosen, asynchronen Scannings, welches mit der Veröffentlichung von ZMap [108] hohe Popularität erfahren hat, z.B. bei der Umsetzung des Mirai-Angriffs. Hierbei werden Pakete direkt über den RAW-Socket (statt über den OS-eigenen Netzwerkstack) verschickt. Die Pakete weisen dadurch bestimmte Eigenschaften in den Paketköpfen auf (hohe TTLs, keine TCP-Optionen). Diese *irregulären Pakete* lassen sich leicht identifizieren, werden aber von bösartigen und gutartigen Scannern gleichermaßen erzeugt.

Sobald die Gegenstelle des Scans mit dem Aufbau einer TCP-Verbindung antwortet, leitet der Eingreifer die zweite Phase ein. Die zweite Phase dient der eigentlichen Infiltrierung des Server-Dienstes. Hierfür folgt der Angreifer dem regulären Protokollverhalten und sendet anwendungsspezifische Daten.

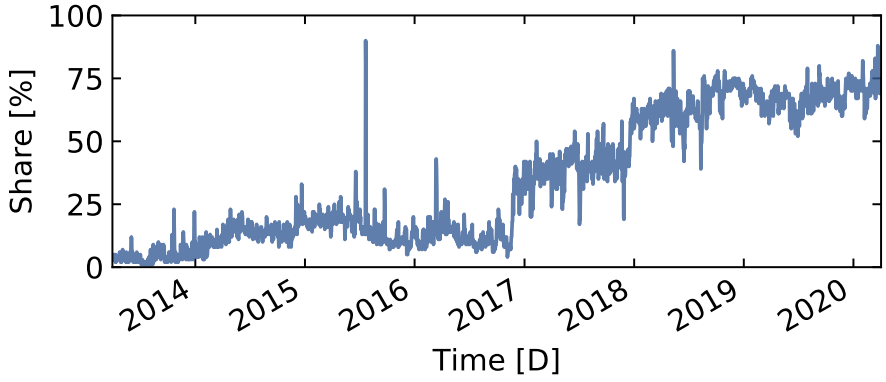


Abbildung 5.12: Anteil der IPv4-Pakete mit einer $TTL > 200$ beobachtet an einem Netzwerk-Teleskop seit 2013. (Quelle: Hiesgen *et al.* 2021)

Beobachtet man den Anteil der IPv4-Pakete mit einer irregulären IP-TTL von einem größeren Netzwerk-Teleskop aus, dann werden zwei Eigenschaften sichtbar (siehe Abb. 5.12).

1. Ein IPv4-Netz, das selber keine Internet-Dienste anbietet, empfängt fast 100% irreguläre IPv4-Pakete im Vergleich aller empfangenen IPv4-Pakete in diesem Netz.

2. Der Anteil der irregulären IPv4-Pakete steigt seit 2013 kontinuierlich. Der Zeitpunkt korreliert mit der Veröffentlichung von ZMap.

3. Ein weiterer Anstieg ist ab Ende 2016 zu beobachten. Der Zeitpunkt ist ca. drei Monate versetzt zu der Veröffentlichung des Quellcodes der Mirai-Schadsoftware am 30. September 2016.

Gemessen an der Zahl der IP-Pakete hat Scanning demnach in den letzten sieben Jahren den Verkehr innerhalb des Internet-Ökosystems verändert. Zudem werden zwei Dinge deutlich. Zum einen das Aufgreifen von wissenschaftlichen Ergebnissen in schädlichen Kontexten. Angreifer bedienen sich Methoden und Scripte, die durch Wissenschaftler generell bereitgestellt werden. Zum anderen die Wichtigkeit der flächigen und langfristigen Beobachtung des Internet-Verkehrs mittels Netzwerk-Teleskope. Das U.S. Department of Defense hat kürzlich den unbenutzten IP-Adressbereich `11.0.0.0/8` aktiviert [109] und entsprechende Routen im Internet annonciert. Über die tatsächliche Nutzung wird noch spekuliert, aber die Vermutung ist, dass in diesem Adressbereich Honeypots u.ä. Beobachtungswerkzeuge installiert werden, um potentielle Angreifer besser zu verstehen. Diese Form der Angriffsdetektion hat messbare Folgen auf das Internet-Ökosystem. Es sind ungefähr 4% mehr IP-Adressen als vorher erreichbar, die Zahl der Routing-Einträge steigt um mehrere Größenordnungen und die mittlere annoncierte Präfixlänge sinkt.

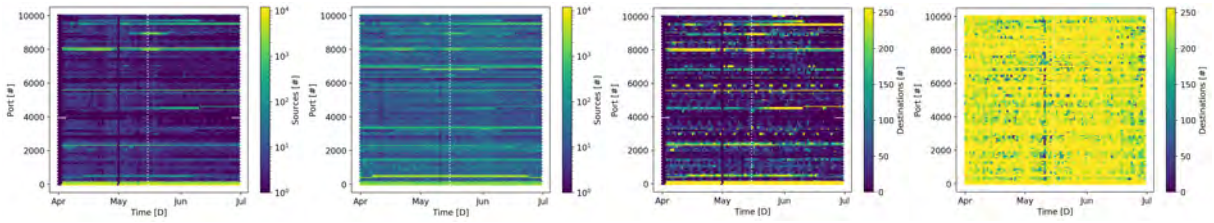
IP-Topologie und geographischer Kontext Zwei-Phasen Scanner unterscheiden sich von Scannern mit einer Phase [107]. Abb. 5.13 illustriert die Anzahl unterschiedlicher Quell- und Ziel-IP-Adressen, die die ersten 10.000 TCP-Ports scannen bzw. Scan-Pakete empfangen. Es sind deutliche Unterschiede zwischen Scannern mit einer und Scannern

mit zwei Phasen sichtbar. Die dargestellten Beobachtungen wurden an einem Netzwerk-Teleskop in den USA aufgezeichnet. Ähnliche Ergebnisse zeigen sich auch in Europa.

Zwei-Phasen Scanner gehen zielgerichtet beim Erkunden des IP-Adressraums vor. Abb. 5.14 zeigt die relative Verteilung der von einem Scanner erkundeten Transportports für einen Beobachtungspunkt in den USA und einen in Europa. Ungefähr 25% aller Scans sind nur in Europa sichtbar. Insbesondere die Ports TCP/1433 und TCP/7547 werden ausschließlich in Europa angegriffen. Der Grund hierfür liegt voraussichtlich in den damit verknüpften Diensten. TCP/1433 wird in SIMATIC-Steueranlagen der europäischen Firma Siemens genutzt. Bis vor wenigen Jahren erlaubte ein Software-Bug den Root-Zugriff über diesen Port auf das System. TCP/7547 wird von dem Protokoll TR-069 genutzt, welches auf Home-Gateways für den Fernzugriff verwendet wird. TR-069 war (und ist) in Europa weitverbreitet.

Ebenfalls zielgerichtet ist das Scan-Verhalten innerhalb des Adressraums, das von europäischen Quell-IP-Adressen ausgeht. Sechs der zehn häufigsten IP-Präfixe, die Scanner in Europa anbinden, sind sowohl untereinander topologisch benachbart als auch benachbart zum Ziel-IP-Präfix. Folgendes Beispiel dient der Illustration. Ein Netzwerk-Teleskop beobachtet den IP-Adressbereich `1.2.10.0/24`. Mit hoher Wahrscheinlichkeit stammen dann die Scans von IP-Adressen aus den IP-Präfixen `1.2.1.0/24` und `1.2.2.0/24` etc, welche sich übergeordnet zu `1.2.0.0/16` zusammenfassen lassen. Ein solches Verhalten konnte nur in Europa, nicht aber in den USA beobachtet werden.

Zusammenfassend lässt sich feststellen, dass rein passive Beobachtungspunkte im Internet-Ökosystem unzureichend sind, da eine neue Welle von Angreifern, Zwei-Phasen Scanner, ihr Angriffsverhalten erst nach einer Antwort vom Ziel offenbaren. Des Weiteren sind viele der Zwei-Phasen Scanner bösartig und gehen fokussiert hinsichtlich der Geographie und Topologie vor. Entsprechend sollte bei der Auswertung von Honeypot-Daten, Teleskop-Daten etc. differenziert werden. Beobachtungen, die z.B. in einem Land gewonnen werden, lassen sich nicht unmittelbar auf andere Länder übertragen. Viele Angreifer gehen nicht mehr blind vor, sondern berücksichtigen den Deployment-Stand von Software in einzelnen Ländern.



(a) Zwei Phasen. Quellen. (b) Eine Phase. Quellen. (c) Zwei Phasen. Ziele. (d) Eine Phase. Ziele.

Abbildung 5.13: Anzahl der verschiedenen Quell- und Ziel-IP-Adressen, die die ersten 10k Ports angreifen bzw. Angriffe registrieren. Zwei-Phasen Scanner gehen zielgerichteter bei den Ports vor, scannen dafür breiter im IP-Adressraum. Zeitraum: April - Juli 2020. (Quelle: Hiesgen *et al.* 2021)

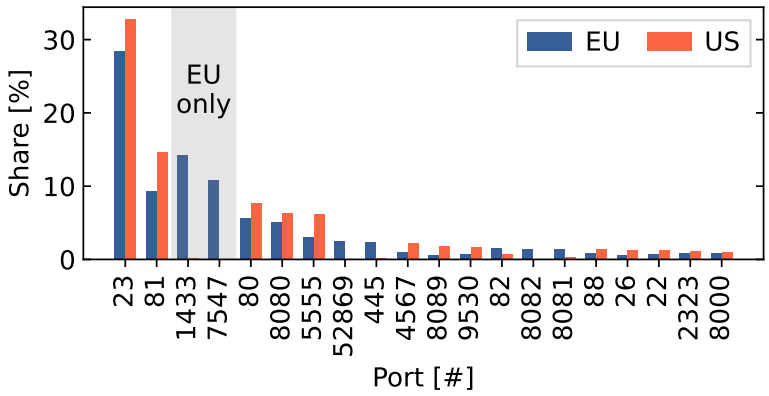


Abbildung 5.14: Verteilung der gescannten Top-20 Ports. 25% aller Scans sind nur in der EU sichtbar. (Quelle: Hiesgen *et al.* 2021)

Informationszentrische Netzwerke für das inhärente Verhindern von DDoS-Angriffen

Die durch DDoS-Angriffe ausgehende Gefahr ist eine der Motivationsgründe für die Erforschung neuartiger Netzarchitekturen. Informationszentrische Netzwerke (*Information-centric Networks*, ICN) stellen einen interessanten Ansatz dar, da sie die Netzkommunikation konzeptuell vollständig neu umsetzen. Der aktuell populärste Ansatz ist das sogenannte Named-Data Networking (NDN), welches explizit die inhärente Überwindung von DDoS als Grund für den Entwurf eines neuen Internet-Paradigmas angibt [110, 111].

Alle ICN-Ansätze [112] vereint die Aufgabe des bisherigen Ende-zu-Ende-Prinzips. Viele ICN-Ansätze, insbesondere NDN, überwinden DDoS-Angriffe auf Endgeräte, indem die Kommunikation auf dem sogenannten *Get-Response*-Ansatz basiert: Ein Endgerät erhält nur dann Daten, wenn es diese Daten vorher angefragt hat. Damit erhält es keine (ungewollten) DDoS-Pakete. Dies steht im fundamentalen Gegensatz zum bisherigen Internet. Das Internet-Protokoll erlaubt es, Internet-Pakete an eine beliebige IP-Adresse zu schicken. Die Aufgabe des Netzes ist, die Internet-Pakete zuzustellen, unabhängig davon, ob ein Empfänger diese angefragt hat oder nicht.

Internet der Dinge

Das Internet der Dinge nimmt in der Diskussion von DDoS-Angriffen einen besonderen Stellenwert ein. Einerseits vereint es besonders schützenswerte Internet-Geräte, da diese Alltagsgegenstände, Produktionsmaschinen etc. darstellen. Andererseits sind diese Geräte leicht angreifbar, da sie aus Kostengründen häufig schlecht geschützt werden. Veraltete Firmware beispielsweise ist oft ein Grund für die erfolgreiche Übernahme der Geräte durch Angreifer [113]. Insbesondere IoT-Geräte aus dem Consumer-Bereich waren bereits in der Vergangenheit die Basis für große verteilte Bot-Netze, von denen aus DDoS-Angriffe durchgeführt wurden.

Infolge der schlechten Absicherung von IoT-Geräten gibt es zunehmend Bestrebungen nach umfangreicher Regulierung in diesem Umfeld. Es muss dabei aber vor Überregulierung gewarnt werden. Das Drängen auf einheitliche Standards und Normen [114] ist

sicherlich ein wünschenswerter Weg. Kritisch wird es aber bereits bei aufwändigen Zertifizierungsverfahren, die womöglich jungen, innovativen Unternehmen den Marktzutritt erschweren. Der teilweise vorherrschende Wunsch nach vollständig geschlossenen IoT-Systemen, bei denen der Besitzer des IoT-Geräts keinen Einfluss auf die dort laufende Software hat, erhöht die Abhängigkeit von Kunden und Herstellern. Solche Bestrebungen widersprechen dem Erfolgsmodell des Internet und begünstigen langfristig Konsolidierungen. Bei Consumer-Geräten sollte der Besitzer die freie Wahl der dort verwendeten Software haben.

Im Gegensatz zu herkömmlichen Internet-Geräten haben IoT-Endgeräte momentan ein wohldefiniertes Kommunikationsumfeld. Die meisten IoT-Geräte kommunizieren über ein Gateway mit einem Cloud-Backend, welches die gewonnenen Daten aufbereitet und als Vermittler zu weiteren Endgeräten (z.B. Smartphones, PCs) dient. Konsolidierungseffekte oder Herstellerabhängigkeiten werden dabei als Sicherheitsvorteil vermarktet: Wenn das IoT-Endgerät mit wohldefinierten Endpunkten kommuniziert, lassen sich Anomalien im Verkehrsverhalten auch leichter erkennen. Einen flexiblen Ansatz stellt die *Manufacturer Usage Description Specification (MUD)* [115] dar. Hierbei ist das IoT-Endgerät in der Lage, über eine Datei mit Meta-Informationen dem Netzwerk legitime Kommunikationsendpunkte und Dienste mitzuteilen. Obgleich dieser Ansatz eine offene Schnittstelle zwischen IoT-Endgerät und Netzwerkinfrastruktur darstellt, um z.B. Filterlisten gerätespezifisch zu konfigurieren, wirkt er Konsolidierungen nur bedingt entgegen. Die Meta-Informationen in den MUD-Dateien müssen bereitgestellt werden. Wenn dies nicht durch den Hersteller erfolgt, der seine Cloud-Infrastruktur favorisiert, müssten diese Informationen durch den Nutzer (Kunden) selbst erzeugt werden. Die damit verbundene Komplexität würde einen sehr informierten Endnutzer oder leicht zu bedienende Werkzeuge erfordern, um erfolgreich zu sein.

5.5.2 Mitigationsmaßnahmen im Kontext der Konsolidierung

DDoS-Angriffe mit einem hohen Angriffsvolumen können aktuell nur von wenigen Internet-Betreibern oder Mitigationsdienstleistern erfolgreich unterdrückt werden. Das erfolgreiche Unterdrücken eines aktiven DDoS-Angriffs erfordert das Filtern von Internet-Verkehr möglichst an der Quelle des Verkehrs oder an kanalisierenden Übergangspunkten.

Blackholing

In den letzten Jahren hat *Remotely Triggered Blackholing* hohe Popularität bei der Eindämmung von DDoS-Verkehr erfahren. Die Idee ist, dass ein Opfer-Netzwerk über das Border Gateway Protocol eine Blackhole-Route an seine Nachbarn signalisiert, welche auf leistungsfähigere Komponenten verweist, die letztlich den DDoS-Verkehr verwerfen. Ein solcher Dienst wird zunehmend von großen öffentlichen Internet-Austauschpunkten angeboten. Sie haben den Vorteil, dass sie per se zwischen mehreren Netzen vermitteln. Die dortigen Route Server stellen zudem eine leichtgewichtige zentrale Komponente für die breite Routen-Verteilung dar. Eine Studie aus dem Jahr 2019 [53] zeigt aber, dass der momentane Einsatz von Blackholing an einem IXP deutlich weniger wirksam ist als er sein könnte. Nur 50% des ungewollten Verkehrs wurde erfolgreich verworfen. Der Grund

hierfür liegt in den Default-Einstellungen für BGP Policies. Eine gängige Richtlinie besagt, dass BGP-Routen mit einer IPv4-Präfixlänge `>/24` nicht akzeptiert werden sollen. Häufig werden aber deutlich spezifischere Blackhole-Routen (insbesondere `/32`) bekanntgegeben, um den Kollateralschaden beim Verwerfen zu minimieren – eine `/32`-Route beschränkt das Verwerfen auf eine einzelne IP-Adresse statt auf einen größeren Adressbereich. Damit die Blackhole-Route dennoch akzeptiert wird, müssten die Netzbetreiber explizit Ausnahmen zulassen.

Solche Missverständnisse sind nicht selten, da vielen kleineren Netzbetreibern das entsprechende Hintergrundwissen fehlt. Umso wichtiger ist es, dass Blackholing-Anbieter nicht nur den Schutz vor bösartigem Verkehr an sich bewerben, sondern auch klare und vollständige Instruktionen aufbereiten, wie dieser erfolgreich genutzt werden kann. Ebenso wichtig ist eine sorgfältige Überwachung des Dienstes. So ist z.B. nicht nur die Zahl der annoncierten Blackhole-Routen oder die Zahl der Netzbetreiber, die das tun, wichtig, sondern auch deren Effektivität, d.h. die Zahl der Netze, die diese akzeptieren.

Blackholing hat den Nachteil, dass es meistens einen Kollateralschaden erzeugt. Blackhole-Routen zielen auf IP-Adressen (z.B. `1.2.3.4/32`) nicht auf Anwendungsdienste (z.B. `TCP/80` für HTTP auf `1.2.3.4/32`). Selbst wenn die Blackhole-Route nur eine einzelne IP-Adresse umfasst, wird der gesamte Internet-Verkehr zu dieser Adresse, also dem Opfer, verworfen. Der Angriff ist somit weiterhin erfolgreich, es werden aber andere IP-Endgeräte geschützt, da die Netzübergänge nicht überlastet werden.

Scrubbing Center und DDoS Open Threat Signaling

Um den Kollateralschaden von Blackholing zu umgehen, gibt es grundsätzlich zwei Ansätze. Zum einen erlauben *Scrubbing Center* (z.B. Neustar, Prolexic/Akamai) das „Waschen“ des Internet-Verkehrs. Hierbei wird der Internet-Verkehr zum Opfer-Netz in die Infrastruktur des Scrubbing-Anbieters mittels BGP umgeleitet. Dort befindliche Infrastruktur-Komponenten analysieren den Internet-Verkehr und verwerfen die bösartigen Pakete. Der verbleibende Verkehr wird an den Kunden wieder ausgeleitet. Das Anbieten eines solchen Scrubbing-Dienstes bedarf ein umfangreiches, leistungsfähiges Backbone-Netz, das nicht viele Firmen betreiben. Große Content-Delivery-Netzwerke sind hierbei deutlich im Vorteil, da sie bereits an vielen Austauschpunkten vor Ort sind. Im Gegensatz zu Eyeball-ISPs oder Transit-ISPs haben sie zudem Messinfrastrukturen, die netzübergreifend die Ende-zu-Ende-Qualität ermittelt, um die Platzierung der Content-Server zu optimieren. Im Jahr 2014 hat Akamai Prolexic, einen der damals führenden DDoS-Mitigatoren, übernommen. Auch andere global relevante CDNs, wie z.B. Cloudflare oder Fastly, bieten DDoS-Mitgationsdienste an. Es kann davon ausgegangen werden, dass zukünftig in diesem Umfeld eine stärkere Konsolidierung für Web-basierte Dienste erfolgen wird.

Eine weitere Alternative für das Verhindern von Kollateralschäden bei der Bekämpfung von DDoS-Angriffen ist das feingranulare Filtern, z.B. anhand des Transportprotokolls und -ports. Das in der IETF standardisierte Rahmenwerk *DDoS Open Threat Signaling (DOTS)* [116] stellt dabei einen herstellerübergreifenden Ansatz dar. Das DOTS-Protokoll erlaubt es einem angegriffenen Netzwerk, netz- und betreiberübergreifend Meta-Daten über den zu filternden Verkehr an DDoS-Mitigatoren zu übermitteln. DOTS wurde

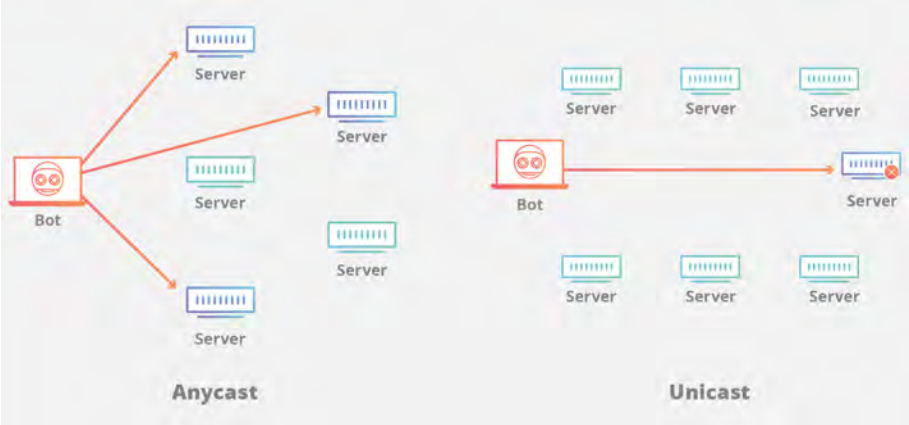


Abbildung 5.15: Anycast zur Abwehr von DDoS-Angriffen. (Quelle: Cloudflare)

stark von Arbor Networks (jetzt Netscout) vorangetrieben, einem führenden Anbieter im Bereich der DDoS-Bekämpfung und der Netzüberwachung. Es gibt Implementierungen von DOTS und erfolgreiche Interoperabilitätstests. Eine umfangreiche Verbreitung steht aber noch aus und kann, betrachtet man den Verlauf innerhalb der IETF, momentan bezweifelt werden. Dies ist insofern bedauerlich, als dass DOTS helfen könnte, Konsolidierungen im Sicherheitsumfeld aufzubrechen. Eine solcher Signalisierungsansatz könnte anregen, dass sich mittlere und kleinere autonome Systeme in einem P2P-Verfahren untereinander direkt helfen.

Anycast

Um bei einem DDoS-Angriff das Angriffsvolumen auf ein einzelnes Ziel abzuschwächen, setzen einige Betreiber auf *Anycast*. Bei Anycast werden die angefragten Inhalte auf mehrere, geographisch verteilte Server hinterlegt. Abhängig vom Standort des anfragenden Endgeräts werden die Daten vom dem nächstgelegenen Server zugestellt. Damit wird im Falle eines Angriffs der (bösartige) Verkehr automatisch auf mehrere Rechenzentren verteilt (siehe Abb. 5.15).

Anycast kann auf unterschiedlichen Schichten implementiert werden. Besonders effektiv umgesetzt wird es auf der Netzwerkschicht. Bei der DDoS-Mitigation muss es sogar auf der Netzwerkschicht erfolgen, da Angreifer IP-Adressen als Ziel wählen.

An sich sind CDNs prädestiniert, DDoS-Mitgationen mittels Anycast durchzuführen, da diese Inhalte per se geographisch verteilt in unterschiedlichen Rechenzentren vorhalten. Das Problem ist aber, dass viele CDNs Anycast mittels DNS umsetzen. Hierbei würden abhängig vom Ort des Angreifers unterschiedliche IP-Adressen einem Namen zugeordnet werden. Diese Indirektion hilft nicht, wenn die Angreifer im DDoS-Fall als Eingabe IP-Adressen nutzen.

Das CDN Cloudflare geht hier anders vor und implementiert Anycast direkt auf der Netzwerkschicht mittels BGP. Mögliche Indirektionen entfallen. Anfragen an eine einzelne IP-Adresse werden automatisch ortsabhängig vom Angreifer diversifiziert. BGP Anycast gilt gemeinhin als komplex in der Umsetzung. In jedem Fall bedarf es umfangreicher

Peering-Beziehungen mit Upstream-Providern und stabil konfigurierter Routen, damit der Netzwerkverkehr nicht zwischen mehreren *Points of Presence* oszilliert.

5.6 Übersicht von Regierungsaktivitäten als Antwort auf aktuelle Internet-Konsolidierungen

Die Konsolidierungen im Internet, seiner Dienste und Anwendungen sind eng mit der Frage nach der Hoheit über Daten verbunden. Um die Konsolidierung der Daten auf einige wenige Firmen zu reduzieren, versuchen einige Staaten die Kontrolle über die Daten mittels Gesetzen, Sanktionen u.ä. im eigenen Land zu halten. Die dabei eingesetzten Mittel können umgekehrt von den Ländern selber genutzt werden, um die Freiheit des Internet im eigenen Land zu beschneiden.

5.6.1 Übersicht zur Freiheit im Internet

Die Freiheit des Internet wird regelmäßig von der NGO „Freedom House“ für 65 Länder bewertet [117]. Diese Länder decken 87% der aktuellen Internet-Nutzer ab. Der dabei erzeugte Index *Freedom on the Net* untersucht pro Land drei Themen: (*i*) Schwierigkeiten beim Internet-Zugriff (*Obstacles to Access*), (*ii*) Einschränkungen auf Internet-Inhalte (*Limits on Content*) und (*iii*) Verletzung der Nutzerrechte (*Violations of User Rights*). Jedes Teilthema wird separat mit einem Index bewertet; der Gesamtindex ist die Summe der Teilindizes.

Abb. 5.16 zeigt die Teilindizes für den aktuellen Untersuchungszeitraum Juni 2019 bis Mai 2020. Bei einer genaueren Analyse der Länder zeigt sich, dass der Wunsch nach einem souveränen Internet-Ökosystem für die Bevölkerung häufig als Argument genutzt wird, eben solche Gesetze einzuführen, die den Staat selber Möglichkeiten der Überwachung und Zensur gestatten. Dieses Spannungsverhältnis wird in Abb. 5.17 illustriert.

Die aktuelle Studie von Freedom House beobachtet die Bemühungen um die eigene „Cyber-Souveränität“ einzelner Regierungen, wobei jeder Staat seine eigenen Internet-Regulierungen aufstellt. Diese Regulierungen versuchen, den Informationsfluss über Landsgrenzen hinweg einzugrenzen. Solche Aktivitäten stehen dem ursprünglichen Internet entgegen, das auf einem offenen, pluralen und konsensgetriebenen Ökosystem basiert.

5.6.2 Zusammenfassung ISOC Global Internet Report 2019

Die Konsolidierungsbestrebungen innerhalb des Internet werden von vielen Staaten als kritisch angesehen. Dabei sehen Staaten nicht nur die Kontrolle des Internet durch einige wenige große Technologiefirmen als Gefahr, sondern deren finanzielle Vormachtstellung im Allgemeinen. Allein der Marktwert von Apple belief sich im Jahr 2020 auf 2 Billionen USD [118] und entspricht damit einer ähnlichen Größenordnung des Bruttoinlandsprodukts von Deutschland (3,8 Billionen USD) oder Frankreich (2,6 Billionen USD). Zu den von Regierungen aufgegriffenen Gegenmaßnahmen [119] zählen u.a.:

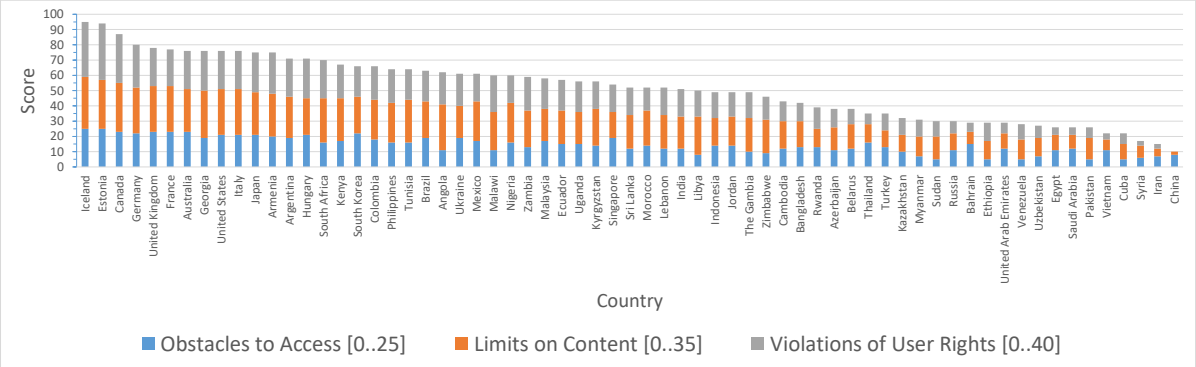


Abbildung 5.16: Internet Freedom Index für 65 Länder, Untersuchungszeitraum Juni 2019 - Mai 2020. Ein höherer Wert signalisiert weniger Einschränkungen. (Datenquelle: https://freedomhouse.org/countries/freedom-net/scores)

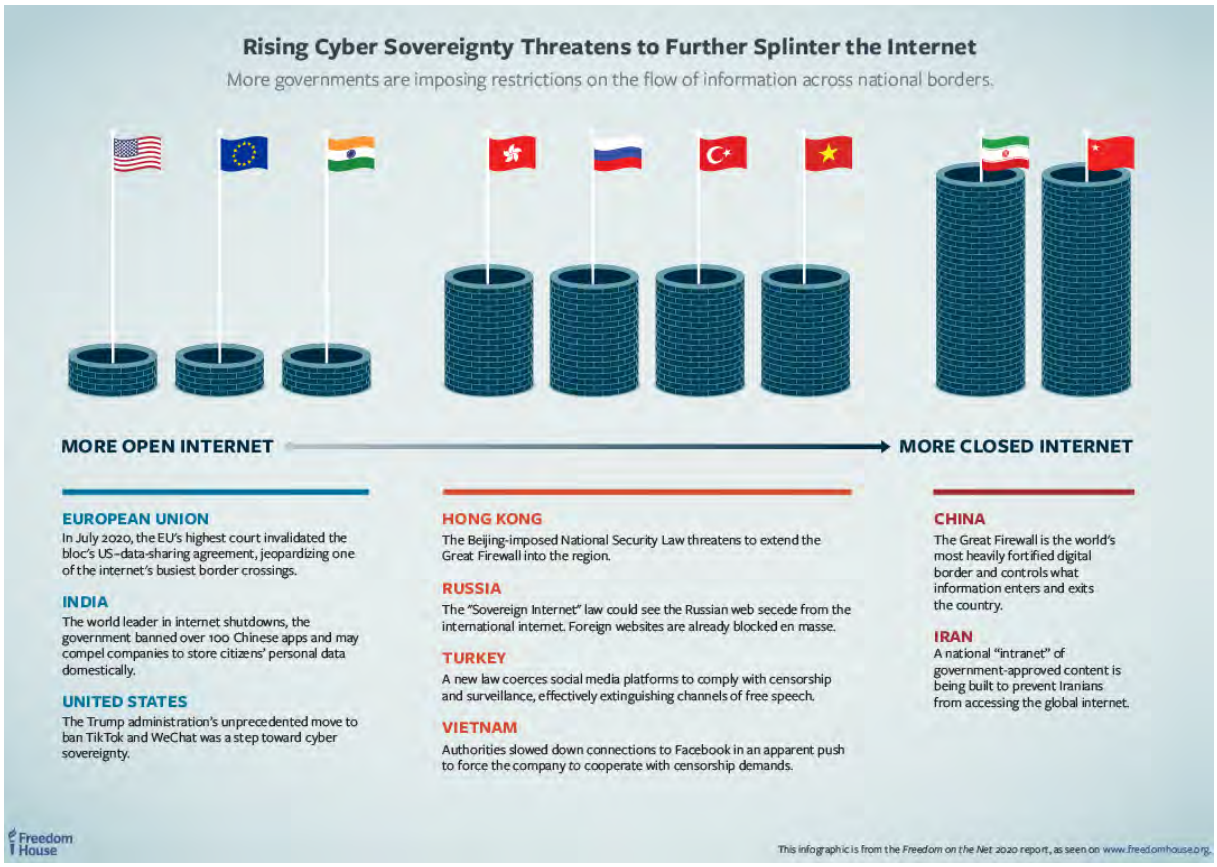


Abbildung 5.17: Spannungsverhältnis von Souveränität im Cyberraum und Offenheit des Internet (Quelle: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow)

1. Gesetze, die den Datenaustausch innerhalb des eigenen Landes sicherstellen (z.B. Russland, China, Indonesien und Vietnam). Hierzu zählen z.B. Vorgaben, dass Anbieter von öffentlichen Internet-Diensten die zugehörige Infrastruktur in lokalen Rechenzentren installieren.

2. Vorschriften zum Datenschutz. Die Datenschutzgrundverordnung der EU ist ein Beispiel, in dem die Verarbeitung personenbezogener Daten geregelt wird, so dass Endnutzer der Erhebung ihrer Daten nicht nur explizit zustimmen müssen, sondern auch die Transparenz jeglicher Datenverarbeitung gestärkt wird. Damit wird u.a. verhindert, dass Daten an Dritte ohne Zustimmung verkauft werden, wodurch auch eine Konsolidierung von Informationen verhindert werden kann. Andere Beispiele sind der *California Consumer Privacy* (Januar 2020) in den USA und die *African Union Convention on Cyber Security and Personal Data Protection* (Juni 2014).

3. Spezifische Steuern, um lokale Unternehmen nicht zu gefährden. Zambia erhebt beispielsweise Steuern auf Internet-basierte Kommunikation, um die Dienste lokaler, klassischer Telekommunikationsanbieter finanziell attraktiver erscheinen zu lassen. Dabei ist aber anzumerken, dass die Überwachung der klassischen Kommunikation einfacher ist im Vergleich zu Internet-basierter Kommunikation.

Die Internet Society hebt in ihrer Studie [119] explizit hervor, dass sowohl die Konsolidierungstrends als auch mögliche Gegenmaßnahmen zwiespältig zu sehen sind, da sie sowohl positive als auch negative Seiteneffekte zur Folge haben.

5.6.3 Fallbeispiel Russland

Russland gehört zu den Ländern, die die Offenheit des Internets als Gefahr sehen. Infolgedessen wird an dem Aufbau einer souveränen IT-Infrastruktur, *RuNet*, gearbeitet, so dass der für Russland relevante Teil des Internets unabhängig von ausländischen Providern und Dienstanbietern funktioniert. Die dafür notwendigen Voraussetzungen werden durch Gesetze geschaffen [120]. Von zentraler Bedeutung ist die Behörde *Roskomnadsor*, welche 2008 als „Föderaler Dienst für die Aufsicht im Bereich der Informationstechnologie und Massenkommunikation“ gegründet wurde.

RuNet Ab dem 1.November 2019 müssen russische Internet-Dienstleister ihre IT-Systeme so gestalten, dass sie von Roskomnadsor kontrolliert werden können. Ziel ist es, dass das „russische Internet“ autark funktioniert, wenn es zu einem Angriff kommt. Die Infrastruktur umfasst alle Betreiber von technischen Kommunikationsnetzwerken, Internet-Austauschpunkten, Verbindungen außerhalb der Landesgrenzen und autonome System. Ein separates nationales Domain Name System soll einen unter russischer Verwaltung betriebenen Namensraum schaffen. Praktisch bedeutet dies, dass russische Provider auch ohne eine Verbindung zu den üblichen Root DNS Servern Namen auflösen können. Der autarke Betrieb von RuNet wird durch simulierte Abkopplungen vom globalen Internet gerprüft. Die erste Simulation fand im Dezember 2019 statt. Vier weitere Ausfälle waren im Jahr 2020 geplant, welche aber aufgrund der COVID-19-Pandemie verschoben wurden.

Die gesetzlichen Vorgaben definieren nicht nur Internet-Austauschpunkte, die Anbindung von Servern etc., sondern auch den Einsatz spezifischer Hardware für die Aufzeich-

nung des Internet-Verkehrs, der Nutzerdaten und der Paketanalyse (Deep Packet Inspection). Die damit verbunden Kosten tragen die Internet Service Provider, wodurch sich die Kosten für den Netzbetrieb erhöhen. Diese Kosten werden auf die Endnutzer umgelegt Für das Jahr 2020 wurde von Preissteigerungen von bis zu 18% ausgegangen, wodurch einkommensschwarche Bevökerungsgruppen langfristig von einem Internet-Zugang ausgeschlossen werden könnten.

Seiteneffekt Zensur Die staatliche Kontrolle von Internet-Zugängen und der Verbreitung von Internet-basierten Inhalten wird auch für die vereinfachte Ausübung von Zensur genutzt. So müssen z.B. Suchmaschinen Inhalte auf Basis vorgegebener Listen filtern. Die Unterbindung des Nachrichten-Dienstes Telegram durch das Filtern von IP-Adressen war nur bedingt erfolgreich. Die Blockaden wurden im Juni 2020 eingestellt. Zum einen haben viele Nutzer über Proxies alternative Zugangswege gefunden. Zum anderen ist ein Teil der Backend-Infrastruktur über Cloud-Dienstleister (Google Cloud, Microsoft Azure etc.) erreichbar. Das Filtern der Cloud-Server hat einen zu hohen Kollateralschaden verursacht, da andere Dienstleister wie z.B. Banken oder Online-Geschäfte ebenfalls blockiert wurden.

5.6.4 Fallbeispiel Indonesien

Indonesien zählt zu den Ländern mit partieller Internet-Freiheit [121]. Die Regierung schränkt den Zugang zum Internet oder Internet-Inhalten situativ ein, z.B. um Proteste innerhalb des Landes zu erschweren oder weil die Inhalte gesetzlich verboten sind.

Im Notfallsituationen kann das Ministerium für Kommunikation und Information den Zugriff auf Social Media Plattformen einschränken. Nach den Wahlen im April 2019 wurden Internet Service Provider angewiesen, den Zugang zu Plattformen wie Facebook, Instagram Twitter und Whatsapp zwischen dem 22. und 24. Mai zu unterbinden, um die Verbreitung von Fehlinformationen zu verhindern, nachdem es in Folge der Wahlen zu gewalttätigen Ausschreitungen kam.

Internet-Dienste werden von wenigen großen Telekommunikationsfirmen angeboten, von denen einige dem Staat gehören. Die *Indonesian Internet Service Provider Association (APJII)* kritisiert, dass die Kosten für die Beantragung einer ISP-Lizenz zu hoch sind.

Für die Erkennung von illegalen Inhalten nutzt die indonesische Regierung ein eigenes System („Cyber Drone 9“), welches Webseiten durchsucht und basierend auf KI-Methoden die Inhalte klassifiziert. ISPs werden dann ggf. angewiesen, die Kommunikation zu den entsprechenden Web-Servern zu blockieren. Die technische Umsetzung der Filter bleibt den ISPs selber überlassen, wodurch es (teilweise gewollt) zu der Blockierung weiterer Inhalte kommen kann. Dadurch entsteht eine inkonsistente Zensur von Inhalten über Provider hinweg.

Anfang 2020 wurde bekannt, dass das indonesische Militär zehn News-Webseiten betreibt bzw. finanziert, um regierungsfreundliche Nachrichten zu verbreiten [122]. Die Etablierung neuer Informationskanäle als Gegengewicht zu etablierten, wenn auch kommerziell getriebenen Informationsangeboten ist demnach nicht per se positiv zu bewerten. Um der zunehmenden Manipulation von Nachrichten innerhalb des Landes zu begegnen, gibt es unterschiedliche Initiativen außerhalb der Regierung. Die Webseite „Cekfakta“ (https://cekfakta.com/) erlaubt Nutzern eine Art Faktencheck von Informationen. Des

Weiteren wurde vom Presserat, einem unabhängigen Gremium, ein Barcode-Verfahren eingeführt, mit dem zuverlässige Medienseiten identifziert werden können. Hierfür müssen die Betreiber der Medienseiten separat akkreditiert werden. Es gab Bedenken, dass ein solches Verfahren etablierte Informationsquellen bevorzugt und neue Mitbewerber benachteiligt.

Kapitel 6
Gesellschaftliche und wirtschaftliche Konsequenzen

In diesem Kapitel stehen die gesellschaftlichen und wirtschaftlichen Auswirkungen der verschiedenen Konsolidierungsentwicklungen im Vordergrund. Wir betrachten hierbei sowohl die Perspektiven der Internet-, als auch der Realwirtschaft sowie Aspekte ihrer Auswirkungen auf das Internet-Ökosystem und die Gesellschaft als plurales Gesamtsystem. Insbesondere soll dabei versucht werden, die widerstreitenden Kräfte und Interessen zu identifizieren und zu bewerten, wie diese sich in den unterschiedlichen Marktsegmenten und gesellschaftlichen Kontexten widerspiegeln.

Dabei wird auch die Rolle der Staaten als Gesetzgeber und Regulierer berücksichtigt. Dies soll sowohl exemplarisch bzgl. bestehender Regelungen und Strategien zur Infrastrukturversorgung, Marktregulierung und Informationsfreiheit geschehen, Aufsichts- und Regulierungsbedarfe sollen aber auch als künftige Handlungsfelder identifiziert werden.

Das sehr breite Spektrum gesellschaftlicher Aspekte wird exemplarisch insbesondere an den Bereichen Informationszugang, Informationsverarbeitung und -hoheit, technische sowie wirtschaftliche Fairness und Transparenz beleuchtet. Ferner sind Diskussionen zur zivilen Sicherheit und Katastrophenschutz sowie ausgewählte, vorsichtige Ausblicke auf gesellschaftliche Auswirkungen von Strukturentwicklungen geplant.

6.1 Entwicklungstrends in der Internet-Ökonomie

Die Internet Society (ISOC) definiert Internet-Ökonomie in ihrem Global Internet Report [119] als alle wirtschaftlichen Aktivitäten, die das Internet befördern oder fundamental von seiner Existenz abhängen. Die ISOC sieht im Wesentlichen drei Domänen, in welche sich die Internet-Wirtschaft gliedern lässt (vgl. Abbildung 6.1): Die Kern-Infrastruktur, den Internet Zugang und die Anwendungsplattformen. Dabei diagnostiziert die ISOC Schwierigkeiten, die Marktbereiche gegeneinander abzugrenzen, da in diesem Technologiemarkt komplementäre Interessen ineinander übergehen und Geschäftsgebiete oft schnell mutieren.[1]

Die Grundkonzepte des Internets sind Erreichbarkeit, Offenheit und Skalierbarkeit:

[1] Ein Beispiel hierfür ist Amazon: Primär als Online-Händler gestartet, dominiert inzwischen das Cloud-Geschäft, welches gegenwärtig wiederum in den IoT- und Datenmarkt expandiert.

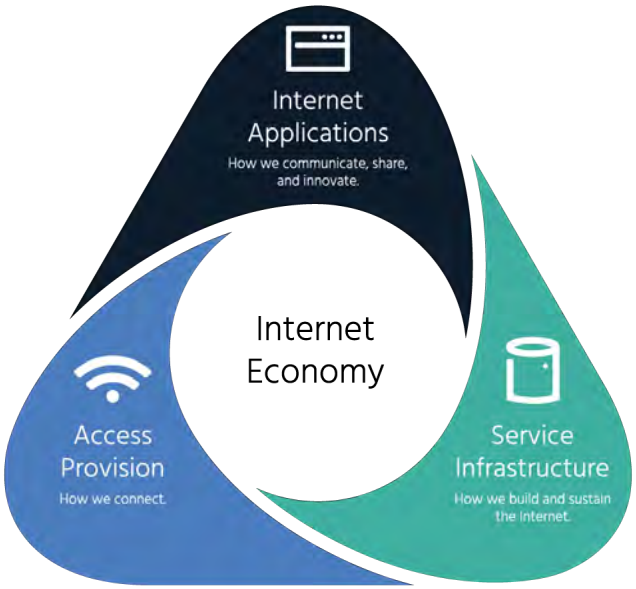


Abbildung 6.1: Die drei Domänen der Internet-Ökonomie (Quelle: Internet Society)

Das Internet ist in seinem Kern nach transparenten Standards und Regeln gebildet, welche es bestehenden genauso wie neuen Akteuren erlauben, die Teilhabe auf allen Ebenen zu erweitern und so ein bedarfsgerechtes Wachstum zu ermöglichen. Betreiber von Infrastruktur und Basisdiensten können genauso das Netz erweitern wie Anwendungsentwickler oder neue Endkunden.

Dieses dynamische Entwicklungspotential wird eindrucksvoll belegt durch die Verbreitung der Smartphones. Während im Jahr 2007 praktisch kein U.S.-Haushalt über ein Internet-verbundenes mobiles Telefon verfügte, waren mehr als 80% der Haushalte im Jahr 2019 im Besitz eines solchen Smartphones [Mobile Fact Sheet, [123]].

Auch wenn die skalierbare Erweiterung des Netzes an sich technisch einfach und unbeschränkt bleibt, können ökonomische Faktoren der eigentlichen Entwicklung entgegenstehen:

> "Expanding a network in its original form may be fairly straightforward, but more complex changes to the operation of a network can be problematic, both because such changes may threaten to disturb the shared rules that make the network function and because the players who would need to invest in the change may find that they are not able to recoup a sufficient share of the benefits from other players in the market to make it worthwhile."
>
> —— Shane Greenstein [124]

Hemmschwellen, die einen Ausbau des Internets beschränken, liegen einerseits in hohen Investitionskosten für physische Infrastruktur, etwa *Investitionen in die Kernnetzinfrastruktur* oder *Investitionen in die Zugangsnetzinfrastruktur*. Beschränkend wirken aber auch "weiche Ressourcen" wie etwa die *Verfügbarkeit von IPv4-Adressen* oder etablierte *faktische Monopoldienste* auf der Anwendungsschicht wie der Google Suchdienst, gegen dessen marktbeherrschende Stellung schwer anzutreten ist.

Insbesondere die internetweiten Anwendungsdienste, die sowohl Funktionen wie Kundenbindungen auf globalem "Internet-Maßstab" besitzen, scheinen gegenwärtig einen schwer einholbaren Trend zur Marktkonsolidierung zu treiben. Google, Amazon, Facebook und Apple (GAFA) hatten 2018 gemeinsam einen Börsenwert, der größer als das Bruttosozialprodukt von Frankreich war. Gemeinsam mit Microsoft operieren sie in Märkten mit ausgeprägten "winner-take-all" Eigenschaften [125].

Die Internet Society identifiziert Konsolidierung im Jahr 2019 als einen dominanten, aber ambivalenten Trend.

> "The Internet Society recognises that the impact of consolidation and concentration on the Internet economy as well as on the open, interoperable, and global Internet are difficult to gauge. [...] there are benefits to operating at scale. Consolidation and concentration can also greatly benefit the user by providing platforms that offer seamless Internet experiences. At the same time, it's unclear what the impact is on innovation, entrepreneurship and, importantly, competition. It's unclear what concentration and consolidation may mean for user choice, including choice of content, services, and provider."
>
> — The Internet Society [119]

Hochskalierbare Großsysteme wie z.B. die Google Suchmaschine bieten einerseits Leistungspotentiale und Nutzererfahrungen, die nur durch ihre Größe möglich werden. Andererseits bedrohen Großsysteme als Monopolplattformen die Offenheit des Internet-Ökosystems. Gerade diese Offenheit bildet seit langem das Fundament für die Innovationskraft des Internets, weil in der breiten, globalen Pluralität der Erfinder und Entwickler langfristig Unkonventionelles und Neues besser gedeihen als in großen Firmenhierarchien.[2]

Pluralität ist als Grundprinzip eines global vernetzten Handelns unverzichtbar, funktioniert aber nur auf der Basis offener Kommunikationsstandards. Diese Standards waren bei der Entwicklung von Anwendungs-Großsystemen oft nicht vorhanden oder wurden regelmäßig zugunsten proprietärer Anwendungslösungen ignoriert. In der Wirkung entstanden singuläre, monopolartige Dienste, welche auch durch unkritisches Konsumverhalten populär wurden: Mit der bereitwilligen Installation proprietärer Client-Software, z.B. WhatsApp, wurden vorhandene, leistungsfähige Standards, z.B. XMPP, im Alltag verdrängt.

6.1.1 Internet Core Infrastruktur

Tier1

Tier1 Internet Transit Provider erbringen zwei Kerndienstleistungen: (1) Bereitstellung von Konnektivität bei sehr hohen Datentransferraten und (2) Herstellung globaler Präfix-Erreichbarkeit in der sogenannten *Default-free Zone* (Default-freien Zone), das Angebot also, jedes Präfix im Internet erreichen zu können. Die gegenwärtig etwa 15 Tier1

[2] Die mehr als 40-jährige Entwicklungsgeschichte der Firma Microsoft illustriert diese Entwicklung lehrbuchartig.

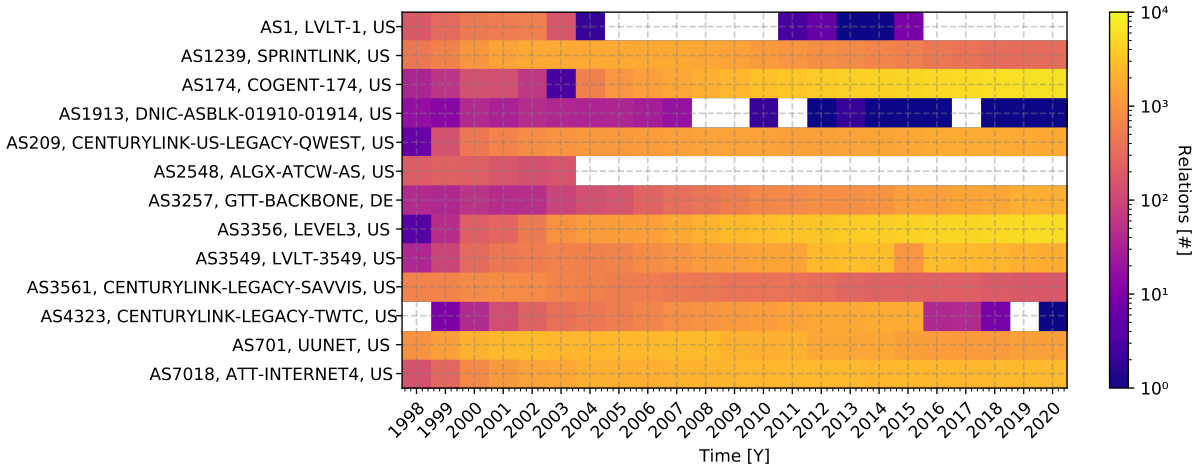


Abbildung 6.2: Akkumulierte top-fünf ASes nach Anzahl der C2P-Beziehungen

Internet Provider bilden eine Clique von gegenseitig verbundenen Routing-Topologien, deren gemeinsamer Customer Cone das ganze globale Internet darstellt. Ohne eine solche Default-freie Hierarchieebene ist die gegenwärtige Routing-Logik des Internets nicht funktionsfähig. Tier1-Provider sind insofern für das Funktionieren des Internets unverzichtbar.

Die kleine Gruppe von Tier1 Providern besteht relativ stabil auf der Ebene der Autonomen Systeme. Abbildung 6.2 zeigt alle (13) ASes, die in den vergangenen 22 Jahren mindestens einmal zu den top fünf Providern gemessen an der Größe ihrer Customer Cones gehört haben. Die zugrundeliegenden Daten entstammen dem CAIDA AS-Ranking [126]. Hiernach hält Level 3, der größte (bis 2017 unabhängige) Transit-Dienstleister, 53% aller Autonomen Systeme in seinem Customer Cone.

Strukturelle Veränderungen in Richtung einer Konsolidierung im Tier1 werden praktisch ausschließliche durch Übernahmen vorgenommen. So wurde MCI (AS 2548) von Verizon und Level3 2017 von CenturyLink (jetzt Lumen) übernommen, nachdem Level3 2011 den Tier1 Provider Global Crossing geschluckt hatte. Sprint wurde 2020 von T-Mobile (US), welches mehrheitlich zur deutschen Telekom gehört, aufgekauft.

Die in der Transitleistung herausragenden, AS-bezogenen Infrastrukturen wurden jedoch während der vergangenen zehn Jahre stabil betrieben und haben ihre strukturelle Bedeutung im Routing weitgehend behalten. Abbildung 6.3 visualisiert die Entwicklung im Routing der letzten zehn Jahre für die (kumulierten) top fünf Provider gemessen an ihren Pageranks. Pagerank [127] ist eine typische Zentralitätsmetrik, welche auch von Google zur Bewertung von Webseiten genutzt wurde. Der Rang eines Knotens ermittelt sich als die Summe aller relativen Ränge der Nachbarknoten, die mit dem ausgewählten Knoten verbunden sind.

Die wirtschaftliche Bedeutung von Tier1 Transit Providern am Markt ist nicht immer transparent und schwer zu bestimmen. Der Gesamtmarkt für internationalen Datentransfer im Internet ist auch in der fünften Dekade seines Bestehens noch wachsend und kann überschlägig wie folgt abgeschätzt werden: Das jährliche globale Wachstum an internationaler Transit-Kapazität liegt oberhalb von 30%, während die Transit-Preise um knapp

30% pro Jahr fallen, wobei die Preisentwicklungen regional sehr unterschiedlich verlaufen.[3] Saldiert ergibt sich ein Umsatzwachstum von $\geq 5\%$.

Die Transitbetreiber werden jedoch von verschiedenen Seiten bedrängt. Einerseits entwickeln sich regionale Peering-Strukturen insbesondere an Internet Exchange Points (IXPs) mit hoher Dynamik. Andererseits errichten CDN- und andere OTT-Betreiber eigene globale Verteilinfrastrukturen, die nicht nur IP-Verkehr durch private Netze routen, sondern auch Kabelinfrastrukturen einschl. Unterseekabeln beinhalten. Google und Microsoft verfügen inzwischen über Customer-Cones, welche nurmehr von den zwei Tier-1 Providern Level-3 und Hurrican Electric übertroffen werden.[4] Die Entwicklung der Investitionen in die Kabelinfrastruktur zeigt Abbildung 6.4 differenziert nach Unternehmenstyp. Demnach ziehen sich die traditionellen Transitprovider zunehmend aus dem Kabelgeschäft zurück, welches einerseits spezialisierte (Tochter-)Unternehmen, andererseits die großen Content-Provider zu je einem Drittel übernehmen.

Die Kabelinfrastruktur, insbesondere auch die Seekabel, bilden die physische Grundlage für das internationale Transitgeschäft. Gleichzeitig ist der Markt für die Glasfaserbereitstellung ein sehr schwieriger, in welchem langfristige Kapitalbindungen für kurzfristige Nutzerverträge bereitgestellt werden müssen. Hierbei ist bedenkenswert, dass Technologieentwicklungen die mittlere Leistungsfähigkeit von Unterseekabeln in den vergangenen zehn Jahren auf 240 Tbit/s vervierzigfacht haben, so dass sehr hohe Abschreibungen auf ältere Kabelinvestitionen zu tätigen waren.

Nahezu alle Tier1 Netzwerkunternehmen verfügen ebenfalls über große Geschäftseinheiten für Endkunden, meist in den Segmenten (mobile) Zugangsnetze, Sprachdienste, Cloud- oder CDN-Infrastrukturen. Diese eigenen Kundenbasen erlauben den großen ISPs einerseits, die Auslastung ihrer Transitnetze zu optimieren, andererseits erhöht sie ihre

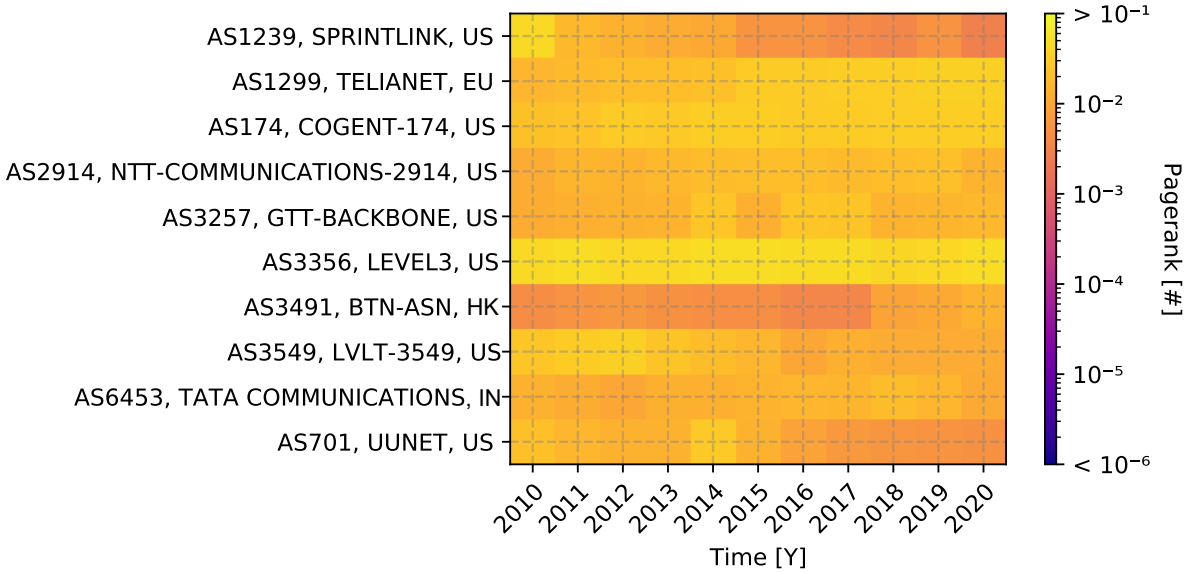


Abbildung 6.3: Akkumulierte top-fünf ASes nach Pagerank der C2P-Beziehungen

[3] vgl. `https://blog.telegeography.com/`

[4] `https://blog.apnic.net/2020/12/04/unpacking-a-flattened-internet/`

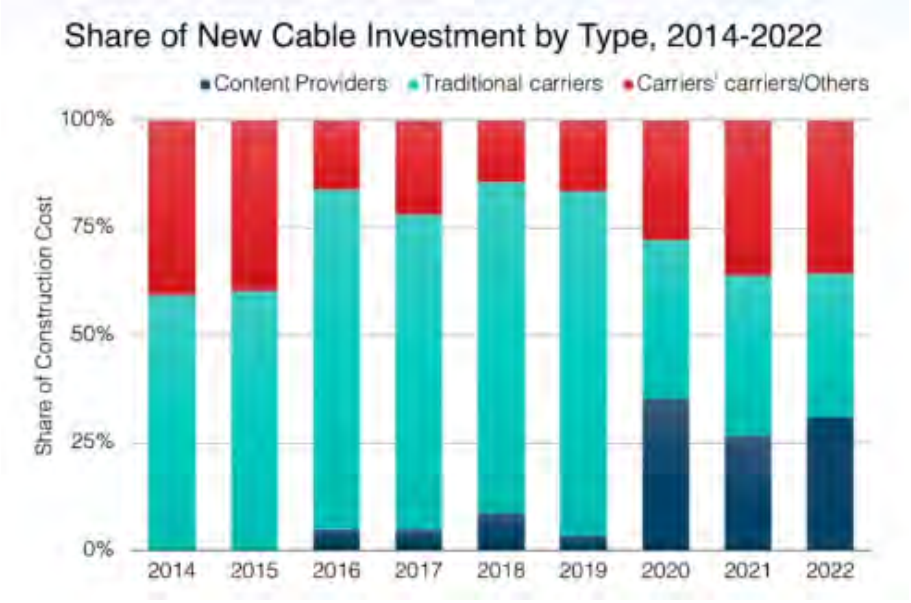


Abbildung 6.4: Entwicklung der Investorenverteilung in die Kabelinfrastruktur (Quelle: telegeography.com)

Bedeutung im Peering, da große Kundengruppen exklusiv erreicht werden. Schließlich bieten anwendungsnahe Dienste höhere Gewinnmargen und erlauben es den großen ISPs, unabhängiger von OTT-Providern agieren zu können.[5]

Internet Exchange Points

Internet Exchange Points (IXPs) liegt die Idee zugrunde, durch lokale Infrastrukturen einen preiswerten Datenaustausch bei geringen Latenzen zu ermöglichen. Sie schöpfen ihren ökonomischen Wert daraus, dass sie regional Internet-Bandbreite generieren, ohne von den Kosten des internationalen Transits oder der Weitverkehrsinfrastruktur abhängig zu sein. Ihr Nutzen ist in ihrer unmittelbaren Nachbarschaft am größten, wie Abbildung 6.5 veranschaulicht.

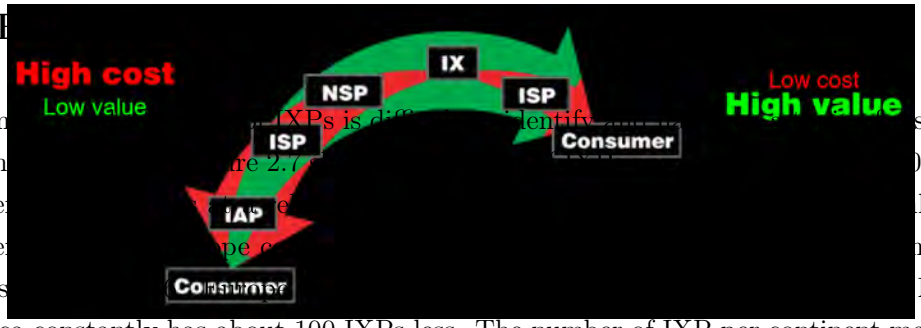
> "A cheap IX is probably a successful one. An expensive IX is always a failure."
>
> — Bill Woodcock, PCH[6]

In ihren Anfängen erforderten IXPs lediglich (ausgemusterte) Switches und zusätzliche Router-Ports der Provider im lokalen Rechenzentrum, um Austauschkapazitäten in Größenordnungen der Transitprovider bereitzustellen. Inzwischen hat sich die IXP-Landschaft sehr stark weiterentwickelt und diversifiziert. Während die Zahl der lokalen und regionalen IXPs kontinuierlich gewachsen ist (vgl. Abbildung 6.6), haben auch einzelne IXP-Betreiber – insbesondere in Südamerika und Europa – ihre Plattformen sehr

[5]Bereits 2011 wurde mit dem Ziel einer OTT-unabhängigen, kooperativen CDN Provider-Infrastruktur die IETF Arbeitsgruppe Content Delivery Networks Interconnection (cdni) zum Leben gerufen, deren Arbeit allerdings als wenig erfolgreich angesehen wird.

[6]`https://www.pch.net/resources/Papers/ixpr/IXP%20Backgrounder.pdf`

2.2 I



The im XPs is di lentify search over th re 2.7). The numbe e ly the numbe be c merica had its North America constantly has about 100 IXPs less. The number of IXP per continent may not be complete, but show the growth of IXPs. However, the fact that the number of IXP's is increasing does not show their importance.

Abbildung 6.5: Die Ökonomische Wirkung von Internet Exchanges (Quelle: Bill Woodcock, PCH)

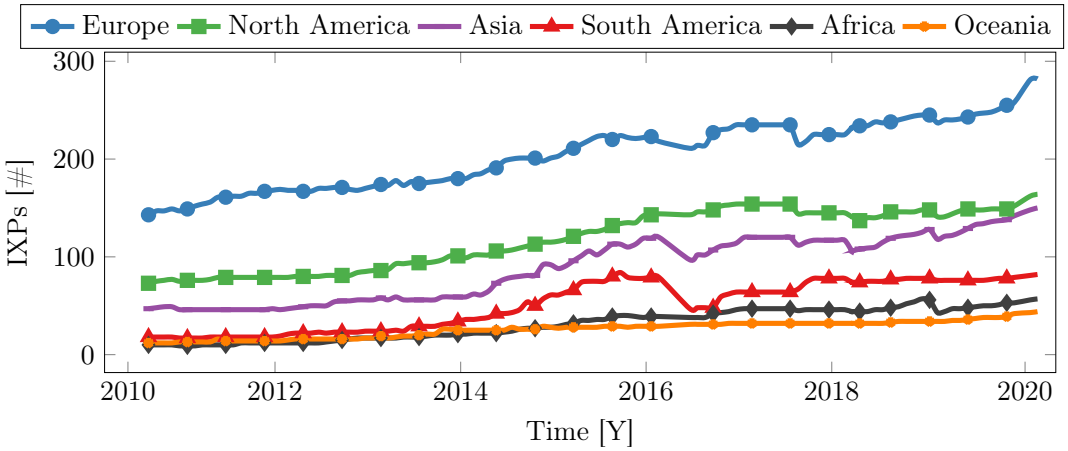


Abbildung 6.6: Entwicklung der IXP Anzahl per Kontinent basierend auf Daten von PeeringDB

Figure 2.7: Number of IXPs per continent [DB]

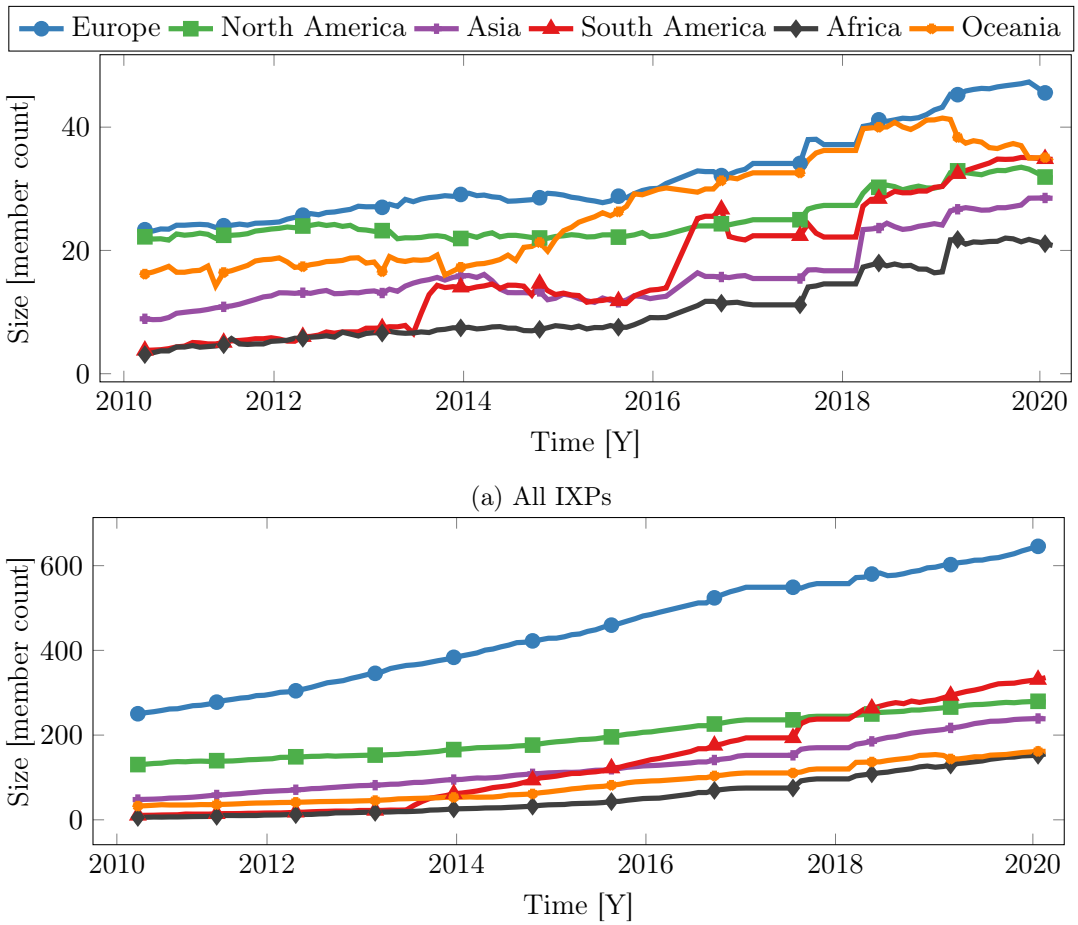
Chatzis et al. showed in 2013 that IXPs are more than "add-ons to an Internet dominated by large Tier-1 ISPs and large content providers/distributors" [14]. Lv et al. conclude that the impact of IXPs on the Internet is increasing [39]. In 2019 Böttger et al. investigated the impact of IXPs on path lengths and how IXPs reduce the need for a transit AS [6]. They showed that IXPs shorten the path lengths decisively, but the transit dependency of ASes still exist. Simultaneously, they observed that the central and large ASes steadily moved away from public peering on IXPs, while the less central and smaller ASes exhibit the opposite behavior.

groß ausgebaut. Viele IXPs erschließen heute Regionen statt einzelner Rechenzentren und konnten so die Teilnehmerzahlen auf ihren Plattformen stark erhöhen. Abbildung 6.7 schlüsselt die Mitgliederentwicklungen während der letzten zehn Jahre nach Kontinenten auf. Überdurchschnittliches Wachstum hat es in Europa und in Lateinamerika gegeben, wobei dies vor allem auf die größten fünf IXPs zurückgeht. Ein durchschnittlicher IXP in Nordamerika verbindet 30 Netze, wohingegen die fünf größten IXPs in Europa jeweils mehr als 600 (DE-CIX Frankfurt: mehr als 1.000) und in Südamerika mehr als 200 Teilnehmer aufweisen.

Sehr große IXPs wie der DE-CIX in Frankfurt, der AMS-IX in Amsterdam und der LINX in London betreiben seit kurzer Zeit eigenständig transkontinentale Weitverkehrsinfrastrukturen, teilweise um Dependancen, also Tochter-IXPs, zu verbinden, teilweise um Remote Peering-Angebote, also den Zugriff auf die IXP Switchplattform aus der Ferne, selbstständig vermarkten zu können. Wird die weitverteilte Infrastruktur betrachtet, ergeben sich noch deutlich höhere Konzentrationszahlen: Mehr als 2.200 Netze verbinden sich irgendwo zum DE-CIX (AMS-IX, Linx: 1.000), oft indem sie Zugangstransport aus der Ferne direkt oder über Wiederverkäufer erwerben. Diese sehr starke Konsolidierungstendenz einiger IXPs widerspricht ihrer originären Geschäftslogik. Der Entwicklungstrend ist aber noch zu jung, um seine wirtschaftliche Nachhaltigkeit beurteilen zu können.

with more than 45 members, Oceania and South America follow with 35 members. Africa has the smallest average size with less than 22 members.

The IXP size difference between the continents is larger for the top five IXPs per continent shown in Figure 2.15b. With almost 650 members Europe has the highest IXP size. In second place is South America with almost 300 fewer members. The size differences of IXPs between North America, Asia, Oceania and Africa are smaller. Figure 2.15c shows the sizes for rank 6 to 30. South America drops from second to fourth place. This indicates that South America has few very large IXPs and otherwise only small ones.



(a) All IXPs

(b) Top five IXPs

Figure 2.16: The historical evolution of the average IXP size by member count per continent

Abbildung 6.7: Entwicklung der mittleren IXP Mitgliederzahlen per Kontinent basierend auf Daten von PeeringDB

Die überregional agierenden IXPs präsentieren zwei zusätzliche Vermarktungsargumente: Zum einen bieten sie Firmen, die nicht selbst in einem regionalen ISP-Umfeld tätig werden wollen, Lokalkompetenz an. Ein Frankfurter Kunde des DE-CIX kann so Peerings in New York oder Dubai schalten lassen ohne je mit einem Verantwortlichen vor Ort verhandelt zu haben. Zum anderen versprechen große IXPs eine höhere Peering-Effizienz auf einer Plattform, welche bereits sehr viele Teilnehmer hat. Letztgenanntes Versprechen greift das Kerngeschäft der Tier1 Provider an, welche globale Konnektivität verkaufen. IXPs können dieses Versprechen gegenwärtig eher schlecht einlösen, weil sie – anders als Tier1 Provider – keine global optimierten Netze betreiben, sondern Verkehr über ihre speziellen PoPs leiten müssen.

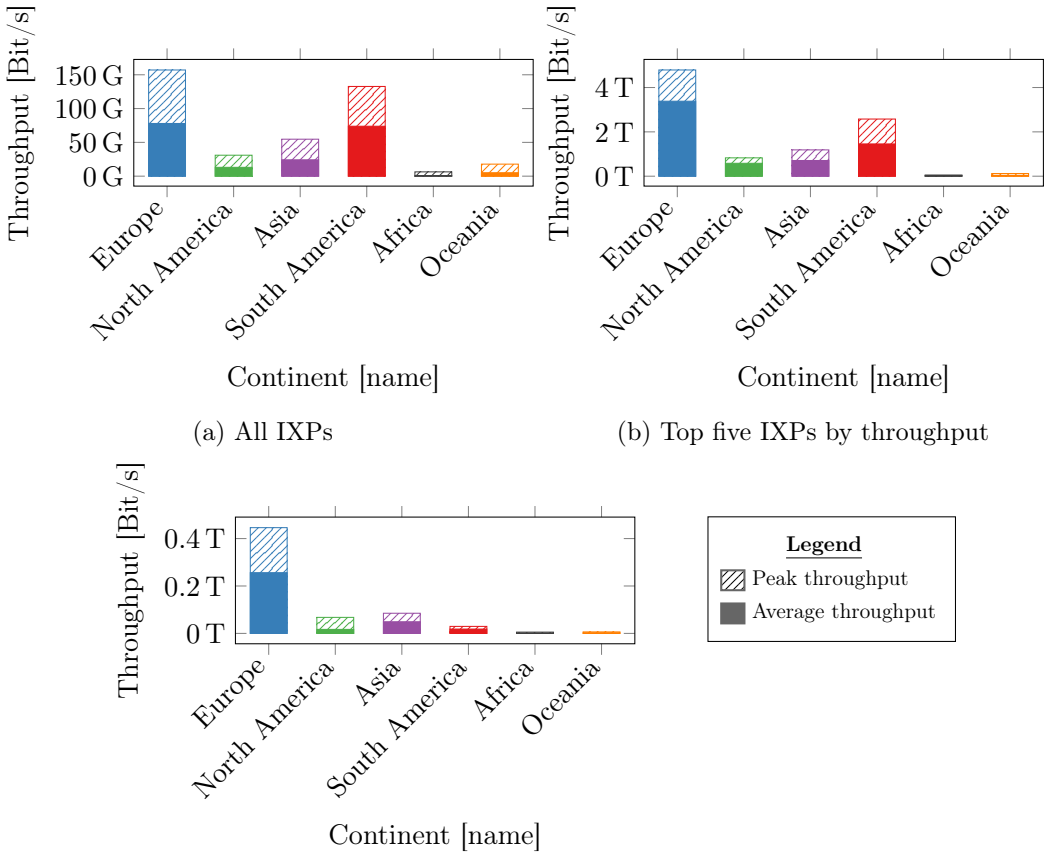
Insbesondere aber enthält das öffentliche Peering keine vollständigen Routing-Tabellen, so dass über IXPs nur Teile des Internets sichtbar werden. Böttger et al. [128] konnten zeigen, dass einzelne IXPs bis zu 70% des IP Adressraums im öffentlichen Peering erreichen, während 20% des IP Adressraums an IXPs vollständig unsichtbar bleibt und nur über Tier1 ISPs erreicht wird. Komplementär konnten die Autoren beobachten, dass große ASes und Transitprovider sich mehr und mehr aus dem öffentlichen Peering an IXPs zurückziehen, während ASes mit kleinem Customer Cone zum öffentlichen Peering streben — eine Entwicklung, die der transitorientierten Strategie der großen IXPs zuwider läuft.

> "Im öffentlichen Diskurs sehen wir als DE-CIX bei einigen unserer über 1.000 Kunden alleine in Frankfurt den Unmut, dass das Thema Peering von einigen wenigen der großen Markteilnehmer nur rudimentär genutzt wird."
>
> —– Thomas King, DE-CIX[7]

Die Entwicklung der großen IXPs wird nur durch erhebliche Investitionen in Infrastrukturen, insbesondere auch durch das Anmieten von Leitungskapazitäten im regionalen, nationalen und auch transkontinentalen Maßstab möglich. Dies erhöht eindrucksvoll die Durchsatzkapazitäten, wie Abbildung 6.8 aufzeigt: Die großen europäischen und südamerikanischen IXPs übertreffen die durchschnittlichen amerikanischen IXPs um mehr als zwei Größenordnungen. Dies erhöht aber auch die Kosten, wie Abbildung 6.9 zeigt: Europäische IXPs sind um ein Vielfaches teurer als nordamerikanische IX-Zugänge. Ein mittelgroßer IXP wie der Berliner BCIX stellt für einen 10 Gbit/s Zugang immer noch mehr in Rechnung als jeder nordamerikanische IXP. Beachtenswert ist hierbei, dass es vielfach in den USA, aber auch auf allen anderen Kontinenten kostenlose Exchange-Services gibt, die Rechenzentrumsbetreiber ihren Kunden mit der Kolokation zur Verfügung stellen. Die hohen Anschlußkosten steigern die Anreize, lokale Kostenvorteile da zu ziehen, wo es einfach möglich ist: Bilaterales Peering zwischen Providern vor Ort, die hohe Datenvolumen austauschen. Ein solcher Rückzug auf bilaterales privates Peering erhöht die Routing-Komplexität und schwächt das öffentliche Peering.

In ihrer Orientierung nach Größe in den Datenaustauschvolumina orientieren sich viele europäische IXPs an den großen, internationalen Content-Providern und bemühen sich primär um die Präsenz von Google, Facebook, Amazon, Akamai, etc.. Verträge mit diesen

[7] `https://www.golem.de/news/de-cix-nutzer-leiden-unter-geringem-peering-grosser-netzbetreiber-2103-155030.html`



(a) All IXPs

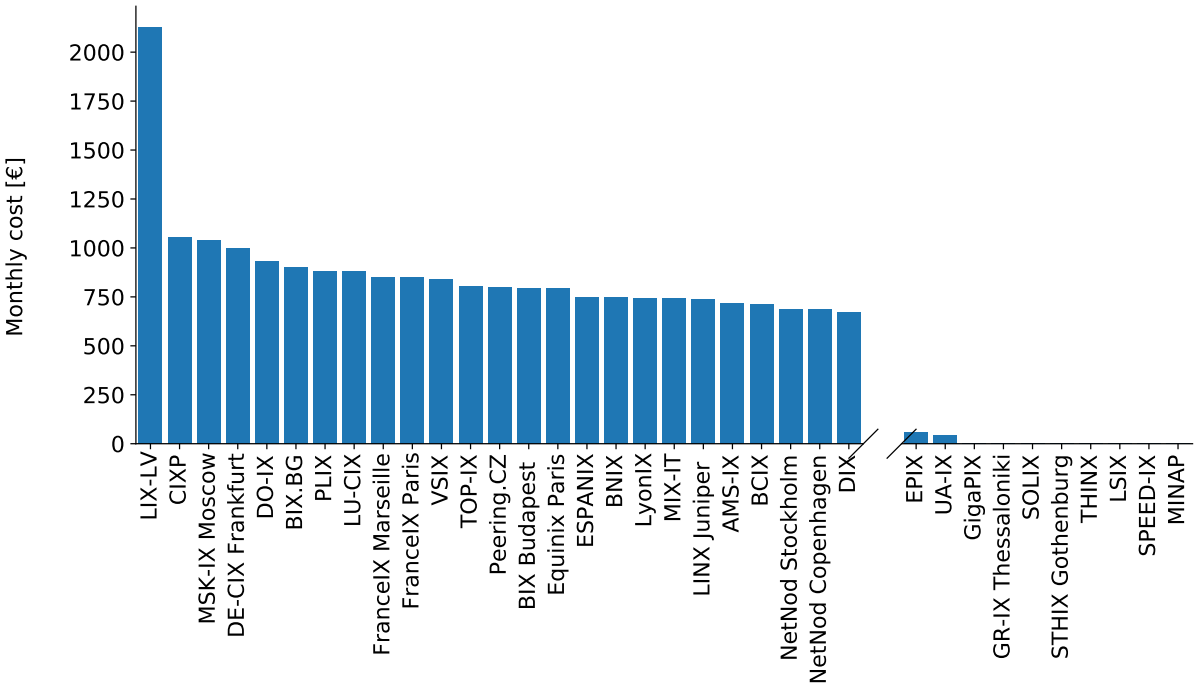
(b) Top five IXPs by throughput

(c) Rank 6 to 30 IXPs by throughput

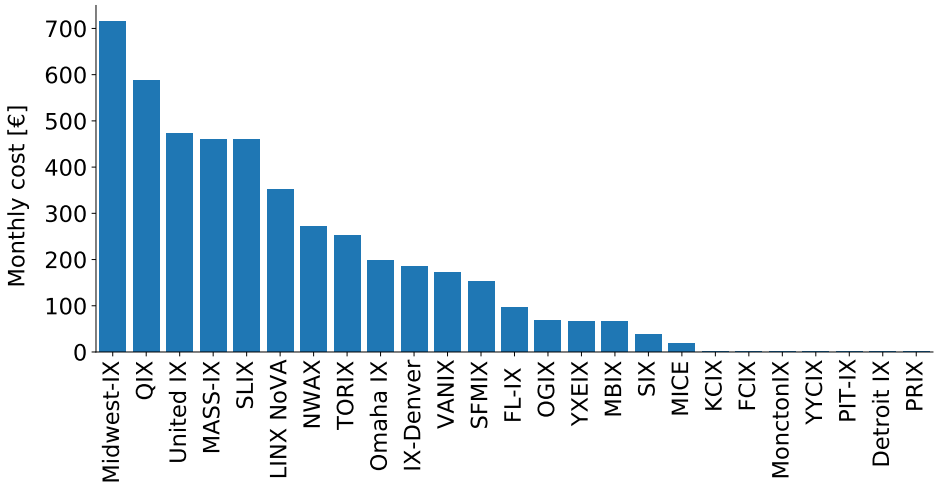
Figure 2.30: IXP throughput per continent (PCH)

Abbildung 6.8: Mittlere IXP-Datenkapazitäten pro Kontinent basierend auf Daten von PCH

Capacity utilization of IXPs: The calculated maximum throughput values are significantly greater than the real throughput values from PCH. There are tow possible explanation, the possible double counting of physical connections, as mentioned above, which could affect the behavior of resellers, as well as the fact that only for a subset of IXPs are throughput values available.



(a) Europäische IXPs nach Kosten gerankt



(b) Nordamerikanische IXPs nach Kosten gerankt

Abbildung 6.9: Monatliche Kosten eines 10G Anschlusses an IXPs in Europa und Nordamerika basierend auf Daten von Snijders et al.

Partnern erhöhen schnell die Portvolumina und Transferstatistik und zwingen darüber hinaus die Eyeball-Provider, ihre Portkapazitäten ebenfalls zu erhöhen. Dabei sind die Peering-Strategien der Hypergiants unterschiedlich: Google, Alibaba und Netflix nehmen am öffentlichen Peering teil, Facebook und Amazon aber grundsätzlich nicht.

Das Streben nach schnellem Wachstum vernachlässigt im Gegenzug oft die regionalen Strukturen, welche den eigentlichen Standortvorteil eines IXPs ausmachen. Dies lässt sich am Beispiel des Berliner BCIX ablesen, wo zwar Akamai, Amazon, Apple, Facebook, Google und Netflix im (z.T. privaten) Peering präsent sind, das lokale Wissenschaftsnetz "Berlin Research Area Information Network (BRAIN)"[8] jedoch nicht. Die lokale Präsenz von mehr als einem Dutzend großer Hochschulen, vielen Forschungseinrichtungen, Bibliotheken, Museen und der Stiftung Preußischer Kulturbesitz, die sich in BRAIN mit einem eigenen Glasfasernetz bündeln, nimmt nicht am lokalen Peering des BCIX teil und verschenkt so die Möglichkeit des lokalen Datenaustauschs in der Größenordnung von mindestens 100 Gbit/s.

6.1.2 Internet Zugangsinfrastruktur

Der Zugang zum Internet in der Fläche, die Konnektivität von Geschäfts- und Privatkunden unabhängig von der Internet-Serverinfrastruktur also, bildet den Edge des Internets. Die Zugänge werden geprägt von der Infrastruktur der sogenannten "letzten Meilen", der Kabelerschließung von Wohn- und Geschäftshäusern also sowie der Mobilfunkabdeckung im Land.

Die Kabelversorgung in der Fläche ist wirtschaftlich doppelt komplex: Die flächige Verkabelung der Haushalte ist zum einen teuer und es ist wirtschaftlich in der Regel für konkurrierende Anbieter nicht darstellbar, Gebäude außerhalb von Innenstadtlagen mehrfach zu erschließen. Bestehende Verkabelungen aus den vergangenen Monopolzeiten sind zudem oft sehr alt, ursprünglich nicht für Breitband-Internetanschlüsse gemacht, aber ihre Erneuerung bzw. Ergänzung durch Glasfasernetze erfordert – insbesondere in ländlichen Gebieten – ebenfalls hohe Investitionen, die kaum ertragsversprechend durchzuführen sind.

Ähnliche Herausforderungen bestehen in der Mobilfunkversorgung: Hier sind zum einen die Frequenzbänder limitiert und reguliert, so dass nur wenige Anbieter überhaupt erschließungsberechtigt werden können. Zum anderen bildet die Funkabdeckung in ländlichen Gebieten eine wirtschaftliche Herausforderung, die im Alltag regelmäßig zu Versorgungslücken und damit einer Dienstverknappung führt.

Pluralität in der letzten Meile

Pluralität in der letzten Meile bildet ein zentrales Grundelement für einen leistungsfähigen Markt mit angemessener Leistungsentwicklung und Preisfindung. Zugangsmonopole behindern Investitionen und Innovationen, wirken preistreibend und gefährden die angemessene Internet-Versorgung der Realwirtschaft sowie der Privathaushalte.

Die Wirkung von Monopolstrukturen am Internet Edge ist aus den USA großflächig

[8] `https://www.brain.de/`

bekannt, wo wenigstens 50 Millionen Haushalte nur Zugriff auf einen Netzprovider haben [129]. “The large telecommunication companies, such as AT&T and Verizon, invest mainly where they face cable competition.” berichtet das ILSR in diesem aktuellen Report über die Monopolsituation im Breitband-Netzzugang der USA. Langsame Netzzugänge zu überhöhten Preisen sind die Folge — spektakulär illustriert durch den prominenten Fall des “Internet-Ingenieurs” Jared Mauch in Ann Arbor (Michigan), der als Privatmann den Bau eigener Glasfaserleitungen für sich und seine Nachbarn wirtschaftlich erfolgreich umsetzen konnte [130].

Die US-Entwicklung lässt sich klar auf mangelnde regulatorische Rahmenbedingungen in einem Markt zurückführen, der infolge der oben dargestellten konkurrenzhemmenden Situation zur Monopolisierung neigt: Nachdem der (Quasi-) Monopolriese AT&T 1984 aufgespalten wurde und die Telefonversorgung in der Fläche auf sieben unabhängige “Regional Bell Operating Companies”, die sogenannten Baby Bells, übertragen wurde, verabschiedete der Gesetzgeber keine weiteren regulatorischen Beschränkungen. In der Folge formten sich zwei neue Versorgungsriesen: Southwestern Bell, eine Baby Bell, kaufte drei weitere Baby Bells und später den verbliebenen Weitverkehrsvermittler AT&T auf, um unter dem alten Namen AT&T das frühere Monopol teilweise wiederherzustellen. Parallel dazu entstand aus weiteren Aufkäufen durch Bell Atlantic der zweite Monopolriese Verizon, welcher sich auch infolge des historisch regional geteilten Marktes mit AT&T die US-Haushalte weitgehend in der Fläche aufteilt.

Die Marktentwicklung in Deutschland

Die Marktentwicklung in Deutschland verläuft anders als in den USA. Die Bundesrepublik Deutschland ist einen regulierenden Weg bei der Ablösung des staatlichen Post-Monopols gegangen. Durch Novellierung des Telekommunikationsgesetzes (TKG) verlor die Deutsche Telekom 1996 das Netzmonopol und muss seither konkurrierenden Unternehmen Zugang zur letzten Meile gewähren (Zugangsregulierung). Gleichzeitig werden die hierfür erhebbaren Gebühren staatlich festgelegt (Entgeltregulierung). Auf der Grundlage des TKG führt die zuständige Bundesnetzagentur eine regelmäßige Marktanalyse durch, welche insbesondere das Ziel hat, marktbeherrschende Stellungen einzelner Anbieter zu verhindern (§§ 10, 11 TKG). Die Marktöffnung gilt angesichts des weiterhin regen Wettbewerbs als gelungen, was vor allem auf die regulatorisch erzwungene Diversität in der Fläche zurückgeführt werden kann.

Zusätzlich zu der Regulierung des Telefonkabelnetzes musste die Deutsche Telekom das TV-Kabelnetz abtreten, welches sie in regionale Gesellschaften aufteilte. Ähnlich zu den Entwicklungen in den USA erfolgten hierauf verschiedene Zusammenschlüsse, welche zunächst zwei überregional agierende Gesellschaften, Kabel Deutschland und Unitymedia, formten. Beide Gesellschaften wurden inzwischen von Vodafone übernommen, die hierdurch zum zweiten bundesweit agierenden Kabel-Betreiber aufgestiegen sind. Auch dieses Netz wurde inzwischen regulatorisch geöffnet. Neben bundesweiten Akteuren existieren heute noch der überregionale Kabelbetreiber Tele Columbus (Mehrheitseigner United Internet) sowie mehrere Dutzend regionaler Gesellschaften, die sich teilweise in kommunalem Besitz befinden. Beispiele sind NetCologne und Wilhelm.tel.

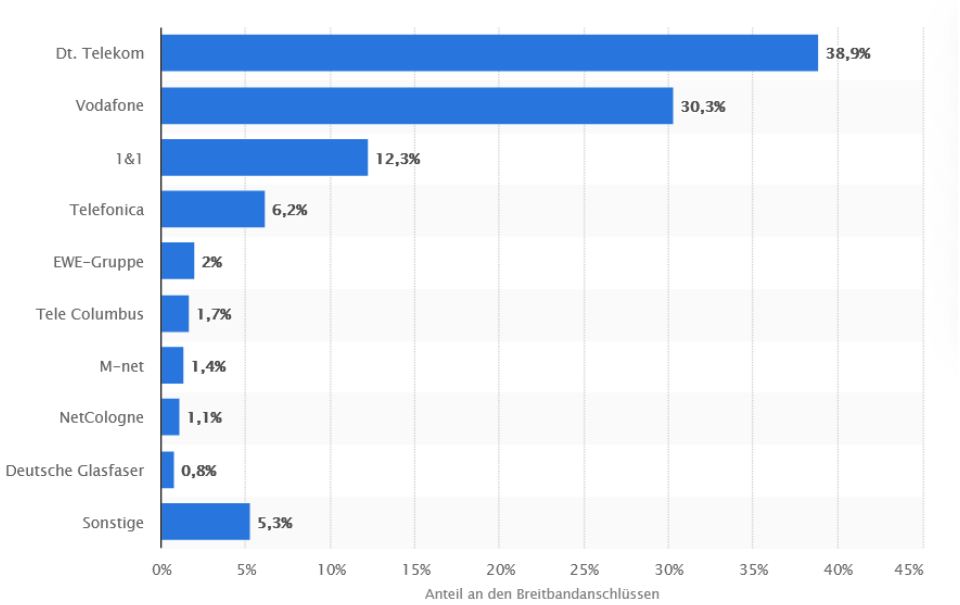


Abbildung 6.10: Anteile im Breitbandmarkt 2020 in Deutschland (Quelle: Statista)

Seit 2011 betreibt das neu gegründete Unternehmen "Deutsche Glasfaser" aktiv die Erschließung von Haushalten in Außenbezirken großer Ballungsräume mit Glasfasern, wodurch die Breitbandanbindung in der Fläche vorangetrieben wird. Die Deutsche Glasfaser plant mittelfristig 6 Millionen Glasfaseranschlüsse deutschlandweit auszubauen und ist nach der Deutschen Telekom und Vodafone der drittgrößte Glasfaseranbieter Deutschlands.

Im Jahr 2020 war der Markt für Breitband-Internetzugänge weiterhin breit aufgefächert, wie in Abbildung 6.10 ersichtlich. Die Deutsche Telekom und Vodafone halten zusammen etwa zwei Drittel des Marktes, gefolgt von einer breiten Verteilung kleinerer und regionaler Anbieter. Die Umsatzentwicklung der großen Telekommunikationsunternehmen hingegen nähern einander während der vergangenen Dekade (vgl. Abbildung 6.11). Während die Umsätze der Telekom sich leicht rückläufig zeigen, steigen Vodafone und Telefonica – letztere vor allem nach der Teilübernahme von E-Plus.

Breitbandversorgung in Deutschland

Hohe Investitionskosten in der Fläche und regulatorisch beschränkte Marktpotentiale bergen die Gefahr, dass Innovationen und Investitionen in leistungsfähige Zugangstechnologien nur sehr eingeschränkt erfolgen und die Breitbandversorgung auf lukrative Ballungsräume beschränkt bleibt.

Das Bundesministerium für Verkehr und digitale Infrastruktur erfasst den Stand der Netzversorgung in Deutschland in seinem regelmäßig aktualisierten Breitbandatlas [131]. Abbildung 6.12 zeigt die Entwicklung der letzten fünf Jahre differenziert nach Leistungsklassen. Mehr als 5% der Haushalte haben demnach heute keinen Zugang zu der mittleren Leistungsklasse von $\approx$ 50 Mbit/s bei sehr geringer Entwicklungsdynamik. Betroffen sind hiervon mehrheitlich Haushalte in ländlichen Regionen – nur eine gute Hälfte der Land-

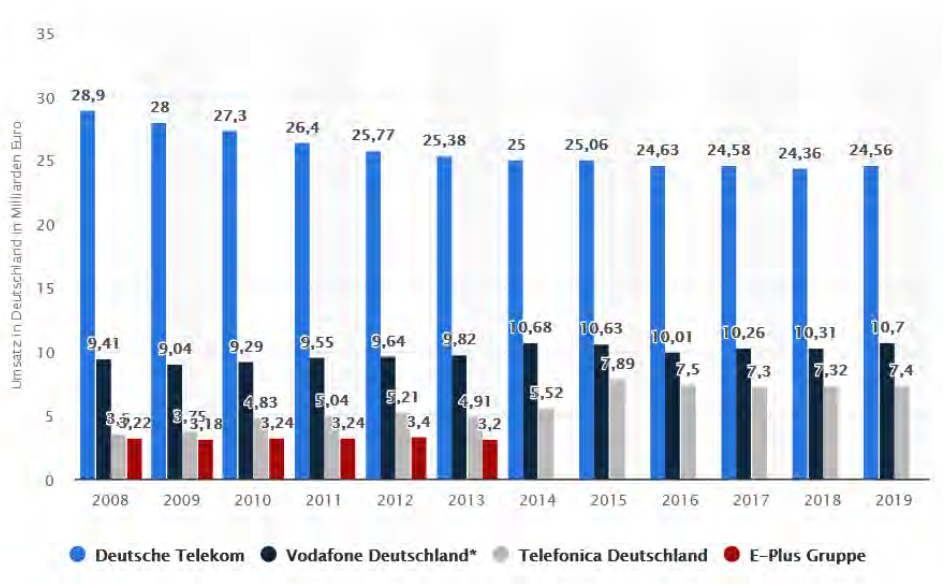


Abbildung 6.11: Umsatzentwicklung der großen Telekommunikationsunternehmen in Deutschland (Quelle: Statista)

bewohner hat Zugang zu Internet-Anschlüssen mit ≈ 100 Mbit/s oder höherer Übertragungsleistung.

Während der flächige Ausbau von Breitbandanschlüssen mittlerer Leistung eher stagniert, wird in den letzten Jahren eine hohe Dynamik bei der Verbreitung von Hochleistungsanschlüssen im Gigabit-Bereich sichtbar. Abbildung 6.13 zeigt diesen Trend der letzten fünf Jahre. Die wachsende Verbreitung stützt sich auf zwei Technologien: Eine Glasfasererschließung von Gebäuden oder Haushalten, welche mit jährlichen Wachstumsraten von etwa 20% an Relevanz gewinnen, wird u.a. von Unternehmen wie Deutsche Glasfaser auch außerhalb großer Städte vorangetrieben. Zum anderen verbreitet sich CATV mit hoher Dynamik. Hierbei handelt es sich um Hybride Fiber Coax (HFC) Netze, die den DOCSIS-Standard 3.1 verwenden. Dabei können die bestehenden TV-Kabel zur Gebäudeerschließung weiterverwendet werden, während die externen Verteilstrukturen auf Glasfaserleitungen umgerüstet werden. DOCSIS (Data Over Cable Service Interface Specification) erlaubt die Übertragung von bis zu 10 Gbit/s im Downstream auf den TV-Coaxialkabeln.

Mobile Internet-Zugänge

Die aktuellen Technologien der Mobilkommunikation im 4G– (LTE) und dem entstehenden 5G–Netz erlauben Breitband-Internetzugriff im Leistungsspektrum der Festnetze. Im Alltag werden diese Datenraten aber nur in Regionen mit hoher Basisstationsdichte erreicht werden. Die Bundesnetzagentur bietet eine interaktive Online-Karte[9] zur Visualisierung der Mobilfunkabdeckung differenziert nach Technologie und Provider an. Demnach deckt keiner der drei gegenwärtig operativen Provider (Telekom, Vodafone

[9] `https://www.breitband-monitor.de/mobilfunkmonitoring/karte`

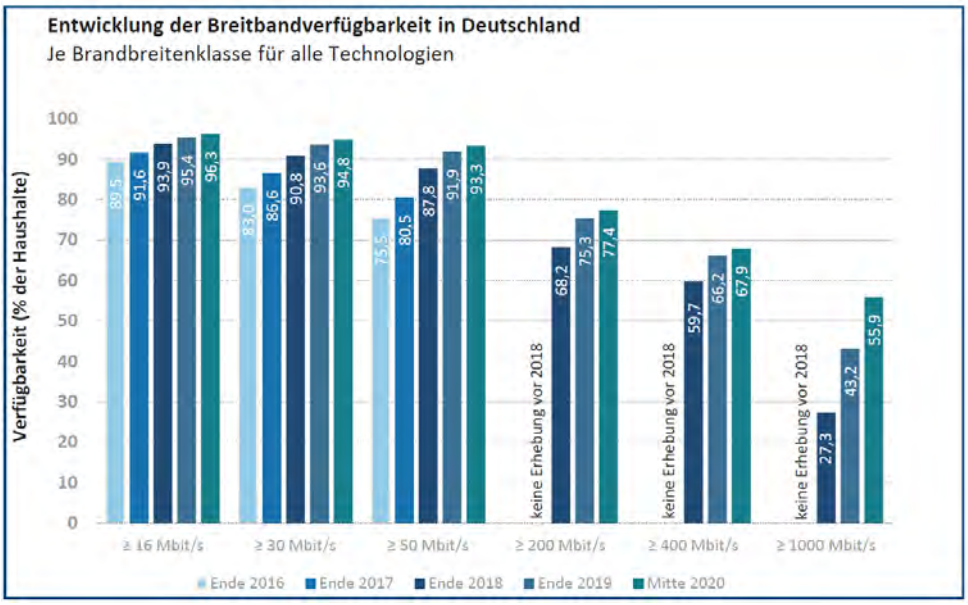


Abbildung 6.12: Entwicklung der Breitbandverfügbarkeit in Deutschland (Quelle: Breitbandatlas)

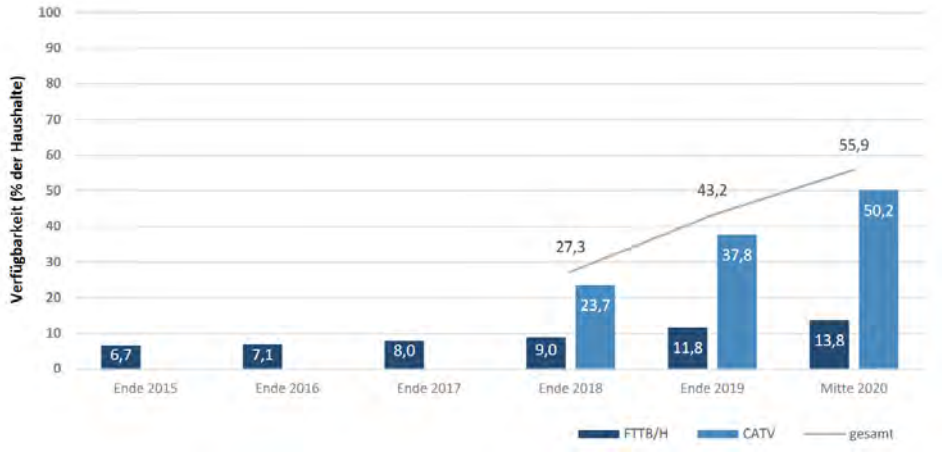


Abbildung 6.13: Entwicklung der Verfügbarkeit von Gigabit-Anschlüssen in Deutschland (Quelle: Breitbandatlas)

und Telefonica) die gesamte Landesfläche ab. Die Regulierung hatte im Rahmen des 5G-Frequenzversteigerungsverfahrens eine 98-prozentige LTE-Netzabdeckung von den Bietern gefordert, wovon alle Netzbetreiber noch weit entfernt sind.

Nationales Roaming, d.h. der bedarfsorientierte Netzwechsel zwischen inländischen Providern, kann hier zu einer merklichen Versorgungsverbesserung in der Fläche führen. In der aktuellen Vergangenheit hat es intensive Debatten über die Notwendigkeit einer Regulierung für ein solches nationales Roaming gegeben, welches insbesondere der Marktführer Deutsche Telekom stets strikt mit dem Argument ablehnte, dass erzwungenes Roaming den Netzausbau bremsen und Trittbrettfahrer unter den Anbietern begünstigen würde. Bisher hat die Bundesnetzagentur keine Regulierung in dem Markt vorgenommen, so dass nationales Roaming nur auf der Basis bilateraler Vereinbarungen zwischen Providern stattfindet. So hat die 1&1 Drillisch ein Roaming-Abkommen mit Telefonica geschlossen, um im Prozess ihres 5G Netzneubaus bereits eine Versorgung in der Fläche anbieten zu können.

Neben hohen Netzbandbreiten verspricht 5G weitere Funktionen für einen "intelligenten Edge", nämlich (1) differenzierte Netzzugangsdienste und (2) die Definition privater Kundendomänen durch "Network Slicing". Erstere Funktion ermöglicht es neuartig im Mobilfunknetz, einerseits ultra-zuverlässige oder latenzminimierte Zugänge mithilfe von zeitschlitzbasierten Funkverfahren zu nutzen und so kritische Infrastrukturdienste an das 5G-Netz anzubinden. Massive Maschinenkommunikation (mMTC) wird auf der anderen Seite ebenfalls unterstützt und erlaubt die Einbindung von ressourcenbeschränkten, Niedrigenergie-Funkknoten, welche vor allem das sich entwickelnde Internet der Dinge (IoT) millionenfach hervorbringt.

Die Funktionen der Netzwerk-Segmentierung, des "Slicing", soll die Installation und den Betrieb sogenannter vertikaler Netze als Grunddienst etablieren. Hiermit sind logisch, ggfs. auch technisch separierte Netzwerke gemeint, welche ortsübergreifend als spezialisierte Anwendungsinfrastruktur zur Verfügung stehen. Beispiele solcher vertikal isolierten Netze könnten einer Fahrzeug-zu-Infrastruktur (Car2X) Kommunikation, speziellen maschinellen Wartungs-Domänen oder auch dem verteilten Betrieb etwa in der Logistik dienen. Es bleibt abzuwarten, welche konkreten Nachfragen der Industrie und Angebote der Provider tatsächlich in den Markt kommen und zu einem Regelbetrieb finden werden.

Exklusivität als Geschäftsmodell

Exklusivität als Geschäftsmodell bleibt auch in Deutschland ein relevantes Konzept. Zwar steht die Regulierung einer regionalen Monopolisierung entgegen und Endkunden haben in aller Regel die Wahl zwischen mehreren Internet-Versorgern, was den Preiswettbewerb für Heimanschlüsse lebendig hält. Dennoch haben Endkunden in der Regel nur einen Provider, dessen Dienste sie häufig über viele Jahre ausschließlich nutzen.

Der exklusive Zugang zu einer großen Zahl von Endkunden besitzt im werbefinanzierten Anwendungsmarkt einen eigenen Wert: Werbende profitieren von dem "direkten" Zugang zu großen Kundengruppen, wobei "direkt" im globalen Internet mit "von hoher Zugangsqualität" übersetzt werden kann. Zugangsprovider verbessern die Zugangsqualität zu ihren Endkunden, indem sie mit Anwendungsprovidern leistungsstark in der Fläche

peeren. Der Werbelogik folgend, wonach nicht die Inhalte sondern die Kundenzugänge geldwert sind, fordern große Zugangsprovider Gebühren für ihre Peering-Bereitschaft mit Anwendungsprovidern. Das traditionelle "Settlement-free Peering" wandelt sich so teilweise in ein "Paid Peering" – zumindest für solche Provider, die eine sehr große Kundenbasis exklusiv versorgen. Die zugrundeliegenden vertraglichen Vereinbarungen sind in der Regel Geschäftsgeheimnisse zwischen den Partnern und nicht öffentlich.

6.1.3 Internet Anwendungsprovider

Das Internet ist anwendungsoffen. Kein Internet Nutzer benötigt eine Erlaubnis, um neue Anwendungen im Internet zu verbreiten oder zu betreiben. Diese Offenheit hat in den vergangenen vierzig Jahren ungezählte Innovationen ermöglicht und dabei ein freies, weitgehend unreguliertes Spiel der Marktkräfte entfacht. Mit der Alterung des Marktes konsolidieren diese zunehmend und führen zu monopolartigen Strukturen.

Gemäß dem Sandvine Global Internet Report[10] kamen 2019 43% des globalen Datenverkehrs im Internet durch Google, Netflix, Facebook, Microsoft, Apple oder Amazon zustande. GroupM schätzte 2017, dass Facebook und Google 84% des globalen digitalen Anzeigenmarktes (außerhalb Chinas) besetzen. Facebook dominiert den Markt der sozialen Netzwerke mit vier der sechs populärsten Plattformen. Google hält 90% des globalen Suchmarktes, hat 60% Browser-Marktanteil, ist Marktführer für mobile Betriebssysteme (Android) sowie nutzergenerierten Video-Plattformen (YouTube) und betreibt diverse weitere Internet-Dienste mit mehr als 1.5 Milliarden Nutzern.

> [...] Alphabet not only operates an online advertising platform, but also a search engine, a mail platform, a document store, a cloud service, a public DNS resolver service, a mobile device platform, a browser, and mapping services to name just a few. It appears that in this case, it is one enterprise with engagement in many discrete activities. The issue with consolidation is whether these activities remain discrete activities or whether they are being consolidated into a single service.
>
> — Geoff Huston, RIPE NCC, December 2018

Die Europäische Union hat Ende 2020 mit dem Digital Markets Act (DMA)[11] einen Gesetzesvorschlag eingebracht, welcher sogenannte digitale Gatekeeper, also zugriffsteuernde Plattformen wie Google und Facebook, in ihren Möglichkeiten einschränkt, die eigenen Angebote durch Selbstreferenzen zu bevorzugen oder die in anderen Geschäftssparten, z.B. WhatsApp, gesammelte Personendaten zur Fokussierung des Plattform-Marketings weiterzuverwenden. Dieser Vorschlag befindet sich gegenwärtig im Gesetzgebungsverfahren des europäischen Parlaments.

[10] https://www.sandvine.com/blog/netflix-vs.-google-vs.-amazon-vs.-facebook-vs.-microsoft-vs.-apple-traffic-share-of-internet-brands-global-internet-phenomena-spotlight

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0842

Vormachtstellung durch Großsysteme

In seinem wegweisenden Artikel "A Theory of Interdependent Demand for a Telecommunications Service" [132] identifizierte Rohlfs 1974 in den Bell Labs die grundlegende Wirkweise, dass die Nützlichkeit und damit der Marktwert eines (Video-) Kommunikationsdienstes mit der Zahl seiner Nutzer steigt, ein Kommunikationssystem per se also mit seiner Größe wertvoller wird. Das Internet unterstützt diese Entwicklung zu Großsystemen zunächst technologisch durch die globale Teilnehmererreichbarkeit und seine sehr hohe Skalierbarkeit. Anwendungen nutzen diese Möglichkeiten seit Beginn des Internets (vgl. E-Mail), haben sich aber weit über die ursprünglich angedachten Kommunikationssysteme hinaus entwickelt: Suchmaschinen, One-stop-Shops und Infotainment-Portale haben erfolgreich am Markt bewiesen, dass ihre Ausprägung als Großsysteme für die Nutzer vorteilhaft sind: Anwender ziehen es vor, auf Informationen und Dienste durch wenige, integrierte User-Interfaces zuzugreifen – mehr als die Hälfte aller US-Bürger versucht heute ein Online-Geschäft zuerst mit Amazon abzuschließen.

Die Designer des Internets haben frühzeitig erkannt, dass offene Standards einen kooperativer Weg zu Wachstum ermöglichen, der für ein plurales Netz essenziell ist. Kommunikationsdienste (wie E-Mail oder VoIP) oder Informationssysteme (wie das Web) können offen und pluralistisch wachsen, weil Standards ihre Interoperabilität absichern. Heute dominante Anwendungs-Provider arbeiten ohne solche Standards. Teilweise existierten diese zur Zeit der Dienstentwicklung nicht (Suchmaschinen), teilweise wurden sie auch gezielt missachtet (WhatsApp, Skype).

Die Bedeutung von zentralistischen Großsystemen wächst heute auch dort, wo offene Standards kooperativ verteilte Lösungen vorsehen. Technisch wird dies dadurch erleichtert, dass einige Anbieter über hochskalierbare, auf der Systemebene verteilte Infrastrukturen verfügen, die im Netz mit einer logischen Schnittstelle auftreten. Aktuelle Entwicklungen betreffen z.B. das Domain Name System (DNS), welches ursprünglich lokal verteilte rekursive Resolver bei jedem ISP nah den Endnutzern vorsah. Eine Kette von Betriebsbeeinträchtigungen — unter ihnen gewollte Funktionsveränderungen und Zensur, aber auch ungewollte Funktionsdefizite, Mißbrauch und Probleme in der Betriebsstabilität — haben den Markt geöffnet für "neue", professionelle und neutrale Anbieter: Google betrat den Markt Ende 2009 mit der eingängigen Entität "8.8.8.8". Cloudflare (1.1.1.1), Verisign (64.6.64.6) und Quad9 folgten. Heute hat Google (8.8.8.8) einen stabilen Marktanteil von etwa 15% an den globalen Namensauflösungen.[12]

Seit über 20 Jahren wird ein proprietär verändertes DNS dazu genutzt, verteilte Content Delivery Networks (CDNs) anstelle eines (oder mehrerer Anycast-) Datenserver für den Content-Zugriff anzusprechen. CDNs liefern heute die Dateninhalte von mehr als 90% der populären Websites aus [119], wobei sich der Markt in Segmente untergliedert. Große Content-Provider wie Google, Amazon oder Netflix betreiben ihre eigenen CDNs. Einige Anwendungsdienste wie z.B. Facebook arbeiten mit hybriden Lösungen aus eigenen und Fremdsystemen. Der breite Markt hingegen greift auf professionelle CDN-Provider zurück, deren Marktanteile nach Kundenzahlen in Abbildung 6.14 gezeigt werden. Dieser Markt ist stark konsolidiert, wobei die Ertragszahlen das Verhältnis der Marktführer Cloudflare, Amazon und Akamai umdrehen. Der traditionelle Marktführer Akamai bedient nach

[12] `https://stats.labs.apnic.net/rvrs`

Abbildung 6.14: Kundenverteilung 2020 am CDN-Markt (Quelle: intricately.com)

eigenen Angaben etwa die Hälfte der größten amerikanischen Kunden (Fortune 1,000), erzielt etwa zwei Drittel der Markterträge und berichtet regelmäßig über Verkehrsrekorde im Ausrollen der Fortnite-Updates.[13]

Cloud Dienste – genauer Cloud Infrastruktur Plattform Services (CIPS) – etablieren sich ähnlich wie CDNs zunehmend am Markt für Internet-Infrastruktur. Clouds erleben gegenwärtig noch sehr hohe jährliche Wachstumsraten von fast 40%. Auch hier gibt es eine starke Marktkonzentration mit dem Marktführer Amazon (45%), Microsoft (18%), Alibaba, Google und Tencent. Mit 80% bzw. 102% wachsen Google und Tencent gegenwärtig am stärksten und wesentlich kräftiger als der Marktdurchschnitt.[14] Da ein Bestehen an diesem Markt mit hohen Investitionen in Infrastruktur und Kompetenzen verbunden ist, werden weitere Konsolidierungen erwartet.

Vormachtstellung durch Endsysteme

Anwender interagieren im Netz mithilfe von Endgeräten. Hersteller von Betriebssystemen für solche Endgeräte halten deshalb eine Schlüsselposition bei der Ausgestaltung dieser Interaktion, ggfs. auch bei der Prägung des Nutzerverhaltens. Microsoft hat dieses Potential in den späten 90er Jahren erkannt und in dem damaligen “Browser-Krieg” mit Netscape (und Nachfolgern) so lange ausgespielt, bis staatliche Wettbewerbsbeschränkungen in Kraft traten.

[13] `https://blog.intricately.com/2020-state-of-the-cdn-industry-trends-market-share-customer-size`

[14] `https://www.gartner.com/en/newsroom/press-releases/2020-08-10-gartner-says-worldwide-iaas-public-cloud-services-market-grew-37-point-3-percent-in-2019`

Zehn Jahre später hat Apple einen neuen, subtileren Weg initiiert, um das Anwendungs-Ökosystem auf seinen Mobilgeräten zu dominieren: den Apple App Store. Streng von Apple kontrolliert, ist der App Store die einzige (legale) Möglichkeit, Anwendungen auf iOS zu installieren und gleichzeitig eine Vermarktungsplattform für Anwendungsentwickler. Diese Dualität, Kontrollinstanz und kommerzieller Marktplatz, hat sehr schnell eine intensive Akzeptanz und Verbreitung erlebt. Entwickler in großer Zahl produzieren vorwiegend netzbasierte Anwendungen, die einerseits die iOS-Plattform attraktiver machen (und an sie gebunden bleiben), andererseits sich der Kanalisierung und Überwachung durch Apple nicht entziehen können.

Google ist dem Vorbild von Apple hastig für Android gefolgt. Beide Hersteller stellen hochstehende, von der zugrundeliegenden Technologie abstrahierende Application Programming Interfaces (APIs) für die Anwendungsentwicklung bereit, welche sowohl die Nutzerschnittstellen als auch die Kommunikationsschnittstellen in der Kontrolle des Betriebssystems behalten. Solche APIs können z.B. die Einführung von modifizierten oder nicht-standardisierten Internet-Protokollen (Google QUIC) verbergen, aber auch Nutzerdaten oder -verhalten in vorgegebener Weise leiten. Die Bedeutung dieser Schnittstellen wird umfassender, je hochstehender und abstrahierter die angesprochenen Funktionen werden. Beispiele für hochstehende, abstrahierende Nutzerschnittstellen entstehen in neuer Dimension für sprachkontrollierte Systeme.

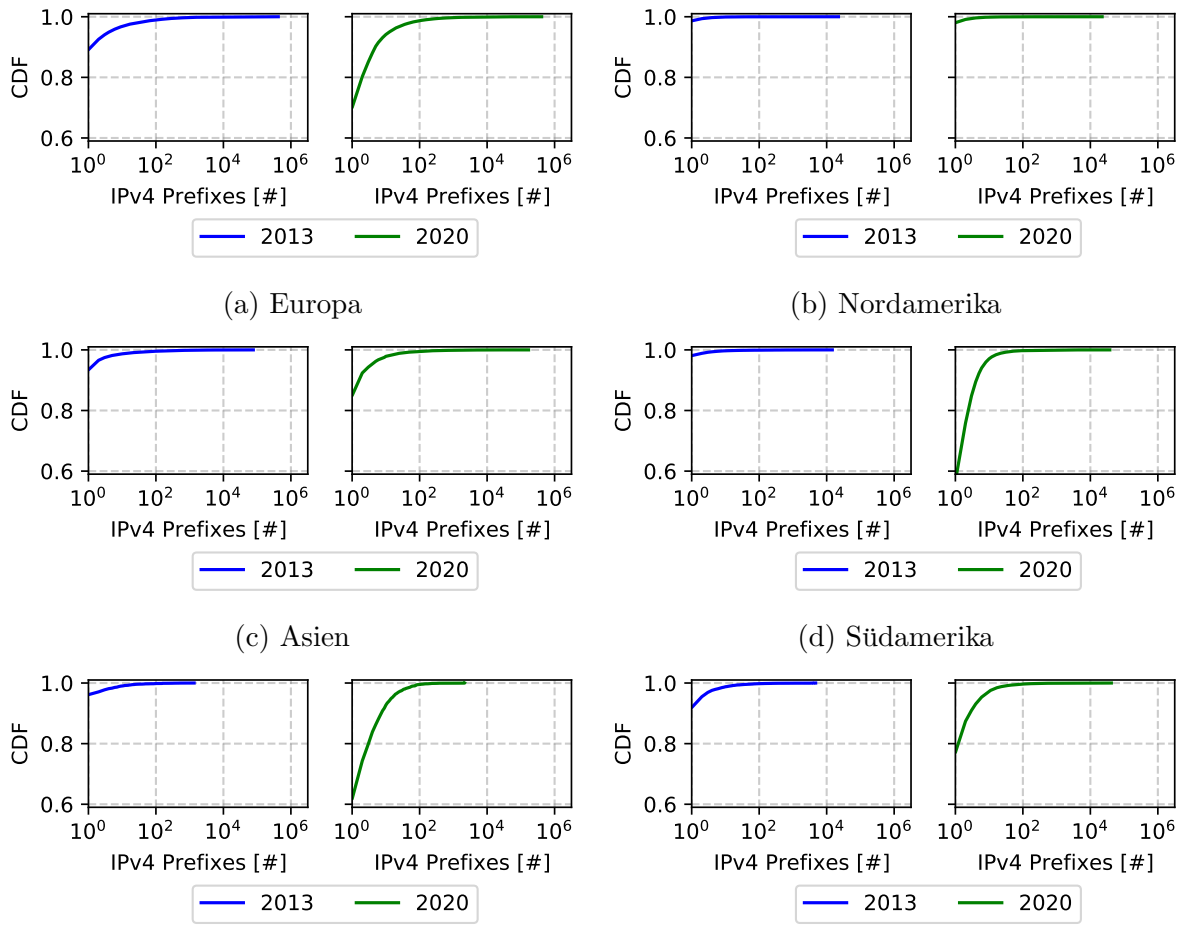
> The growing use of APIs puts more of the Internet's innovation, functionality, and interoperability into the hands of the dominant Internet platforms, whose interests may not always align with those of the broader technical community and other players.
>
> — Internet Society [119]

6.1.4 Internet-Ressourcen: IPv4-Adressblöcke

Internet-Ressourcen sind für den Betrieb und die Entwicklung des Netzes zentrale Voraussetzung und so ist ihre Ungleichverteilung ein wichtiger Indikator für Konsolidierung und Monopolisierung. Gegenwärtig sind IPv4-Adressen die am meisten beschränkte Ressource, weshalb wir analysieren, wie sich ihre Verteilung über die Akteure in den letzten Jahren entwickelt hat.

Wir identifizieren hierfür zunächst die Akteure aus den WHOIS-Datenbanken und werten dann die zugehörigen IPv4-Präfixobjekte aus. Präfixe können unterschiedlich lang sein, weshalb hierbei nicht die absoluten Anzahlen von Adressen gemessen werden. Vielmehr liegt diesem Vorgehen das Verständnis zugrunde, dass Internet-Akteure Ressourcen in ihrem jeweiligen Gebrauchskontext beantragen – ein kleiner ISP erhält geringeren Adressraum als z.B. die Deutsche Telekom.

Die Ergebnisse dieser Analyse sind in Abbildung 6.15 zusammengefasst: Pro Kontinent werden Präfix-Verteilungen aus 2013 und 2020 nebeneinandergestellt. Mit Ausnahme von Nordamerika sehen wir für alle Kontinente eine starke Tendenz hin zu wachsender Ungleichverteilung der Ressourcen: Insbesondere Südamerika, Afrika und Europa zeigen für das Jahr 2020 signifikante Anteile von Akteuren, die über eine größere Anzahl an Präfixen



(a) Europa

(b) Nordamerika

(c) Asien

(d) Südamerika

(e) Afrika

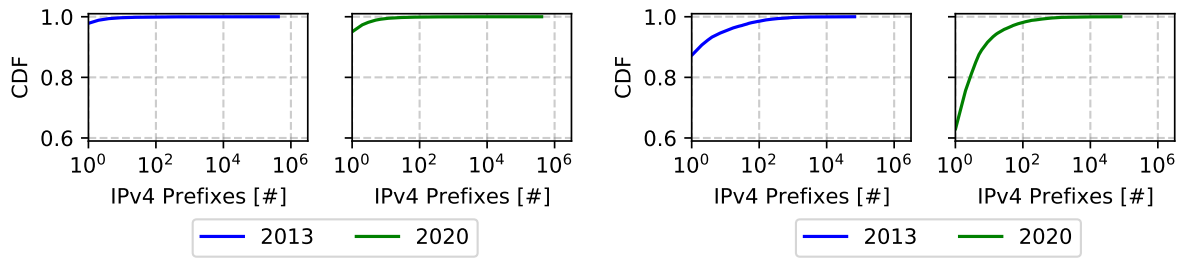
(f) Ozeanien

Abbildung 6.15: Kontinentale Entwicklung der Verteilung von IPv4 Ressourcen zwischen Internet-Akteuren

verfügen – teilweise mehr als 100.

Abbildung 6.16 vergleicht diese Entwicklung für Deutschland mit dem weltweiten Trend. Klar ersichtlich ist ein deutlich stärkerer Trend zu einer Konzentration von IPv4 Präfixen. Insbesondere ist der Anteil an Organisationen, die nur ein IPv4 Präfix besitzen, in Deutschland um 10% geringer als in Gesamteuropa.

Zusammen legen diese Ergebnisse zwei Schlussfolgerungen nahe: Zum einen mag die Anzahl der kleinen, "zersplitterten" IP-Blöcke außerhalb der USA stark angewachsen sein, weil zunehmend Präfixe mit 24 Bit Länge vergeben wurden. Andererseits legen die Verteilungen nahe, dass Provider angesichts der zunehmenden Adressknappheit unzusammenhängende Präfixe zusammengesammelt, also zu unterschiedlichen Zeiten und auf unterschiedlichen Wegen – ggfs. auch über Zukäufe – Adressblöcke akkumuliert haben.



(a) Weltweit (b) Deutschland

Abbildung 6.16: Entwicklung der Verteilung von IPv4 Ressourcen: Deutschland im weltweiten Vergleich

6.1.5 Wechselwirkungen von Internet– und Realwirtschaft

Wie die meisten Staaten dieser Welt, verfügte Deutschland mit der Deutschen Post über eine staatliche Monopolgesellschaft, die ein landesweites Telefonnetz betrieb, dessen Erhalt und Entwicklung als staatliche Infrastrukturaufgabe verstanden wurde. Mit dem Fall der Staatsmonopole und der nachfolgenden Deregulierung und Privatisierung entließen viele Staaten die Netzinfrastruktur in den privaten Markt und die Infrastrukturinvestitionen in das Wechselspiel der (teilregulierten) Marktkräfte.

Internet-Infrastrukturentwicklung als gesamtwirtschaftliches Handlungsfeld

Der Fall der Telekommunikationsmonopole in Europa folgte zeitnah auf die sich ab 1995 entwickelnde “Internet-Revolution”, die ein merkliches Stimulanz für neue Akteure und Investoren in dem Telco-Infrastrukturmarkt wurde. Dieser Markt versprach großes Wachstum. In Deutschland traten neben der Telekom neue, auch ausländische Kommunikationsfirmen, dazu Trassenbesitzer wie kommunale oder private Versorgungsfirmen sowie die Bahn in den Markt ein. Versorger kamen in Städten wie Köln mit NetCologne, in Hamburg mit HanseNet oder in Berlin mit Berlikom zu dem regionalen Infrastrukturwettbewerb hinzu und errichteten lokale Zugangsverkabelungen.

Ein weiteres Stimulanz für Investitionen in die Infrastruktur der Netze entwickelte sich mit der wenig später aufkommenden 3GPP/UMTS Mobilfunktechnologie und ihren Potentialen für ein mobiles Internet. In Deutschland folgte der Lizenzversteigerung im Jahr 2000 eine Investitionswelle in die neue Mobilfunk-Infrastruktur, welche Masten, Kabel und Basisstationen in deutlich erhöhter Dichte und damit in bisher unbekannter Häufung erforderte.

Abbildung 6.17 zeigt die Entwicklung der Investitionsvolumina der Telekommunikationsunternehmen und einen Spitzenwert für die Investitionen in den frühen 2000er Jahren, in welchen die moderne Mobilfunk-Infrastrukturen entstanden sind. Investitionen umfassen sowohl Komponenten und Anlagen, als auch den Bau von Trassen, Masten und Rechenzentren einschließlich hierfür notwendiger Planungs-, Ingenieurs- und System-Dienstleistungen.

Nach dem mobilnetzgetriebenen Höhepunkt sinken die Investitionen von Telekom und

Abbildung 6.17: Investitionsverlauf der Deutschen Telekom und ihrer Mitbewerber (Quelle: Statista)

ihren Mitbewerbern zwar zunächst deutlich ab, steigern sich aber dann wieder kontinuierlich und erreichen inzwischen fast ein jährliches Investitionsvolumen von 10 Milliarden Euro. Diese Investitionen umfassen den Erhalt und Ausbau der kabelgebundenen und der Mobilfunknetze und sind in der Höhe vergleichbar mit den gegenwärtigen Investitionen in Anlagen zu erneuerbaren Energien (10,5 Mrd.€ in 2019 laut BMWI[15]). Investitionen in den flächigen Breitbandausbau werden von der Bundesregierung unter Federführung des BMVI dort gefördert, wo der Abstand zum Ziel eines flächigen Gigabit-Netzes noch signifikant ist und die Versorgung noch unter der Schwelle von 30 Mbit/s liegt.

Das Gewicht der Internet-Wirtschaft

Mit der "Internet-Revolution" und der sich zeitgleich entwickelnden globalen Hochleistungsnetzinfrastruktur entwickelten sich weltweit Wirtschaftszweige, die maßgeblich auf den verfügbaren Internet-Technologien beruhen. Eine interessante Fragestellung liegt in der Messung und Quantifizierung dieses Marktes und seines Anteils am Bruttosozialprodukt (BSP) sowie weiterer Auswirkungen auf die Realwirtschaft. Die OECD hat sich in einer umfangreichen Studie mit den Möglichkeiten und Methoden für eine solche Erfassung befasst [133]. Sie identifiziert hier die drei Ansätze (*i*) Mehrwert, der durch Internet-basierende Angebote entsteht, (*ii*) Erhöhung des BSP durch Internet-basierte Handlungen und (*iii*) Konsumentenvorteile und Wohlstand, welche sich auf Internet-Dienste zurückführen lassen.

Die OECD entwickelt in ihrer Analyse drei wesentliche, aufeinander aufbauende Beiträge zum Mehrwert der Internet-Wirtschaft (vg. Abbildung 6.18): die Internet-Basisinfrastruktur, welche es ohne das Internet nicht zu geben bräuchte, die reinen Internet-Dienste, welche erst durch das Internet hervorgebracht wurden, und die Leistungsverbesserungen und Synergien, die durch Internet-Technologien in tradierten Geschäftsbereichen möglich werden.

[15] `https://www.bmwi.de/Redaktion/DE/Publikationen/Energie/erneuerbare-energien-in-zahlen-2019.pdf`

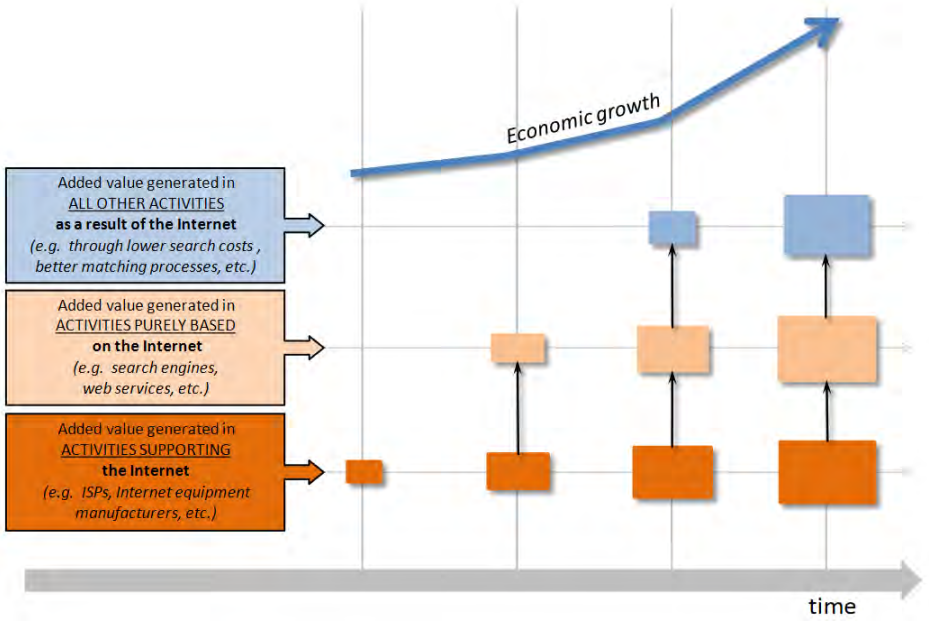


Abbildung 6.18: Aufeinander aufbauende dynamische Beiträge des Internets zum Bruttosozialprodukt (Quelle: OECD)

Bosten Consulting definiert vier Kenngrößen, welche die direkten ökonomischen Wirkungen des Internets auf ein Land ausmachen (zitiert nach [133]):

1. der direkte Anteil am BSP, der auf die Errichtung und den Betrieb der Internet-Infrastruktur entfällt – einschließlich aller Investitionen, Nutzungsgebühren, staatlichen Förderungen und des Exports von Netzdienstleistungen;

2. der im BSP nicht erfasste Anteil von Einflüssen auf Konsumenten und Geschäftspartner durch E-Commerce, Online-Werbung und andere konsumbeeinflussende Angebote;

3. Produktivitätssteigerungen durch vernetzte Abläufe einschließlich der Online-Abläufe in der Beschaffung und der Werbung;

4. der breite soziale Einfluss der Online-Medien einschließlich nutzergenerierter Inhalte, sozialer Netzwerke, Betrug und Angriffe bis zur Produktpiraterie.

Eine entsprechende multi-nationale Evaluierung der nationalen Internet-Wirtschaften von Boston Consulting und der OECD ist für 2016 in Abbildung 6.19 dargestellt. Neben den quantifizierten BSP-Anteilen haben die Autoren auch eine qualitative Klassifikation der Länder vorgenommen: Länder mit vollständig ausgebildeter, entwickelter Internet-Wirtschaft (Natives) bilden die Minderheit, wohingegen eine breitere Gruppe, zu der auch Deutschland gehört, zu den “Mitspielern” (Players) gerechnet wird. Neben Nachzüglern (Laggards) werden viele, insbesondere Schwellenländer als sich rasch entwickelnde Anwärter (Aspirants) auf eine vollwertige, reife Rolle in der Internet-Wirtschaft identifiziert – eine Entwicklung, die sich in den letzten Jahren für China und Indien, aber auch für Brasilien bewahrheitet hat.

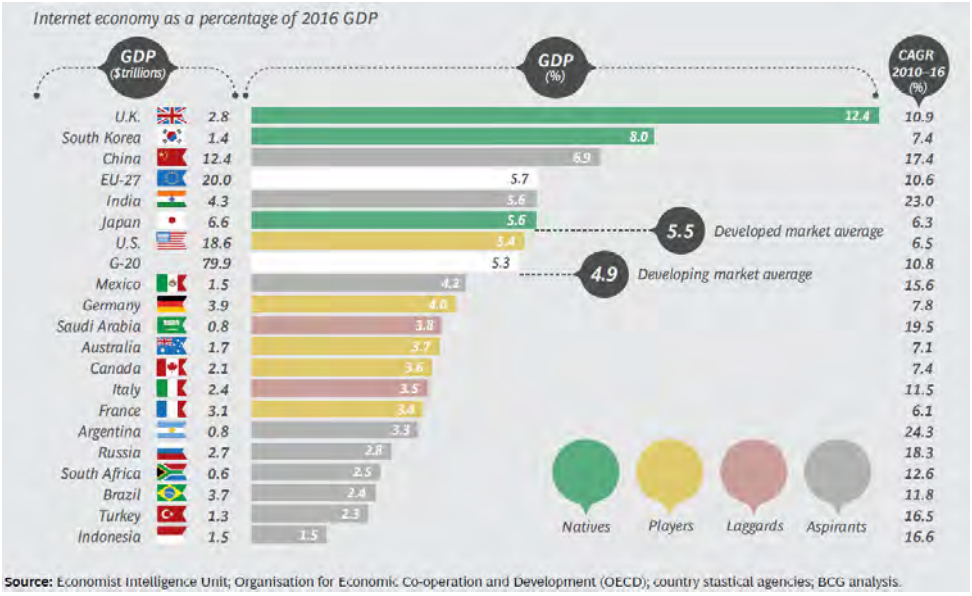


Abbildung 6.19: Anteile der Internet-Wirtschaft an internationalen Bruttosozialprodukten in 2016 (Quelle: Boston Consulting)

Der Anteil der Internet-Wirtschaft am BSP in Deutschland liegt mit 4,0% deutlich unter dem Durchschnitt der entwickelten Digitalmärkte (5,5%). Dieser Anteil ist weitgehend stabil geblieben – laut ECO-Verband wuchs er nur leicht auf 4.2% in 2020. Auch bei den kumulierten jährlichen Wachstumsraten seit 2010 (CAGR) bleibt Deutschland mit 7,8% deutlich hinter dem EU-Durchschnitt zurück. Allerdings nahm Großbritannien in der EU eine herausgehobene Führungsrolle ein, so dass die gemittelten Leistungsindikatoren für die digitale Wirtschaft seit dem britischen Ausscheiden aus der EU deutlich gesunken sein dürften.

Ein Grund für diese zögerliche Entwicklung in Deutschland kann in der oft unzureichenden Breitbandversorgung in ländlichen Regionen liegen, welche in Deutschland stärker als in anderen Ländern besiedelt sind.

Verfügbarkeit und Kosten der Internet-Infrastruktur

Die Realwirtschaft nutzt Internet-Dienste zunehmend im Rahmen ihrer alltäglichen Geschäftsprozesse, und die Versorgung mit leistungsfähigen Internet-Zugängen bildet eine grundlegende, geschäftskritische Infrastruktur. Der Bedarf reicht über die Bürovernetzung von KMUs und Freiberuflern bis zu Hochleistungsrechenzentren, wobei die Mehrzahl der Unternehmen heute Breitbandanforderungen für digitale Geschäftsintelligenz, Logistikprozesse und insbesondere auch die Technologieentwicklung braucht. Je nach Art und Größe des Unternehmens schwanken die Anforderungen, wobei ein Kleinunternehmen im IT-nahen Bereich Anschlußmöglichkeiten von weniger als 100 Mbit/s als einschränkend wahrnehmen dürfte, und ein Co-Working-Space ab 50 Arbeitsplätzen mindestens über einen Gigabit-Anschluß verfügen sollte.

Diese Anschlußkapazitäten sind in Deutschland gegenwärtig leider in Gewerbegebieten nicht üblich, wie Abbildung 6.20 zeigt. Gut drei Viertel der Gewerbestandorte können

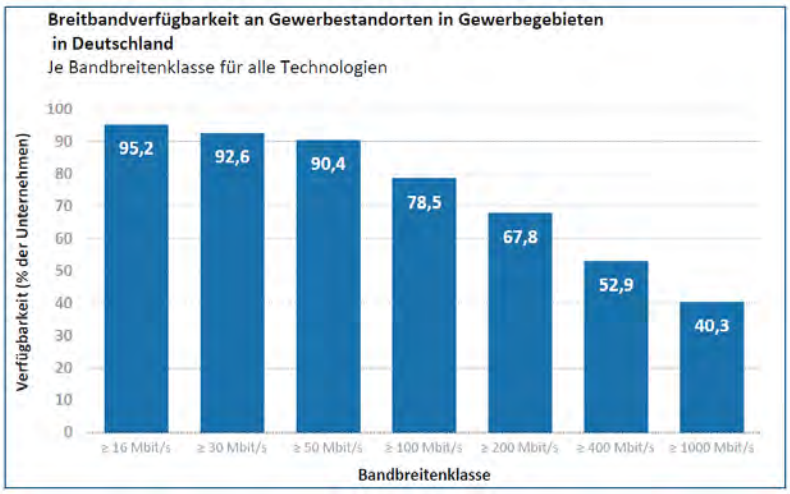


Abbildung 6.20: Verfügbarkeit von Breitband-Anschlüssen in deutschen Gewerbegebieten (Quelle: Breitbandatlas)

mit 100 Mbit/s versorgt werden, aber nur 40% verfügen über Gigabit-Technologien. Diese Versorgungsengpässe beschränken die Ansiedlung und hemmen ggfs. die Entwicklung von Unternehmen. Soweit verfügbar, unterscheiden sich die Anschlusskosten für Geschäftskunden nicht signifikant von Privatanschlüssen und bleiben mehrheitlich moderat.

Differenziert man die Breitbandversorgung nach der Prägung in der Fläche, ergibt sich ein deutlicher hervortretendes Bild: Nur etwa die Hälfte der ländlichen Gewerbestandorte hat Zugriff auf 100 Mbit/s Anschlüsse und fast fünf Sechstel können keine Gigabit-Versorgung erhalten.

Die **wirtschaftliche Bedeutung der Abdeckung in der Fläche** ist dabei komplex zu bewerten: Einerseits ist das Land geprägt von außerstädtischen Strukturen, die sich aber in Ballungsregionen organisieren. So gilt für Deutschland in etwa ein "Drittelungsgesetz" bei einem Pareto-Clustering der Bevölkerung: 80% der Deutschen leben in einem Drittel der Landesfläche, weitere 15% leben in einem zweiten Drittel und die verbleibenden 5% bevölkern das restliche Drittel [134].

Andererseits bieten ländliche Räume mit alternder, abnehmender Bevölkerung Raum und preiswerte Möglichkeiten für die Gründung und Ansiedelung von neuen Gewerben. Dabei spielen insbesondere netzbasierte Hochtechnologie-Branchen ein große Rolle, weil sie weitgehend standortunabhängig sind. Komplementär gibt es eine wachsende Zahl von naturliebendem, gut ausgebildeten Nachwuchs, der gerne abseits der Metropolen selbständig tätig wäre und dies wirtschaftlich auch leicht realisieren könnte, wenn denn die Netzversorgung in hinreichender Qualität verfügbar wäre. Hier bestehende und aufgrund defizitärer Breitbandversorgung ungenutzter Potentiale sind naturgemäß unbekannt.

Die Kosten für regulär verfügbare Breitbandanschlüsse sind in Deutschland weitgehend ortsneutral, da große Anbieter wie die Telekom landesweite Tarife ausweisen. Preise können im Bereich der Hochleistungsanschlüsse stärker variieren. Ausbau und Erschließung von Regionen mit neuen Glasfaserleitungen wird häufig von den zu erwartenden Anschlussmargen abhängig gemacht. So führt die Deutsche Glasfaser in Beispielfällen die

Breitbandverfügbarkeit über alle Technologien (in % der Gewerbestandorte)							
Prägung	≥ 16 Mbit/s	≥ 30 Mbit/s	≥ 50 Mbit/s	≥ 100 Mbit/s	≥ 200 Mbit/s	≥ 400 Mbit/s	≥ 1.000 Mbit/s
Städtisch	97,4	95,2	94,0	84,8	76,8	63,0	50,4
Halbstädtisch	93,1	90,0	86,8	71,2	57,1	41,1	27,4
Ländlich	85,2	80,8	75,3	56,0	37,6	22,7	17,8

Abbildung 6.21: Verteilung der Breitband-Verfügbarkeit für Gewerbe in der Fläche (Quelle: Breitbandatlas)

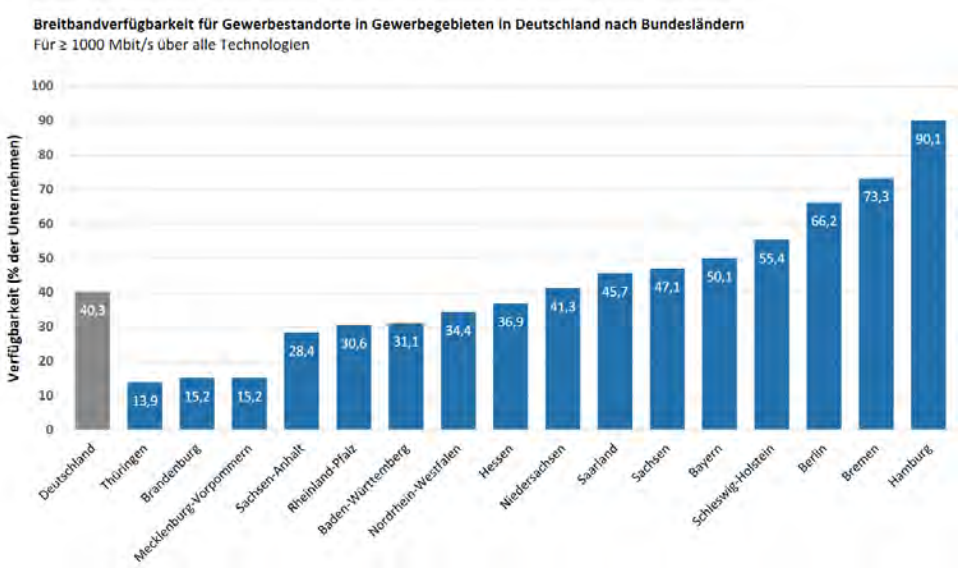


Abbildung 6.22: Verteilung der Gigabit-Verfügbarkeit für Gewerbe nach Bundesländern (Quelle: Breitbandatlas)

Erschließung von Ortskernen und Straßenzügen nur dann durch, wenn wenigstens die Hälfte der Haushalte auch einen Anschluss bestellen — ein Rate, die in vielen ländlichen Regionen mit überalterten Bevölkerungsstrukturen oft nur schwer zu erreichen ist. Hier wirkt das DigiNetz Gesetz (2016) entgegen, indem es Synergiepotentiale beim Tiefbau zu heben versucht und Glasfasererschließung bei Neubauten erzwingt.[16]

Infolge der hohen Tiefbaukosten bei der Erschließung ländlicher Regionen entstehen fast zwangsläufig (regionale) Monopole, die allerdings auch von den Gebietskörperschaften selbst gestellt werden können. Solche Infrastrukturmonopole sind in Deutschland nicht wettbewerbskritisch, da der Wettbewerb auf dem Netz durch die Bundesnetzagentur reguliert wird. Allerdings ergeben sich Betriebs- und Versorgungsabhängigkeiten, welche besser auf der kommunalen Ebene als mit einem überregional gewinnstrebenden Netzbetreiber verhandelt werden können.

Die Verfügbarkeit von Hochleistungs-Netzanbindungen unterscheidet sich nicht nur stark zwischen Stadt und Land, sondern auch zwischen den Bundesländern, die selbst eine wesentliche Rolle in der Infrastrukturentwicklung einnehmen. Der Stadtstaat Hamburg weist eine um 40% bessere Gigabit-Versorgung auf als die Stadt Berlin, welche wieder-

[16] In der Praxis scheint die Umsetzung des Gesetzes an der fehlenden Datentransparenz zur Netzinfrastruktur zu scheitern, wie der Europäische Rechnungshof in seinem Sonderbericht, Nr. 12/2018 bemängelt.

um ähnlich gut versorgt ist wie der Flächenstaat Schleswig-Holstein. Schleswig-Holstein verfolgt bereits seit 2013 das ehrgeizige Infrastrukturziel, bis 2025 flächendeckend Glasfaseranschlüsse in die Gebäude zu verlegen [135], was offenkundig Wirkung zeigt. Weitgehend abgeschlagen wirken Thüringen, Brandenburg und Mecklenburg-Vorpommern, deren Hochleistungsvernetzung sich auf sehr wenige, urbane Flecken beschränkt.

Diese sehr starken Gefälle zwischen Stadt und Land sowie zwischen Regionen (Nordwest versus Nordost) können dauerhafte Strukturnachteile bewirken. Da netzbezogene Unternehmen und ihre Berufe mehrheitlich dem höher qualifizierten Segment zuzurechnen sind, können diese Infrastrukturdefizite zu einer Abwanderung der hochqualifizierten Bevölkerung führen und damit zu langfristiger wirtschaftlicher Nachrangigkeit führen. Solche Strukturentwicklungen wirken auch auf die alte Ökonomie zurück, da neue Innovationskerne auch in Gebäude, Ausstattungen, Anlagen und Freizeitangebote investieren. Fehlen diese Investoren, reduzieren sich Nachfragen, fallen Gebäudepreise und die Lebensqualität sinkt oft schon dadurch, dass signifikante Teile der jungen Generationen fortziehen.

6.2 Gesellschaftliche Auswirkungen und Entwicklungen

6.2.1 Netzdienste als Teil gesellschaftlicher Grundversorgung

Wir leben im vielbeschworenen digitalen Zeitalter, für welches der Breitbandzugang zum Internet eine allgegenwärtige Voraussetzung ist: Infotainment – von online Nachrichtenseiten bis zu Netflix –, das Teilen unterschiedlichster Dokumente, die Bereitstellung und Aktualisierung von Software und Diensten, schließlich auch das einfache Telefonieren sind ohne leistungsfähige Zugänge zur Internet-Infrastruktur kaum mehr durchführbar. Seit der Zeit der Covid-19 Pandemie sind Video-Konferenzen als Alltagswerkzeug der Kollaboration, des heimgebundenen Lernens in Schulen und Hochschulen sowie für die soziale Kontaktpflege hinzugekommen.

Begleitend zum Ausbruch der Covid-19 Pandemie führte das Capgemini Research Institute eine globale Studie zur digitalen Grundversorgung durch mit dem speziellen Fokus auf Menschen ohne Internet-Zugang [136]. Demnach liegen die häufigsten Gründe für die Versorgungslücken in den Kosten für Providerzugänge und Endgeräte. Die größte Altersgruppe der vom Internet Abgekoppelten sind junge Erwachsene (22 bis 36 Jahre). Die Mehrzahl von ihnen (59%) hatte bereits einmal Netzzugang und wünscht sich diesen auch zurück. 52% der Deutschen, die keinen Internet-Zugang haben, wünschen sich diesen ebenfalls für die Zukunft.

Das Kostenproblem im Providerzugang dominiert insbesondere in den ländlichen Regionen der Länder, die keine breite Anbieterkonkurrenz in der Fläche haben, wie z.B. die USA (vgl. Abschnitt 6.1.2). Schmidt und Power [137] zeigen diese Effekte der digitalen Isolation auch für Übergangsregionen am aktuellen Beispiel von “Quasi-rural Illinois”. Die Capgemini Studie, in welcher auch Führungskräfte von gemeinnützigen Organisationen und NGOs befragt wurden, unterstreicht die Dringlichkeit der Überwindung dieser digitalen Kluft, denn

- offline zu sein führe zu sozialer Ausgrenzung und behindere den Zugang zu öffentli-

chen Dienstleistungen;
- offline zu sein schränke die berufliche Mobilität ein;
- mit der digitalen Spaltung gehe es auch darum, die Kluft bei den digitalen Fähigkeiten und Bildung zu überwinden.

Diese Hintergründe werfen die Frage auf, warum zwar eine Befreiung von den Rundfunkgebühren sowie eine Ermäßigung von Telefon-Verbindungsentgelten[17], nicht aber eine Internet-Grundversorgung als Sozialleistungen in Deutschland vorgesehen sind.

Bildung Eine Studie der Michigan State University diagnostiziert eine ausgeprägte Korrelation zwischen der Leistungsstärke von Schülern der Klassenstufen 8 bis 11 und ihrem häuslichen Zugang zu Breitband-Internet.[18] Besonders berücksichtigt wurden hierbei häusliche Gegebenheiten in ländlichen Gebieten, in welchen Internet-Zugänge nur ungenügend oder überhaupt nicht zur Verfügung standen, aber auch familiäre Gegebenheiten, in welchen eine Internet-Versorgung nicht finanzierbar war. Schüler der betroffenen Altersgruppen hatten in 82% der Fälle Hausarbeiten, die eine Internet-Unterstützung zumindest teilweise erforderten. Entsprechend waren Schüler ohne häuslichen Internet-Zugang bei den Hausarbeiten merklich benachteiligt. Im Gegenzug nutzten Schüler mit leistungsfähigem Internet-Anschluss diesen in zwei Drittel der Fälle, um sich mit ihren Mitschülern per Video-Chat auszutauschen und zu mehr als 50%, um ihre Lehrer per E-Mail für Rückfragen zu kontaktieren.

> "Children in urban areas are exposed to the digital world almost from the time they are born. However, children in tribal, rural communities may never even have access to primary education, let alone the digital world. While literacy levels are going up across the country and connectivity is improving, people in remote areas remain excluded as a result of not having access to reliable, high-speed connectivity." —— Amit Chakravarty, ICRISAT [136]

In Deutschland verfügt die überwiegende Mehrzahl der Haushalte über einen Internet-Zugang, wenn auch zuweilen nur mithilfe eines Smartphones. Einer aktuellen Studie des Deutschen Instituts für Wirtschaftsforschung (DIW Berlin)[19] zufolge haben deutlich weniger als 10% der Haushalte keinen Internet-Zugang, wohingegen mehr als 10% keinen PC/Laptop ihr Eigen nennen. In beiden Fällen zählen die Schüler dieser Haushalte überwiegend zu den Leistungsschwächeren.

Wirtschaftliche Rückwirkungen und Geschäftschancen Für den deutschsprachigen Raum haben Briglauer et al. [138] empirisch ausgewertet, wie die Versorgung mit unterschiedlichen Breitbandtechnologien das regionale BIP-Wachstum in Landkreisen beeinflussen. Auf der Basis von mehrjährigen Umfragedaten wurden sowohl die technischen wie die sozialen (etwa Schulabschlüsse und Ausbildungsgrade) Entwicklungsdaten in 401 Landkreisen analysiert. Im Ergebnis stellt die Studie fest: "Wenn in einem Landkreis die Versorgung mit schnellem Breitband-Internet um einen Prozentpunkt steigt, wächst das regionale BIP zwischen 0,05 Prozent und 0,09 Prozent. Dieser Effekt ist etwa doppelt so hoch,

[17] Hierbei handelt es sich um freiwillige Leistungen einiger Telekommunikationsanbieter.

[18] `https://quello.msu.edu/broadbandgap/`

[19] `https://www.diw.de/documents/publikationen/73/diw_01.c.758242.de/diw_aktuell_30.pdf`

wenn regionale externe Effekte einbezogen werden. Das heißt: Die Breitband-Infrastruktur eines Landkreises wirkt sich signifikant positiv auf die Breitband-Infrastruktur benachbarter Landkreise aus."[20]

Die Autoren finden ferner Evidenz dafür, dass regionale Verdichtung der Breitbandversorgung besonders starke Wirkung in ländlichen Regionen entfaltet. Die Ursachen für diesen Wirkungstrend können zum einen in dem Mangel an einfachen Ausweichstrategien gesehen werden. Ansässige eines unterversorgten Landkreises müssten ihre angestammte Region verlassen, um in Gebiete mit guter Breitbandversorgung umzuziehen, und würden dadurch unter Umständen ihre Kundennähe und ihre soziale Einbettung aufgeben. Dies steht im Gegensatz zu Akteuren in Metropolregionen, für welche ein Wechsel des städtischen Bezirks oder Vororts bereits die gleiche Wirkung erzielen kann, aber viel weniger beeinträchtigend wirkt.

Erhebliche Potentiale liegen andererseits in den geringeren Kosten für Wohn- und Gewerberaum bei gleichzeitig höherer Eigentumsquote in ländlichen Gebieten. Der Auf- bzw. Ausbau eines Gewerbes oder einer selbständigen Tätigkeit kann – soweit Kollaborationen und Logistik mithilfe vernetzter Prozesse ortsungebunden möglich sind – oft mit erheblich geringeren geschäftlichen Risiken realisiert werden als in Metropolregionen. Darüber hinaus ist schon statistisch zu erwarten, dass die Digitalisierung auch im ländlichen Raum erhebliche Entwicklungsmöglichkeiten für bestehende Klein- und Mittelständler sowie Gründungspotentiale für heranwachsende Generationen und auch jene eröffnet, die ein Leben auf dem Lande der Stadtwohnung vorziehen. Eine flächig verfügbare Grundversorgung mit leistungsfähiger Netzwerkinfrastruktur kann solche Geschäftschancen in ländlichen Regionen deutlich verstärken.

Politische und soziale Spaltung Bereits im Jahr 2013 haben Townsend et al. [139] eine vielschichtige Untersuchung über die Verbreitung von Breitbandzugängen im ländlichen Raum des Vereinigten Königreichs durchgeführt und – neben der Verfügbarkeit von Zugangstechnologien – vor allem auf Akzeptanzprobleme bei der ländlichen Bevölkerung hingewiesen, welche in einer empirischen Studie vom PEW Research Center aus den USA aktuell bestätigt werden.[21] Hohe Kosten, vor allem aber fehlendes Interesse bzw. "digitaler Analphabetismus", welcher nur zum Teil altersbedingt ist, bremsen die Verbreitung. Die Autoren heben das Spannungsverhältnis zwischen Nutzungsangeboten und Exklusion hervor: Ein Schlüsselweg zur Verbreitung digitaler Technologien sind digitale Angebote und ihre Nutzung, z.B. die Verbreitung von Funktionen im eGovernment und anderen digitalen Diensten des Alltags. Je mehr allerdings digitale Dienste den Alltag bestimmen, umso stärker werden diejenigen ausgegrenzt, welche – aus welchen Gründen auch immer – über keinen Zugang verfügen.[22] Politik und Gesellschaft müssen deshalb erhöhte Sorgfalt und Umsicht bei der Einführung und Verbreitung digitaler Technologien des Alltags aufbringen, um die digitale Spaltung nicht in eine tiefe soziale Spaltung münden zu lassen.

[20] https://www.zew.de/presse/pressearchiv/schnelles-breitbandinternet-steigert-das-regionale-bruttoinlandsprodukt/

[21] https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/

[22] Ein aktuelles Beispiel ist die Umsetzung der EU PSD2 Richtlinie zur 2-Faktor-Authentifizierung durch viele Banken mithilfe des SMS-basierten "3D-Secure"-Verfahrens, welches alle Kunden ausschließt, die keinen SMS-Zugang haben.

Die Spaltung zwischen städtischen und ländlichen Räumen besitzt eine lange Tradition in Europa, welche sich zunächst entlang der ungleichen Bildungsversorgung entwickelte, später aber auch in einer ungleichen Verteilung qualifizierter Arbeitsplätze und Aufstiegschancen festigte. In ihrer "Dialektik der Aufklärung" [140] haben Horkheimer und Adorno diese Spaltung als eine Ursache für die Verbreitung des Nationalsozialismus in Deutschland identifiziert — nicht zuletzt deshalb haben Bildungspolitiker insbesondere der 60er und 70er Jahre in Deutschland stark in die Versorgung der ländlichen Räume mit Schulen, aber auch mit höheren Bildungseinrichtungen wie Fachschulen und Fachhochschulen investiert. Die urban-ländliche Spaltung besteht aber in Europa fort. So hat die EU in einer Studie über die Entstehung des Brexits [141] auch die Rolle der Bevölkerungen in Stadt und Land untersucht. Die Analysen zeigen u.a. ein ausgeprägteres anti-europäisches Wahlverhalten in ländlichen Regionen, welches zusätzlich mit geringeren Bildungsabschlüssen korreliert.

Digitale Kommunikations- und Kollaborationstechnologien gemeinsam mit einer flächigen Breitbandvernetzung machen heute Qualifikation genauso wie viele qualifizierte Tätigkeiten weitgehend ortsunabhängig. Sie eröffnen damit weitreichende Möglichkeiten für die Überwindung der Spaltung zwischen städtischen und ländlichen Regionen. Deshalb erscheint es auch aus soziologischer Sicht vordringlich, den Breitbandausbau in den ländlichen, teilweise abgeschiedenen Landesteilen zügig voranzutreiben.

6.2.2 Sicherheit und Katastrophenschutz in einer konsolidierten IP–Welt

Die Aufrechterhaltung der öffentlichen Sicherheit, eine allgegenwärtige Unterstützung in Notfällen sowie der Schutz vor Katastrophen sind fundamentale, unverzichtbare Leistungen des Staates für seine Bevölkerung. Ihrer Absicherung dienten in der Vergangenheit verschiedene spezialisierte und weitgehend isolierte Infrastrukturen wie Sirenen, Notrufsäulen, reservierte Telefonkanäle etc.. So verfügte das öffentliche Telefonsystem bis zur Ablösung der (digitalen) ISDN-Infrastruktur über eine eigenständige Stromversorgung – Notrufe konnten auch nach einem Stromausfall vor Ort abgesetzt werden. Darüber hinaus konnten die Broadcast-Medien von Radio und Fernsehen als zuverlässige Informationsverbreitung für das Erreichen der Gesamtbevölkerung angesehen werden. Inzwischen sind die spezialisierten Infrastrukturen weitgehend abgebaut, das Telefonnetz ist auf das Internet-Protokoll migriert, und viele Menschen konsumieren Audio- und Video-on-Demand Dienste anstelle der klassischen Broadcaster. Entsprechend müssen die Kommunikationskanäle für die zivile Sicherheit und den Katastrophenschutz angepasst werden.

Pluralisierung durch Privatisierung der Infrastruktur Die weitgehend vollständige Konsolidierung der Kommunikationsdienste in eine IP–Welt muss als ein horizontaler Prozess in dem Sinn verstanden werden, dass alle Kommunikation auf eine gemeinsame Netzwerkschicht, dem Internet Protokoll, zusammengeführt wurde. Diese standardisierte Abstraktionsschicht vereint unterschiedliche Netzwerkzugangstechnologien genauso wie unterschiedliche Infrastruktur-Provider. Der Konvergenz der Dienste im Internet ging die flächige Internet-Versorgung voraus, welche wiederum durch den (regulierten) Wegfall der Telekommunikationsmonopole in den 90er Jahren und dem nachfolgenden Entstehen vieler Netzdienstleister beschleunigt wurde. Im Gegensatz zum Internet waren die nationalen Telekommunikationsmonopolisten vertikal konsolidiert. Alle Zugangs- und Vermittlungs-

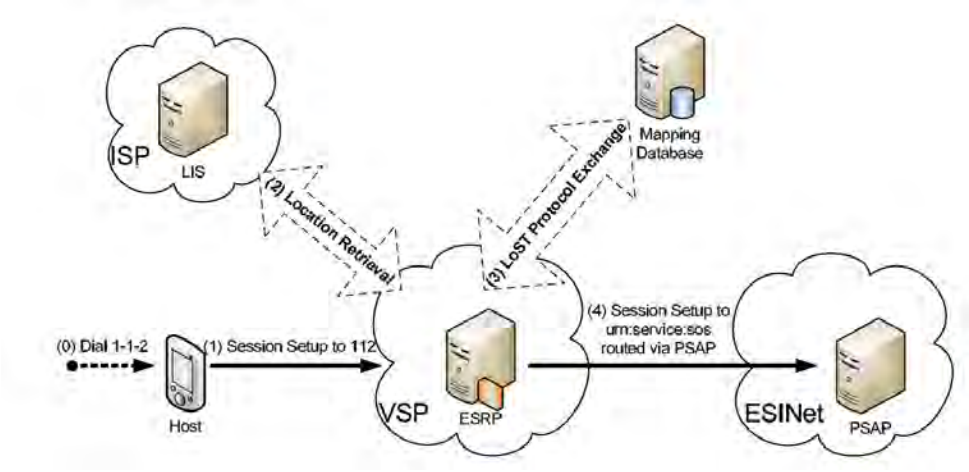


Abbildung 6.23: Internet Architektur für Notrufdienste: Ein eingehender Notruf wird über eine LoST–Ortsabbildung auf den lokale zuständigen Rettungsdienst abgebildet (Quelle: Tschofening)

technologien genauso wie alle Infrastrukturdienste waren in der Hand der Monopolisten vereint und standardisierte Datenaustausche fanden (schichtenübergreifend) an den Infrastrukturübergängen zwischen den nationalstaatlichen Versorgern statt.

Die horizontale Integration entlang der Internet-Protokollschicht eröffnete einfache Wege, um die monolithischen Infrastrukturen der "Telekoms" aufzubrechen und die (internetbasierte) Kommunikationsversorgung durch viele, meist privatwirtschaftliche Betreiber erbringen zu lassen. Insofern hat die (horizontale) Konsolidierung auf der Netzwerkschicht eine (vertikale) Pluralisierung bei der Versorgung mit Kommunikationsinfrastrukturen bewirkt. Diese Pluralisierung der Infrastruktur erschwert die Erbringung einheitlicher Rufdienste und ihre Absicherung auf gleichmäßigen Qualitätsstandards erheblich. Die Erbringung dieser gesellschaftskritischen Dienste kann einerseits über robuste, weitflächig implementierte Anwendungsstandards oder durch eine partielle Rückkehr zu einer vertikalen Dienstmonopolisierung erfolgen.

Notrufe in einer "All-IP" Welt Notrufdienste wie nach Feuerwehr oder Rettungsdienste werden in Deutschland wie in vielen Regionen der Welt dezentral (kommunal) beantwortet. Dem liegt die Idee zugrunde, bei kurzen Wegen schnell Hilfe leisten zu können. Das traditionelle Konzept der Notrufabwicklung besteht darin, dass eine in Not geratene Person einen einfachen, allgemeingültigen Zugang zu dem nationalen Notrufsystem anwählen kann — die Sammelnummer 112 etwa oder Notrufsäulen in Straßen oder Bahnhöfen — und daraufhin zu der lokal zuständigen Hilfsorganisation vermittelt wird. Während die leitungsvermittelnde Festnetzinfrastruktur die Lokalisierung und Vermittlung durch lokale Rufweiterleitung einfach ermöglichte, machen die Ortsveränderlichkeit von Mobiltelefonen, insbesondere aber die Ortstransparenz einer durchgängigen Internet-Welt die Lokalisierung und Zuordnung von Notrufen komplizierter. Zunächst muss der Ort eines Notrufenden bestimmt werden, hiernach muss die lokal zuständige Notrufinstanz ermittelt und angerufen werden.

Die Ortung eines Mobiltelefons kann mithilfe von eingebauten Sensoren (etwa GPS-Empfängern) oder kurzreichweitigen Zugangspunkten (z.B. WLAN Access Points) erfol-

gen. Gängige SmartPhones (z.B. iPhones oder Android-Geräte) führen heute diese Ortung nach der sogenannten Advanced Mobile Location (AML) der European Emergency Number Association (EENA) durch. Diese Mechanismen sind ausgeprägt gerätespezifisch und werden von den Mobilgeräteherstellern favorisiert. Sie sind für generische Internet-Geräte ohne spezifische Sensorik genauso ungeeignet wie für den IoT Edge. In Deutschland werden die AML-Rufe über die zentrale Einrichtung der "ILS Leitstelle" in Freiburg verteilt – eine vertikal integrierte, singuläre Einrichtung.

Die IETF hat im Rahmen ihrer ECRIT (Emergency Context Resolution with Internet Technologies) Arbeitsgruppe die Internet Emergency Services Architecture [142] (vgl. Abbildung 6.23) und insbesondere das Location to Service Translation (LoST) Protokoll [143] als offene Standards entwickelt. Die LoST Mapping Architecture kann in mehreren verteilten Hierarchien (Forests) angeordnet werden und erlaubt so eine transparente Weitverkehrsverteilung [144], welche horizontal integrierbar ist. Diese Standards werden in den US Notrufnetzen für die Rufweiterleitung genutzt, in der europäischen Regulierung sind sie erst wenig präsent und werden auf den Endgeräten nicht unterstützt.

Schutz kritischer Komponenten, Abwehr von Informationsverfälschungen und Betriebsgefährdungen Notruf- und Alarmsysteme der Behörden für den Bevölkerungsschutz, im Englischen „Alerting Authorities', bilden eine kritische Infrastruktur, deren zuverlässiger Betrieb, deren Verfügbarkeit und Informationsqualität und -integrität wichtige Güter bilden. Ihr Schutz ist unmittelbar verknüpft mit dem Vertrauen der Bevölkerung in die Institutionen und ihr Handeln.[23] In den horizontal integrierten, internet-basierten Systemen, wie sie gegenwärtig dominieren, muss die technische Sicherheit und Zuverlässigkeit auf jeder Schicht separat hergestellt werden.

Dienste im Internet werden fast immer per Namen angesprochen, weshalb dem Schutz der Namen und ihres DNS-Auflösungsprozesses zentrale Wichtigkeit zukommen. Namen können vielfältig angegriffen werden. Neben der Namensauflösung selbst, die mittels DNSSEC [145, 146, 147] abgesichert werden kann, können Namensnutzungen durch fehlgeleitete Intuitionen (z.B. `Hilfe.de`) oder per Typosquatting (z.B. `Polizei.org`) auf Abwege geführt werden. Um solchen Gefährdungen vorzubeugen, haben die Gestalter des DNS Namensraumes ursprünglich eine eingeschränkte Namensvergabe in ausgewählten Toplevel-Domains vorgesehen (z.B. `.gov, .mil`). Es steht Nationen frei, über nationale Gesetzgebungen die Namensräume ihres Landes (z.B. .de) entsprechend zu regulieren.

Ist ein Dienst über seinen Namen gefunden, so muss seine Authentizität i.d.R. über ein Zertifikat nachgewiesen werden. Zertifikate können einen Ursprung dabei über ein "organisation/extended validation certificate" (OV/EV) stark authentifizieren oder lediglich über ein "domain validation certificate" die (aktuelle) Zugriffsverfügung auf die Web-Domain schwach authentifizieren. Im letztgenannten Fall, den populäre CAs wie Let's Encrypt verfolgen, können Zertifikate vergleichsweise leicht duch Überlisten erschlichen werden. Der Zugriff auf die Dienstrepräsentanz, den aktuellen Server im Internet also, wird über das Internet Routing möglich gemacht, welches wiederum über die Resource Public Key Infrastruktur (RPKI) [148] absicherbar ist.

[23] Wir erleben in der andauernden Corona-Krise, dass bereits kleine Unstimmigkeiten und operative Probleme in der Datenerhebung – etwa bei den täglichen Inzidenzermittlungen – zu Irritationen und Spekulationen in der Bevölkerung führen.

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	126
				Total:	1036 (≈ 78%)
				Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate (see Table 1)

Abbildung 6.24: Web-Sicherheitsanker der FEMA “Alerting Authorities”

Exemplarisch haben wir die effektiven Schutzmaßnahmen der Alarm-Infrastrukturen für die USA untersucht, wie sie in der Federal Emergency Management Agency (FEMA) zusammengefasst sind [149].[24] Ergebnisse für die ungefähr 1.300 beteiligten Institutionen sind in Tabelle 6.24 zusammengefasst.

Klar ersichtlich wird, dass nur etwa 2% der Institutionen alle erforderlichen Mechanismen zur Absicherung ihrer Namen und Zertifikate einsetzen. 98% machen unter Sicherheitsgesichtspunkten Fehler. Dabei sichern weniger als 4% der Institutionen ihre Namensauflösung per DNSSEC ab. Nur 22% der Beteiligten bietet eine zuverlässige Namensidenifikation – mehr als die Hälfte verfügen über gar keine eigene Namensdomäne. Fast 80% nutzen nur “domain validation” Zertifikate, die schnell und kostengünstig verfügbar sind. Mehr als 10% verzichten vollständig auf Zertifikate.

Insgesamt zeigt diese Analyse, dass horizontal integrierte Sicherheitsmechanismen, wie sie die Internet-Infrastruktur erfordert, in Kontexten von eingeschränkter Kompetenz und beschränkten Budgets nur unvollständig oder überhaupt nicht angewendet werden. Es erscheint vergleichsweise schwierig, Minimalstandards der Internet-Sicherheit in einem flächigen Deployment zu verbreiten und über die Zeit des Dienstebetriebs zu erhalten.

6.2.3 Konsolidierung der Content-Plattformen und das “Rabbit Hole”

Angebotsplattformen im Internet bauen ihr Geschäftsmodell auf Plattformbesucher, also Kunden, die Plattformangebote betrachten, auf. Diese Angebote können unmittel-

[24] Eine analoge Untersuchung für Europa bzw. Deutschland konnte aufgrund fehlender Verzeichnislisten für die Sicherheitsorganisationen nicht durchgeführt werden.

bare Waren, etwa in der Amazon Handelsplattform, sein oder (audiovisuelle) Inhalte wie in Youtube, Instagram, Twitter oder Facebook, deren Betrachtung zur Verbreitung von Werbung sowie zur Schärfung von werbewirksamen Persönlichkeitsprofilen dient.

Ein universelles Ziel dieser Plattformen besteht deshalb darin, die Betrachter auf der Plattform zu halten, also die Präsenz der Nutzer solange wie möglich auszudehnen. Moderne Plattformen beinhalten zu diesem Zweck Empfehlungssysteme. Nachdem Amazon sehr frühzeitig "Buchtips" an die Käuferseite stellte ("Kunden ... haben auch dieses Buch gekauft") und damit zunächst auf ein bildungsbürgerliches Wohlwollen (etwa: Amazon hilft bei der Erweiterung des Bildungshorizontes) getroffen sind, haben sich online-Konsumenten daran gewöhnt, dass Plattformen ihnen Inhalte zum Konsum vorschlagen. Inzwischen schlagen Plattformen wie Youtube nicht mehr nur potentielle nächste Klicks vor, sondern reihen Filme automatisch aneinander und spielen Folgevorschläge ohne weitere Nutzerzustimmung einfach ab.

Sogenannte "Recommender-Systeme" sind inzwischen integraler Bestandteil aller großen Plattformen und verfehlen ihre Wirkung, die Kunden auf der Plattform zu halten, nicht. Jahrelange Forschungs- und Entwicklungsarbeiten sind z.B. bei Google in Youtube geflossen, um ein erfolgreiches Empfehlungssystem zu schaffen, welches in der kritischen Fachliteratur als "Youtube Rabbit Hole"[25] bekannt geworden ist. Vorgehen und Algorithmik sind nicht vollständig transparent, doch soll das Google KI-Team "BRAIN" zunächst zwei Neuronale Netze, eines zur Klassifizierung des Nutzerverhaltens und eines zur Klassifizierung der Inhalte betreiben, welche dann so verknüpft werden, dass sich die Präsenzzeiten der Betrachter maximieren.[26]

Einfache Lernverfahren neigen jedoch dazu, auf ausgeprägte Merkmale zu konvergieren und so nur inhaltlich eng zusammenhängende Angebote auszuwählen – etwa Inhalte desselben Autors bzw. desselben Kanals. Begleitende Nutzerstudien haben dies als "langweilend" identifiziert, weshalb das Google BRAIN Team komplexere, sogenannte Reinforcment-Lernverfahren eingeführt hat. Beim Reinforcement-Learning werden mithilfe von Monte-Carlo-Techniken gesteuerte Zufallssprünge im Zustandsraum durchgeführt, so dass das KI-System sich auch von den ursprünglichen Inhalten diskontinuierlich fortbewegen kann. Dem Betrachter soll so nie langweilig werden und Gründe, die Plattform zu verlassen, minimiert werden.

Das "Rabbit Hole" steht im Verdacht, wesentlichen Einfluß bei der Verbreitung abseitiger Inhalte und der Radikalisierung einzelner Bevölkerungsgruppen zu haben. Das naive Verbreitungsbild verläuft etwa wie folgt: Ein (mehr oder minder) Ahnungsloser erhält auf einem Drittweg, etwa per Mail oder sozialem Netzwerk, Stichworte[27] oder Links auf Inhalte am gesellschaftlichen Rand, z.B. aus einer Verschwörungstheorie. Die neugierige Person sucht oder klickt auf die verteilten Schlüsselinformationen, woraufhin die Lernmechanismen der Content-Plattform die Person mit dem entsprechenden inhaltlichen Cluster verknüpfen. Fortan werden der Person Inhalte aus dem betroffenen Cluster angeboten und darüber hinaus bringen die Sprungfunktionen des Reinforcement-Learnings auch ent-

[25] Der Begriff ist von dem Kapitel "Down the Rabbit Hole" aus dem Buch Alice in Wonderland abgeleitet, in welchem Alice durch das Hasenloch in eine gefangene Welt eintaucht.

[26] `https://medium.com/swlh/understanding-the-youtube-rabbit-hole-4d98e921eabe`

[27] Ein beliebter, werbewirksamer Verbreitungsweg animiert Empfänger zur aktiven Informationssuche: "Schau selbst, was es mit XYZ auf sich hat."

ferntere, aber kategoriell noch ähnliche Inhalte in die Vorschlagslisten. Insbesondere die letztgenannten Sprünge werden oft für die Radikalisierung der Betrachter verantwortlich gemacht, weil hierdurch auch extremistischere bzw. komplementär verstärkende Inhalte in den Fokus gerückt werden.

Dieses naive Bild wird in letzter Zeit zunehmend auch wissenschaftlich untersucht. O'Callaghan et al. [150] haben den Einfluss des Youtube Empfehlungssystems auf die Bildung "extrem rechter" (ER) Gesinnung im englisch- und deutschsprachigen Raum untersucht. Die Autoren verwenden Methoden zur Themenmodellierung, um viele tausend Youtube-Kanäle und Dokumente zu klassifizieren. Klassifikationen erfolgen sowohl nach ER-Kategorien (z.B. antisemitisch, revisionistisch, neo-nazi, etc.), als auch nach unabhängigen Kategorien (z.B. Musik, Gaming, Nachrichten, Religion, etc.) Auf dieser Basis gelingt es, sowohl im Englischsprachigen wie im Deutschen sogenannte ER "Content Bubbles", also Gruppen von Inhalten, die vom Youtube Recommender-System wechselseitig empfohlen werden und als Blase konstant präsent bleiben, zu identifizieren. Die Autoren schließen, dass Nutzer schon nach wenigen Klicks von diesen Inhaltsblasen eingefangen werden, wenn sie sich nicht aktiv dagegen stemmen. Dieselben Autoren [151] konnten ebenfalls zeigen, dass Twitter und sein Recommender-System eine Eintrittsfunktion in extremistische Inhalte wahrnimmt, also als Gateway in extremistische Kanäle z.B. bei Youtube fungiert.

Der Einfluss der Inhaltsempfehlungen im Fall von ER – hier Inhalte der amerikanischen Alt-right Bewegung – wurden von Ribeiro et al. [152] im Rahmen einer großen empirischen Studie untersucht: 330.925 Videos aus 349 Kanälen wurden zusammen mit ihren 72 Millionen Nutzerkommentaren analysiert. Die Autoren klassifizieren die Youtube-Kanäle zunächst in die Kategorien "Media", also normale Medienkanäle wie Vox oder Vice News, "Intellectual Dark Web (I.D.W.)", also Inhalte von Kommentatoren wie von der Prager University, die oft konservativ und oppositionell zu Mainstream und Identitätspolitik stehen, "Alt-lite" als gemäßigtere Eintrittsportale in die rechte Szene sowie "Alt-right" Inhalte als Cluster der extremen Rechten. Die Autoren identifizieren Nutzer und analysieren ihre Kommentare auf der Plattform. Hierdurch wird einerseits der spezifische Inhalte-Konsum sichtbar, andererseits werden Verhaltensstudien über mehrjährige Zeiträume möglich.

Die Autoren können zunächst durch eine Korrelationsanalyse der verschiedenen Nutzergruppen zeigen, dass seit 2015 die Konsumentengruppen von I.D.W., Alt-lite und Alt-right mit aktuellen Überlappungen zwischen 10 und 20% immer ähnlicher geworden sind.

Die Nachverfolgung des Nutzerverhaltens nach dem Erstkontakt mit Alt-right-Inhalten werden in Abbildung 6.25 gezeigt. Differenziert nach der vorherigen Zugehörigkeit zu einer Inhaltsgruppe und nach den Zeitpunkten des Erstkontakts mit Alt-right Content, wird die Wanderung von Nutzern in den Alt-right Inhaltskonsum gezeigt. Dabei untergliedern die Autoren je nach Häufigkeit von Nutzerkommentaren in drei Intensitätsgruppen (Light, Mild, Severe). Diese Graphen zeigen zwei deutliche Tendenzen. Zum einen ist die Migrationstendenz der Nutzer aus der Alt-lite-Gruppe deutlich ausgeprägter als der der I.D.W und noch geringer bei den Media-Konsumenten. Zum anderen beschleunigt sich die Migration insbesondere seit den Jahren 2015/2016, d.h. Nutzer wandern entschiedener in den Konsum von Alt-right Inhalten. Die Autoren führen dies auf die Einführung des Video-Pipelinings in Youtube zurück und können weiterhin zeigen, dass mehr als 40% der gegenwärtigen Alt-right Content-Konsumenten von hoher Intensität (Severe) aus der

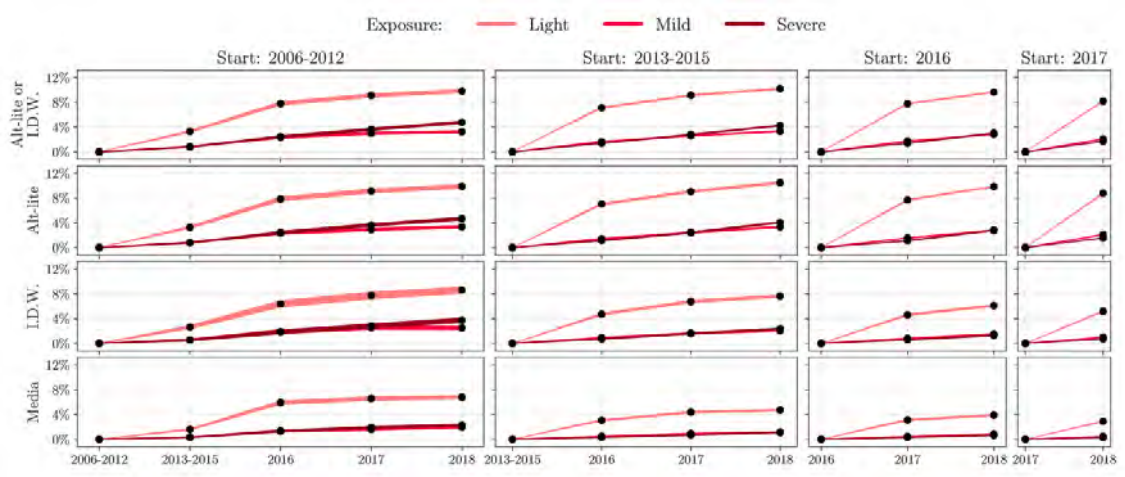


Abbildung 6.25: Wanderbewegung verschiedener Inhaltskonsumenten hin zu Alt-right Content nach der ersten Konfrontation mit diesen Inhalten - die Graphen beziehen sich auf unterschiedliche Zeiträume. Unterschieden wird zwischen geringer Bindung (Light: ein bis zwei Kommentare), mittlerer Bindung (Mild: drei bis fünf Kommentare) und starker Bindung (Severe: sechs und mehr Kommentare). (Quelle: Ribeiro et al.)

Gruppe derer entstammen, die vor 2015 lediglich Alt-lite oder I.D.W. Inhalte betrachteten. Damit ist eine sehr deutliche Radikalisierungstendenz der Youtube Plattformnutzer im Falle von Alt-right-Inhalten belegt.

Für 2019 analysieren Ledwich und Zaitsev [153] den algorithmischen Einfluss auf die Radikalisierung der Nutzer. Dabei nutzen sie die Daten von 800 politisch orientierten Youtube-Kanälen, welche inhaltlichen Kategorien zugeordnet werden, und messen die von Youtube vorgeschlagenen Übergänge. Eine detaillierte Flußanalyse der Autoren zeigt auf, dass Youtube Empfehlungen mehrheitlich in derselben inhaltlichen Kategorie oder zu einer benachbarten erfolgen, wie die Flußübersicht in Abbildung 6.26 zeigt. Allerdings ändern sich die Häufigkeiten der Kanalübergänge mit den Kanälen bzw. Kategorien. “Center/Left MSM” etwa hat 51% Kanalübergänge innerhalb derselben Kategorie und starke Kategorieübergänge. Andere Kategorien fluktuieren deutlich schwächer.

Die Autoren diagnostizieren auch, dass das Empfehlungssystem Sprünge in extreme Inhalte, insbesondere stark rechts gerichtete oder dubiose Kanäle eher meidet. In Abbildung 6.26 fällt so der vernachlässigbare Zufluß zu Verschwörungskanälen auf, welche wiederum als Ursprung in rechtsrebellische Kanäle der Kategorie “Partisan Right” geleitet werden. Youtube Empfehlungen, so identifizieren die Autoren, haben thematisch differenzierte Akzente und tendieren gegenwärtig eher zu Mainstream-Inhalten. Es ist denkbar, dass diese aktuellen Beobachtungen, welche früheren Untersuchungen eher widersprechen, auf neuere Modifikationen des Youtube Recommender-Systems zurückzuführen sind.

6.2.4 Aspekte der Netzneutralität

Ein wirtschaftlich wie gesellschaftlich kontroverses Handlungsfeld wurde unter dem Schlagwort Netzneutralität bekannt. Netzneutralität bezeichnet den diskriminierungsfrei-

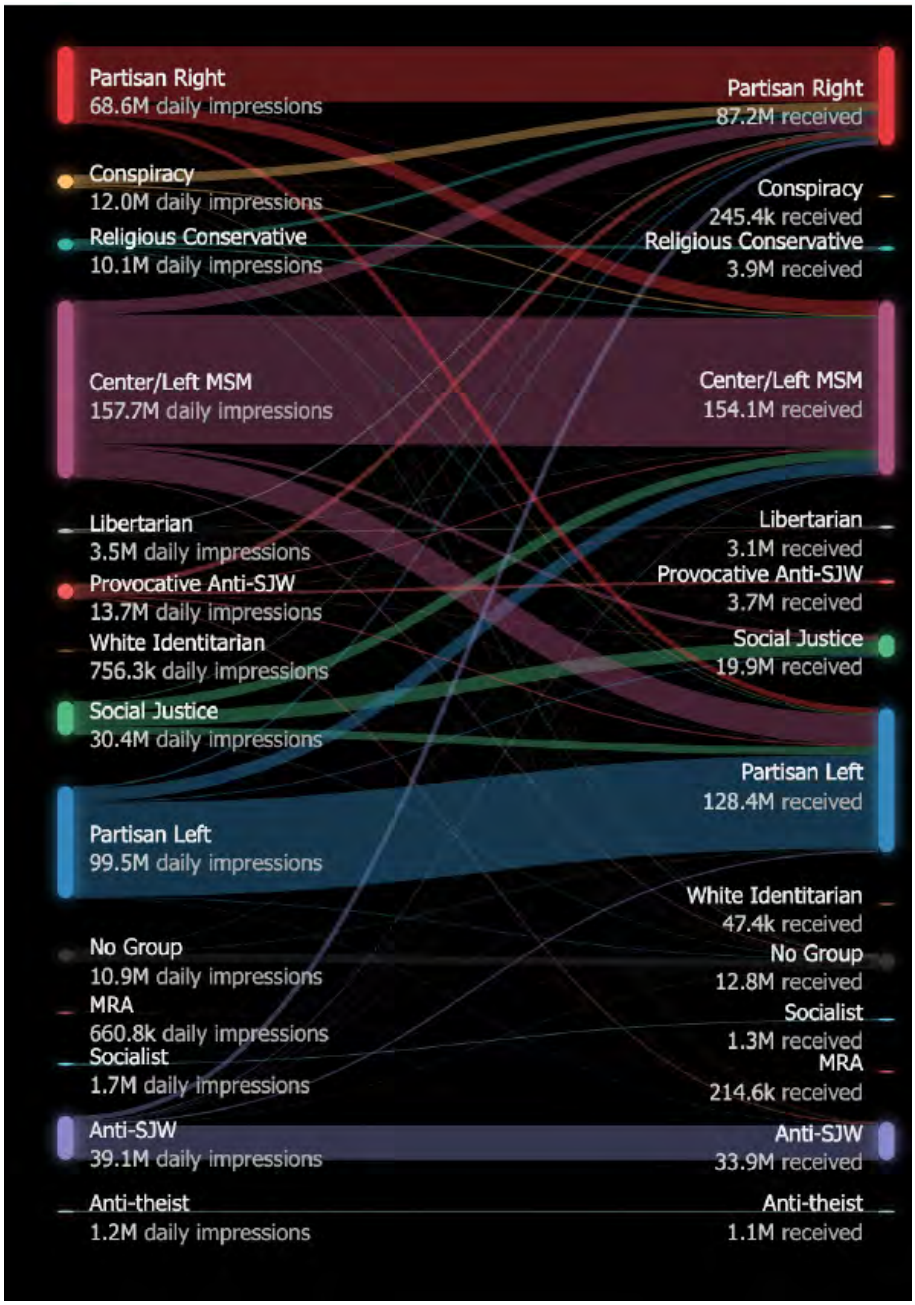


Abbildung 6.26: Übersicht über die Flüsse von Empfehlungen zwischen kategorisierten Kanälen. (Quelle: Ledwich und Zaitsev)

en Netzbetrieb, also die gleichmäßige Paketweiterleitung unabhängig von Inhalt, Ursprung oder Ziel. Der Begriff wurde bereits 2003 von Tim Wu, Columbia University, im Zusammenhang mit der künftigen wettbewerblichen Entwicklung der Internet-Infrastruktur und ihren regulatorischen Anforderungen eingeführt [154].

Netzneutralität verneint die Frage, ob Provider im Zugang oder beim Weiterleiten von Daten inhaltlich oder topologisch differenzieren dürfen – etwa Dienste bevorzugen oder benachteiligen bzw. sogar blockieren dürfen. Netzneutralität steht im Gegensatz zu vielfältig ausgeübter Provider-Praxis, wonach Priorisierungen als Spezialdienste vermarktet werden. In enger Auslegung steht Netzneutralität ebenfalls im Widerspruch zu vertikal integrierten Diensten, etwa QoS-gestützten Sprachdiensten oder Notrufsystemen. Das Thema birgt also eine deutlich höhere Komplexität als der einfache Titel suggeriert.

Ambivalenz der Neutralität im Netz Es erscheint dementsprechend sinnvoll, Neutralität im Netz aus verschiedenen Perspektiven zu betrachten und Netzneutralität als vielschichtiges Phänomen zu begreifen. Ganz allgemein hängt die Bewertung von Neutralität von der Grundmenge derer ab, die gegeneinander neutral sein sollen. Betrachten wir mit der Kern-Netzwerkschicht im Sinne des Ende-zu-Ende Prinzips [155] nur IP Pakete, so wäre Netzneutralität gleichbedeutend mit dem gleichmäßigen, ungefilterten Weiterleiten der Pakete.[28] Betrachten wir dagegen Netzanwendungen, so wären gleichmäßige Übertragungsqualitäten konform zu den Anforderungen ihrer Anwendungsklassen – etwa hohe Datenraten versus geringe Latenzen – im Fokus.[29]

> "IP was only neutral among data applications. Internet networks tend to favor, as a class, applications insensitive to latency (delay) or jitter (signal distortion)." —— Tim Wu, Columbia University [154]

Eine alternative, heute vielfach bevorzugte Annäherung an das Thema Neutralität im Netz kann über die Identifikation von Diskriminierungen erfolgen, welche dann einzeln zu bewerten sind. Diskriminierungen zum Schutz des Netzes, die Blockade von DDoS Angriffen etwa, können so differenziert betrachtet werden von der Diskriminierung einzelner Inhalte, etwa die Benachteiligung des Cloudflare CDNs gegenüber Akamai. Es bleibt dabei fallweise das breite Feld der wirtschaftlichen Diskriminierungen zu regeln, wie sie heute gängig angewandt werden. Beispiele reichen vom Unterbinden permanenter Serverdienste an Endkundenanschlüssen über dediziert buchbare "Kanäle" mit geringer Latenz bis zu beschränkten Zugängen, welche den Zugriff auf Dienste (z.B. E-Mail oder SSH) oder Inhalte (z.B. Youtube Videos) zu kostenpflichtigen Zusatzpaketen machen.

Es ist überraschend schwierig, Netzneutralität bzw. deren diskriminierende Verletzung zweifelsfrei zu bestimmen, denn Provider differenzieren Datenflüsse im Alltag auch ohne Diskriminierungsabsicht. Reguläres Traffic Engineering balanciert z.B. Datenflüsse zwischen großen Peers, um die Transferkapazitäten gleichmäßig auszulasten. Hierbei wird z.B. ziel- und zeitabhängig entschieden, welche Präfixe an welchen Übergängen entgegengenommen werden. Änderungen in der Datenübergabe zwischen Providern können

[28] DDoS Mitigationstechniken stünden dann streng genommen im Konflikt zur Netzneutralität.

[29] Als ein Beispiel der Neutralitätsverletzung haben in den Anfangszeiten der 3G Internetzugänge einzelne Provider künstlich Jitter induziert, um VoIP-Anwendungen zu stören.

zu topologisch bedingten Laufzeitschwankungen, aber auch zu Überlast und Datenstaus führen. Entsprechend müsste ein Nachweis der Diskriminierung auch die Datenübergänge in der Fläche dokumentieren und klar belegen, dass bestimmte Präfixe systematisch benachteiligt werden.

Auch im Netzwerkzugang ist Netzneutralität nur kompliziert erfassbar. Die reguläre Entwicklung der Leistungsfähigkeit und Verfügbarkeit erfordert Investitionen in Leitungen und Zugangstechnologien, welche in aller Regel nicht gleichzeitig, sondern kontinuierlich durchgeführt werden. Es ist deshalb normal, dass zeitlich befristete Schwankungen im Leistungsangebot gegenüber den Kunden auftreten. Allerdings geben verschiedene wirtschaftliche Argumente auch Anreize zur Diskriminierung: In Abschnitt 6.1.2 wurde bereits die strukturelle Benachteiligung der ländlichen Regionen diskutiert sowie gebremste Investitionsverläufe bei mangelndem Wettbewerb. Im zugangsregulierten deutschen Markt ließe sich zudem ein negativer Investitionsanreiz für einen Infrastrukturprovider in solchen Regionen denken, welche hohe Anteile von Kundenverträgen mit den Konkurrenzanbietern aufweisen. Ob ein Netzprovider aber bestimmte Nutzer oder Kundengruppen gezielt benachteiligt, lässt sich nur unter Würdigung des Providerhandelns über einen längeren Zeitraum beurteilen.

Die politische Dimension Unabhängig von den technischen Möglichkeiten und Grundlagen ist die Frage nach einem netzneutralen Providerverhalten eine politische, die ggfs. gesetzlich verankert werden muss. In den USA konnte das entsprechende Gesetz, der "Save the Internet Act", nach jahrzehntelanger öffentlicher Debatte noch nicht den Senat passieren. In der EU wird ein diskriminierungsfreier Internet-Zugang seit 2015 vorgeschrieben (vgl. EU Regulation 2015/2120). Die in Litauen angesiedelte BEREC: Body of European Regulators for Electronic Communications veröffentlicht Rahmenrichtlinien für die Implementierung eines offenen Internets im Einklang mit den Europäischen Regularien.[30]

Gezielte Verletzungen der Netzneutralität durch Provider wurden in der Vergangenheit zunächst vereinzelt öffentlich dokumentiert. Dabei dienten sie vor allem dem (wirtschaftlichen) Schutz der eigenen Dienste und Netze, etwa die mehrfache Störung von VoIP zum Schutz der Sprachdienste, das Blockieren von P2P-Verkehr (Comcast 2007) zur Begrenzung des Upstreams und das Beschränken von Videoströmen zur Entlastung der Zugangsnetze. Ein weiterreichender Geschäftskonflikt eskalierte von 2011 bis 2013, als AT&T, Sprint and Verizon Google Wallet blockierten, um ihren eigenen Bezahldienst Isis zu protegieren.

Messungen zur differenzierten Dienstqualität Für eine fundierte Lagebeurteilung und die valide Identifikation von Diskriminierungen sind kontinuierliche Messungen der Zugangs- und Dienstqualitäten nötig. Die amerikanische Federal Communications Commission (FCC) hat unter der technischen Leitung von Henning Schulzrinne vor 10 Jahren begonnen, hierfür Verfahren und Standards zu entwickeln. Die Aktivitäten wurden in der IETF Arbeitsgruppe LMAP[31] standardisiert.

David Choffnes, Northeastern University, leitet seit etwa drei Jahren ein Projekt

[30] https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation

[31] https://tools.ietf.org/wg/lmap/

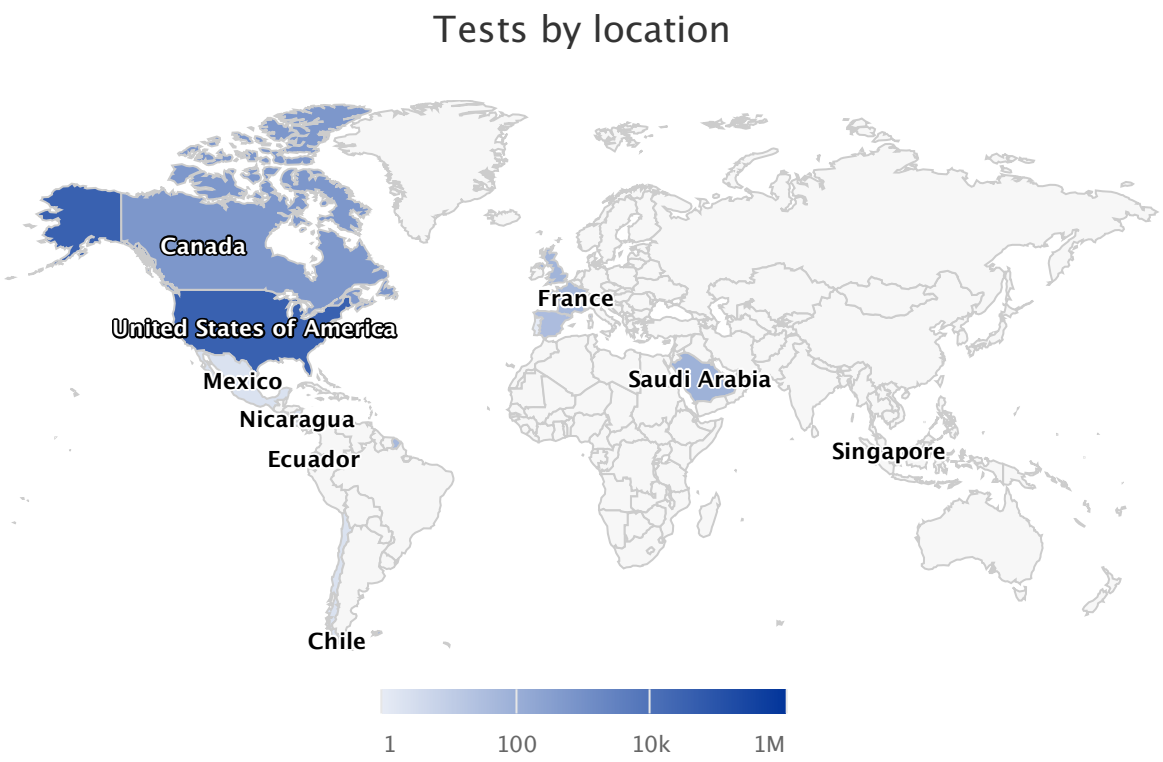


Abbildung 6.27: Geographische Verteilung der gemessenen Dienstbeschränkungen von Zugangsprovidern (Quelle: Choffnes et al.)

zur flächigen Analyse von Dienstdifferenzierungen durch Zugangsprovider. Mithilfe der Messanwendung Wehe[32] können Endnutzer ihren Provider vermessen. Das Projekt zielt auf eine weltweite Verbreitung, richtet aber besonderes Augenmerk auf die USA und Frankreich.[33] Mehr als 2 Millionen Tests wurden seit Dezember 2017 durchgeführt, wobei die Messabdeckung stark schwankt und gegenwärtig in Nordamerika, Brasilien, Europa und Australien gut ist.

Abbildung 6.27 zeigt die geographische Verteilung der Messungen, welche Netzbeschränkungen für einzelne Dienste erkennen. Neben den USA und Kanada fallen diese Beschränkungen vor allem in Großbritannien, Frankreich, Spanien und Saudi Arabien auf. Die gedrosselten Dienste sind vornehmlich Video-Anwendungen (vgl. Abbildung 6.28), was auf ein Bandbreitenmanagement der Provider zu Lasten ihrer Kunden schließen lässt.

Vor dem Start der Messungen hat die Forschungsgruppe untersucht, wie Provider die zu drosselnden Anwendungen, deren Datenverkehr ja in der Regel in *https* transportiert wird, identifizieren [156]. Dabei wurden Schlüsselwortlisten ermittelt, welche die Zugangsprovider auf (i) Hostnamen, (ii) User Agent Namen, (iii) Content Type Deklarationen und (iv) SNI-Felder der Zertifikaten anwenden. Mithilfe von Deep Packet Inspection wer-

[32] `https://wehe.meddle.mobi/`

[33] Die Messergebnisse von Wehe sind Teil des aktuellen nationalen Internet-Berichts von Frankreich: `https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2021-edition-july2021.pdf`

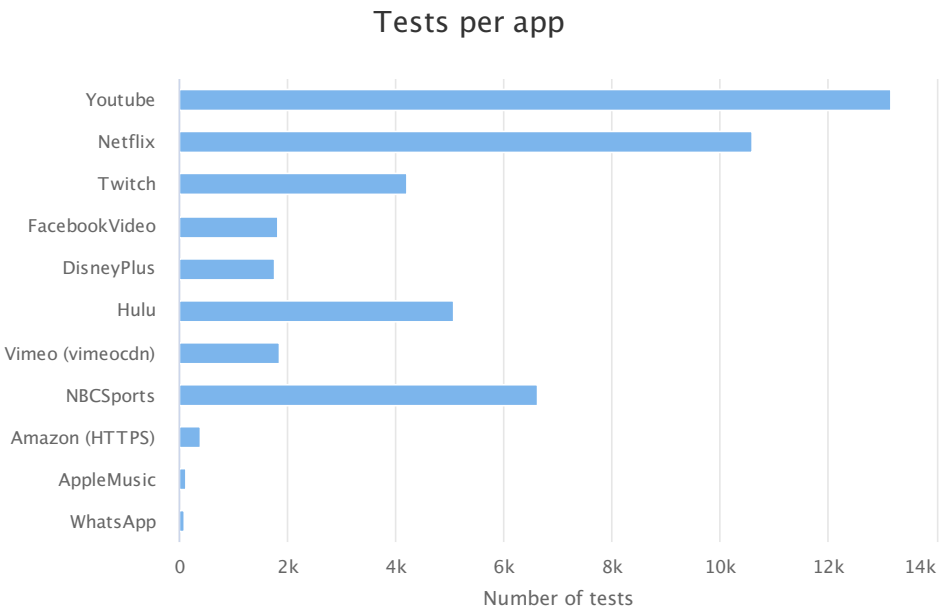


Abbildung 6.28: Anwendungsverteilung mit gemessener Dienstbeschränkungen von Zugangsprovidern (Quelle: Choffnes et al.)

den also (grobe) Inhaltsklassifikationen durchgeführt, welche Zugangsprovider technisch problemlos mit den vorhanden Kundendaten abgleichen könnten. Hieraus erwächst die prinzipielle Möglichkeit, personalisierte Inhaltspriorisierungen z.B. im Bündnis mit Werbeauftraggebern einzuführen, so wie es die Digital Gatekeepers in ihren Plattformen und Kanälen seit Jahren vormachen.

Neue Aspekte durch die Konsolidierung: DNS-Zentralisierung Das ursprünglich vollständig auf die Provider verteilte Namensverzeichnis DNS wird — getrieben von den Browser-Herstellern und den CDNs[34] — mittels der verschlüsselten Zugriffsprotokolle DoT bzw. DoH zunehmend an wenigen rekursiven Resolvern zentralisiert, wie in in Abschnitt 5.1.3 ausführlich dargestellt wurde.

Zentrale DNS-Resolver können per se Namensauflösungen verfälschen, was jedoch als grobe Störung des Internet-Betriebs auffiele. Subtiler ist ihr Zusammenspiel mit CDNs, welche die Cache-Lokalisierung optimiert für die anfragende Quelle vornehmen wollen. Um diese Cache-Lokalisierung auch für entfernte (zentralisierte) Resolver sinnvoll durchführen zu können, sind DNS Informationen über das `EDNS Client Subnet` erforderlich [157]. Diese Erweiterung des DNS ist optional, ihre Unterstützung erhöht die Nutzung von CDN-Caches in den lokalen Zugangsnetzen bei zentralisiertem DNS-Einsatz erheblich. Umgekehrt behindert die Nichtunterstützung dieses Attributs alle CDN-Dienste, welche nicht von dem zentralen DNS-Anbieter betrieben werden und deshalb keine Kenntnis der Adressen von den ursprünglich Anfragenden besitzen. Aktuelle Dispute [89] beziehen sich auf Diskriminierungen durch einen DoH-Einsatz ohne EDNS Erweiterungen (vgl. Abschnitt 5.1.3 für eine weiterführende Diskussion).

Die gezielte, willkürliche Verletzung der Netzneutralität auf der Anwendungsebene

[34]Im Fall von Apple, Google und Microsoft liegen beide Aktivitäten in denselben Unternehmen.

durch Internet-Provider, das Blockieren, Behindern oder Differenzieren von Anwendungsströmen also im Gutdünken der Netz- oder Dienstbetreiber, kann erhebliche Auswirkungen auf Kunden haben. Das Vorgehen ist häufig für Endanwender nicht einfach zu ermitteln und deshalb sind Gegenmaßnahmen wie ein Providerwechsel nur schwer rational zu entscheiden. Eine weitere Konsolidierung der Netzbetreiber, schlimmer noch regionale Monopolstellungen führen zu einem verstärkten Ausgeliefertsein der Kunden, was eine klare antidiskriminierende Regulierung unverzichtbar macht.

6.2.5 Daten, Persönlichkeitsrechte und Privatsphäre

Die Entwicklungsgeschichte des Internets hat das Entstehen indirekter Geschäftsmodelle für die Anwendungen begünstigt. Sie begann mit dem Erlebnis kostenfreier Dienste und Informationen, weil Wissenschaftler, Enthusiasten und engagierte Hobbyisten die Angebote im jungen Netz unkommerziell offerierten. Früh beteiligten sich auch kommerzielle IT-Unternehmen, die Reputationsgewinne und andere indirekte Geschäftschancen für sich identifizierten,[35] wodurch sich das konzeptuelle Konsumentenverständnis unentgeltlicher Internetdienste festigte.

Die frühen Internet-zentrierten Neugründungen wie Yahoo und Google, insbesondere aber auch die breite Welle der Internet Start-Ups in den späten 90er und frühen 2000er Jahren, sind diesem Konzept gefolgt und haben mehrheitlich auf indirekte, werbefinanzierte Geschäftsmodelle gesetzt. Mit den Ansprüchen der Werbefinanzierung wurde schnell die Personalisierung von Werbung und damit die differenzierte Erhebung von Nutzerdaten wirtschaftlich attraktiv. Mittlerweile hat sich diese Entwicklung verselbstständigt und der Handel bzw. der gezielte Anwendungsverarbeitung mithilfe von spezialisierten Daten hat sich verselbstständigt und sogar eigenständige Fachdisziplinen wie “Big Data” und “Datenzentrierte Künstliche Intelligenz” etabliert.

Datenräume und Daten-Potentiale Daten zur unmittelbaren Beeinflussung des Konsumverhaltens waren für die Internetkonzerne von Beginn an interessant, weil personalisiertes Werbeverhalten entweder die Attraktivität der eigenen Plattform steigern konnte, wie etwa bei Amazon, Facebook oder Youtube, oder an werbetreibende Dritte teurer vermarktbar war als kundenneutrale Anzeigen. Der Personalisierung lagen dabei einerseits Verhaltensdaten zugrunde, also was interessiert (per Suche oder per Klick) den Nutzer? Anderseits wurden Beziehungsdaten, also mit wem kommuniziert oder verknüpft sich ein Nutzer, schnell als wertvoll erkannt — zusammen bilden diese die primären Geschäftsgrundlagen für Google und Facebook.

Digitale Gatekeeper haben diese Interessen schnell um Kontextdaten erweitert, wie etwa: Wo und in welcher Situation befindet sich der Konsument gerade, was Smartphone-basiertes Crowdsensing ermöglicht. Wie verhält sich ein Angebot im geographischen Kontext des Nutzers — ortsbasierte Dienste also. Die äußeren Umgebungsumstände werden zusätzlich vom sich etablierenden Internet der Dinge (IoT) erfasst und erweitern die kommerzielle Datensicht grundsätzlich: Der Zugriff auf die realen Umgebungsdaten, etwa unter welchen realen Umgebungsbedingungen sich ein Mensch befindet, wie lange er z.B. auf

[35] AltaVista, die erste populäre Suchmaschine im Web, wurde 1995 von Digital Equipment in Betrieb genommen, um die Leistungsfähigkeit ihrer Alpha-Prozessoren zu demonstrieren.

den nächsten Bus warten muss und ob es dabei regnet, eröffnen nicht nur viele digitale Einblicke in die reale Welt, sondern ermöglichen neue und optimierte Geschäftsmodelle, die vor wenigen Jahren noch undenkbar gewesen wären. Die systematische, flächige Erfassung der Umgebungsdaten – von der lokalen Straßenbelagsbeschaffenheit etwa bis zur globalen Erfassung der Wälder – und der faktischen Verhaltensdaten – von der aktuellen Insektenverbreitungen etwa bis hin zu den Gesprächen in Haushalten.

Diese noch vor wenigen Jahren unvorstellbar umfangreiche Datengrundlage zusammen mit elaborierten, sich schnell verfeinernden statistischen Auswerteverfahren erlauben es einer überschaubaren Menge von Expertenteams, welche auch über die notwendige Infrastruktur verfügen, mithilfe von Korrelationsanalysen zeitnah sehr weitreichende und spezialisierte Aussagen zu ermitteln, deren künftige gesellschaftliche Brisanz weitgehend unvorhersagbar ist. Bereits 2015 warnte die Internet Society deshalb:

> "Generally, privacy concerns are amplified by the way in which the Internet of Things expands the feasibility and reach of surveillance and tracking. Characteristics of IoT devices and the ways they are used redefine the debate about privacy issues, because they dramatically change how personal data is collected, analyzed, used, and protected."
>
> —— The Internet Sociecty [158]

Datenhoheit und ihre Durchsetzbarkeit Die sich rasch ausweitenden technischen Möglichkeiten zur Datenerhebung und netzweiten Aggregation werfen vielfältige Fragen der Datenhoheit und gesellschaftlichen Bestimmung auf: Ein Sensor des Herstellers A, der sich in einem Gerät von Hersteller B (mit Betriebssystem von C) befindet, D gehört, aber (in einer Infrastruktur) von E betrieben wird und letztlich Daten von F (oder der Allgemeinheit) erfasst, lässt die Frage unbeantwortet, wem welche Daten gehören und wer aus ihnen welchen Nutzen ziehen darf. In der Vergangenheit wurden diese Fragen oft pragmatisch von den Technologieunternehmen im Eigeninteresse entschieden: Wer Daten erfassen konnte, nutzte sie auch. Dabei entwickelten sich höchst unterschiedliche Nutzungskanäle von zentralisierter Aggregation durch die großen Plattformbetreiber über die Betriebssystemhersteller zu System- und Cloudbetreibern bis hin zu neuen Daten-Ökosystemen, welche die Hersteller von Haus- oder Industriesystem, Fahrzeugen etc. gegenwärtig aufbauen. So verfügen viele moderne Geräte über online-Anbindungen in herstellerproprietäre Cloud-Lösungen und die Fahrzeughersteller planen, ihre Neuwagen um mobile Sensoren zur Umgebungsdatenerfassung zu erweitern.

Die Europäische Union hat mit der General Data Protection Regulation GDPR (EU Regulation 2016/679)[36] die Rechte natürlicher Personen an ihren Daten sowie deren Weitergabe geregelt. Die EU ist hiermit in eine weltweit beachtete Vorleistung bei der Ausgestaltung auch des bisher Ungeregelten gegangen. Insbesondere knüpft die GDPR personenbezogene Datenverarbeitung an explizite Erlaubnistatbestände und legt eine Rechenschaftspflicht für die Verantwortlichen in der Personendatenverarbeitung fest, was als elementare Grundlage für eine Justitiabilität der Datenverwertung verstanden werden kann.

[36] `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679`

Unabhängig von Persönlichkeitsrechten bilden – auch personenungebundene – Daten einen wirtschaftlichen und gesellschaftlichen Wert, was eine andauernde öffentliche Debatte ausgelöst hat. Bei aller Vorsicht, die unserer nicht-juristischen Studie zugrunde liegen muss, scheint sich die gegenwärtige Rechtslage wie folgt zusammenfassen zu lassen: Es gibt kein originäres Eigentumsrecht an Daten, und wer im Besitz von Daten ist, kann damit erst einmal frei umgehen — wenn dem nicht gesetzliche Vorschriften oder vertragliche Vereinbarungen entgegenstehen. Datenerhebung und Datenübergänge unterliegen somit weitgehend der freien Vertragsgestaltung. Diese Ausgangslage bleibt für den öffentlichen Raum, die Natur und das nicht explizit geschützte Allgemeinwesen unvollständig, weil die Datenerhebung ohne Weiteres vertragslos möglich ist, aber dennoch aufgrund finanzieller, administrativer oder anderer faktischer Hürden oft nur wenigen zugänglich ist. Ebenfalls unbefriedigend bleibt, dass Kunden zuweilen Koppelgeschäften ausgesetzt werden, etwa wenn sie beim Kauf eines Autos gleichzeitig einer Datenerhebung zwingend zustimmen müssen.

Verschiedene Akteure schaffen hier durch ihr Handeln Fakten und – teilweise vertragsgestützte – Rechtslagen. Neben den großen Kartenerfassern Google, Apple etc., die Umgebungsdaten regelmäßig aufnehmen und ggfs. dem nationalen Rechtsraum entziehen, sind dies auch staatliche Institutionen, die z.B. in "Smart City" Projekten öffentliche Daten teilweise exklusiv zur kommerziellen Nutzung weitergeben.[37]

Vor dem Hintergrund der wachsenden wirtschaftlichen und gesellschaftlichen Bedeutung der netzbasierten Datenausbeutung, welche immer umfassender und im Zuge der Konsolidierung durch immer weniger Infrastrukturprovider stattfindet, erscheinen die Gesetzgeber gefragt, kluge, allgemeinverständliche und einfach durchsetzbare Rahmenbedingungen zu finden. Hierfür bildet ein gründliches Verständnis der Daten und ihrer Bedeutungen in den verschiedenen Branchen und Einsatzfeldern eine wichtige Voraussetzung. Für den Bereich der netzverbundenen Fahrzeuge hat das BMVI 2017 die Studie "Eigentumsordnung für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive"[38] erstellen lassen, aber zwischenzeitlich wieder aus dem Netz genommen.

Exklusivität und Informations-Asymmetrie Der Wert von Daten steigt mit mehreren Dimensionen. Aus der Perspektive ihrer Verwertung ist es einerseits erstrebenswert, möglichst umfassende Informationen über einen Zielmarkt bzw. das Umfeld künftigen datengestützten Handelns zu besitzen. Bei gleichzeitig intelligenter und fehlerfreier Auswertung können so Entscheidungen bestmöglich begründet bzw. Angebote mit höchster Zielgenauigkeit entwickelt werden. Weitergehende, in losen Kontexten gekoppelte Daten können darüber hinaus die Grundlage für subtile Korrelationsanalysen sein, welche wiederum weiterreichende Vorhersagen ermöglichen.

Der Wert dieser Daten steigt andererseits mit ihrer Exklusivität: Je weniger Akteure Zugriff auf gleichartige Informationen besitzen, desto weniger Konkurrenz muss derjenige Anbieter befürchten, welcher Dienste hierauf verwertet. Eine Konsolidierung von datengestützten Informationsdiensten führt so zunächst zu dem klassischen Mehrwert, wie er

[37] https://www.telekom.com/de/medien/medieninformationen/detail/parkplatz-finden-leicht-gemacht-smarter-parken-in-pisa-347826

[38] https://www.forschungsinformationssystem.de/servlet/is/485060/

sich im Prozess einer Monopolisierung ergibt. Informationen, über welche exklusiv verfügt wird, gewähren jedoch noch eine zusätzliche Dimension des Mehrwerts: die Informations-Asymmetrie.

Informations-Asymmetrie entsteht, wann immer zwei Verhandlungspartner über unterschiedliche, vertragsrelevante Informationsstände verfügen – etwa beim Handel eines Gebrauchtwagens, wo nur der Verkäufer über bestimmte verdeckte Mängel weiß. Im Kontext der netzbasierten, großen Daten-Ökosysteme entsteht eine strukturelle Informationsasymmetrie zwischen Systembetreibern und der restlichen Welt immer dann, wenn Daten exklusiv vom Betreiber gehalten werden und dieser sich der Exklusivität auch sicher sein kann. Die Google Suchmaschine mit einem weltweiten Marktanteil von $92,5\%$ bildet ein solches Monopol und kann sich ihrer Informations-Asymmetrie sicher sein, seit (nach Snowden) alle Anfragen transportverschlüsselt ablaufen, also vor dem Mithören durch Dritte geschützt sind.

Der Inhaber eines solchen exklusiven Informationsmonopols kann nun nicht nur als Einziger geeignete datengestützte Auswertungen durchführen, sondern er kann auch gegenüber Dritten lügen, ohne Angst vor Entdeckung haben zu müssen. Er kann Narrative prägen, die keiner Überprüfung standhalten müssen und Halbwahrheiten in Gestalt von Analyseergebnissen verbreiten, die nur scheinbar rigoros datengestützt sind, tatsächlich aber Drittinteressen folgend modifiziert oder rearrangiert wurden.

Aus gesellschaftlicher Sicht erscheinen deshalb exklusive Akkumulationen relevanter Daten in hohem Maße bedenklich. Dies gilt umso mehr, wenn Mechanismen zum Aufbruch solcher – im Internet oft globalen – Monopole nicht oder nur sehr eingeschränkt zur Verfügung stehen. Vor diesem Hintergrund sollten insbesondere die öffentlichen Handlungsverantwortlichen solchen Tendenzen zur exklusiven Datenkonsolidierung sehr konsequent entgegenwirken. Als positives Beispiel sei hier die Stadt Hamburg genannt, welche mit ihrem öffentlichen Urban Data Hub[39] alle gesammelten Daten zum freien Zugriff für alle Interessierte anbietet.

6.2.6 Gesellschaftliche Wahrnehmung

Die Relevanz von Daten ist heute weitgehend im Allgemeinwissen angekommen, wobei die Ernsthaftigkeit bei der Auseinandersetzung mit dem Thema stark mit dem Alter, dem Bildungsstand und der Region schwankt. So haben etwa nach einer PWC-Studie von 2018[40] 59% der Deutschen zwischen 30 und 39 Vertrauen in die sozialen Medien und ihren Umgang mit persönlichen Daten, wohingegen nur halb so viele der über 60-Jährigen dieses Vertrauen teilen. Die deutsche Gesellschaft erscheint in dieser Studie, welche im Kontext des Skandals um Cambridge Analytica zur vorletzten US-Wahl stattfand, deutlich gespalten: 48% der Befragten haben höchstens geringe Bedenken gegen den Weiterverkauf ihrer persönlichen Daten, ebenfalls 48% lehnen eine solche Weitergabe ab.

Daten in staatlichen Händen Traditionell waren es staatliche Organe, welche systematisch und umfassend Daten über Bürger, das eigene Land und auch Drittländer erhoben

[39] `http://www.urbandataplatform.hamburg/`

[40] `https://www.pwc.de/de/technologie-medien-und-telekommunikation/pwc-studie-vertrauen-in-medien-2018.pdf`

haben. Es ist entsprechend folgerichtig, dass Erwartungshaltungen, Mißtrauen und Kritik zuerst der staatlichen Datenerhebung entgegenschlugen. Der Staat wird auch heute als primäre Quelle für richtige, unverfälschte Informationen angesehen, seine Datenerhebung wird regelmäßig misstrauisch hinterfragt, spätestens seit der Volkszählung 1987.

Staatlich erhobene Daten wurden auch vor dem Zeitalter der digitalen Massendatenverarbeitung ausgewertet und auf verborgene Muster untersucht, z.B. in der polizeilichen Arbeit. Nassehi [159] weist zu Recht darauf hin, dass die Digitalisierung hier keine strukturellen gesellschaftlichen Veränderungen bewirkt hat. Neu sind hingegen Umfang und Intensität sowie die Geschwindigkeit der Erhebung und Verarbeitung. Zygmunt Bauman sieht in seinem einflussreichen Buch "Liquid Modernity" [160] die Geschwindigkeit (gesellschaftlicher Prozesse) als maßgeblich prägend an:

> "Once the distance passed in a unit of time came to be dependent on technology, on artificial means of transportation, all extant, inherited limits to the speed of movement could be in principle transgressed. Only the sky (or, as it transpired later, the speed of light) was now the limit, and modernity was one continuous, unstoppable and fast accelerating effort to reach it."
>
> — Zygmunt Bauman [160]

Vor allem das Internet, aber auch die Privatisierung von Telekommunikations- und Medienunternehmen haben mit ihren globalen Online-Diensten und personalisierten Plattformzugriffen neuartige Datensilos in private Hände gelegt, was die Datenhoheit der Staaten in vielen Bereichen aufgelöst oder mindestens vermindert hat.

In umfangreichen Studien des Forschungsforums Öffentliche Sicherheit Berlin wurde die staatliche Rolle bei der Datenerfassung für den Bereich Sicherheit untersucht. Sicherheit bleibt gestützt auf das Gewaltmonopol des Staates und "gilt als letzte Bastion effektiver Staatlichkeit" [161]. In einer ausführlichen empirischen Analyse zeigen Krasmann et al. [162] ein differenziertes Vertrauensbild für die deutsche Bevölkerung in 2009. Während sich eine breite Mehrheit von mehr als 70% für biometrische Kontrollen, Antiterror-Dateien und online-Lichtbildüberprüfungen ausspricht, akzeptieren nur 50% den Zugriff auf Bankdaten. Online-Durchsuchungen (55%) und Vorratsdatenspeicherung (70%) werden mehrheitlich abgelehnt.

Dagegen werden Abwehrmaßnahmen gegen staatliche Datenerhebungen nur von Minderheiten erwogen: Ein Drittel der Befragten in [162] hat sich zwar schon mindestens einmal über die Datenschutzrichtlinien einer Behörde informiert, 23,3% haben sich schon einmal geweigert, einer Behörde bestimmte persönliche Daten oder Informationen zu geben, fokussierteres Abwehrverhalten wie eine An-/Ummeldeverweigerung, Nutzung von Anonymisierungsdiensten oder Internet-Cafes zur Identitätsverschleierung wurden aber von weniger als 10% der Teilnehmer bestätigt.

Ganz allgemein haben die deutschen Bürger ein eher differenziertes Verhältnis zu staatlichen Institutionen und deren Datenerhebungen im Einzelfall, so dass sich ein klares summarisches Bild nicht zeichnen lässt. Während das Vertrauen in Polizei und Gerichte sehr hoch ist, misstrauen etwa 40% der Bundesregierung und dem Bundestag. Als Beispiel differenzierter Wahrnehmung zur Datenerhebung kann aktuell die Corona WarnApp dienen:

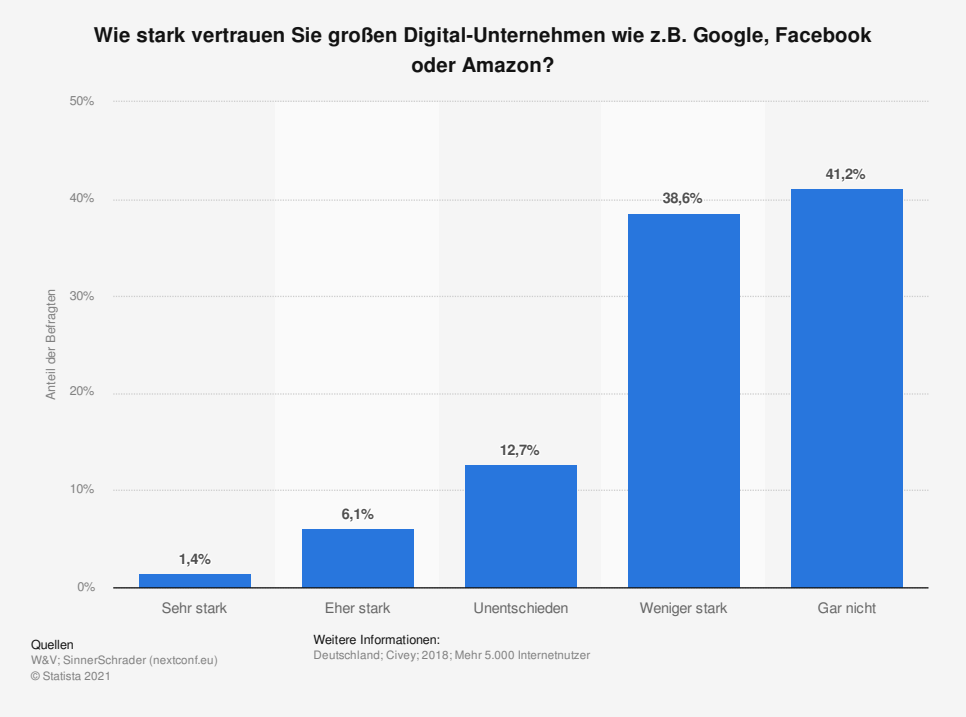


Abbildung 6.29: Vertrauen in große Digitalunternehmen in Deutschland (Quelle: Statista)

Etwa 30% der Deutschen nutzen sie, weitere 10% sind gleichfalls positiv eingestellt, aber ebenfalls 40% lehnen sie ab. Neben allgemeinem Vertrauen in die Datenverarbeitung ist das Antwortverhalten auch eng verknüpft mit Einschätzungen der Qualität und der Nützlichkeit, technischer Passfähigkeit (aktuelles SmartPhone) und allgemeiner technischer Vorbildung. Eine Bewertung solcher Umfragedaten muss deshalb fallweise differenziert vorgenommen werden.

Daten in privaten Händen Große Online-Plattformanbieter aus den Bereichen der Social Media, des Infotainments und der digitalen Gatekeeper, aber auch Systemhersteller, Datenhändler und Analytiker verfügen heute über Personendatenbestände, die an Tiefe, Breite oder Aktualität die staatlichen Daten nicht nur erheblich übertreffen, sondern oft auch international erhoben werden und sich so dem staatlichen Vergleich per se entziehen. Nutzer stimmen diesen Datenerhebungen teilweise versteckt in allgemeinen Geschäftsbedingungen zu, teilweise aus Bequemlichkeit oder weil die Nutzung vieler Dienste eine Zustimmung zur Datenerhebung erzwingt.

Das Vertrauen in private Firmen in Deutschland ist signifikant geringer als in staatliche Institutionen. Der überwiegende Teil der Deutschen (72%) informiert sich über öffentlich-rechtliche Medien und vertraut diesen auch, stellen PWC in ihrer Studie[40] fest, wohingegen weniger als die Hälfte den privaten Medien und weniger als 20% den Online-Plattformen vertrauen. Interessanterweise sind nur 48% der Deutschen besorgt bezüglich der Weitergabe ihrer Daten – das Misstrauen richtet sich offenbar stärker gegen Fehlinformationen als gegen Datenmissbrauch.

Das Vertrauen in die großen Digitalunternehmen ist dabei in Deutschland besonders schwach ausgeprägt (vgl. Abbildung 6.29). Weniger als 10% der Deutschen vertrauten

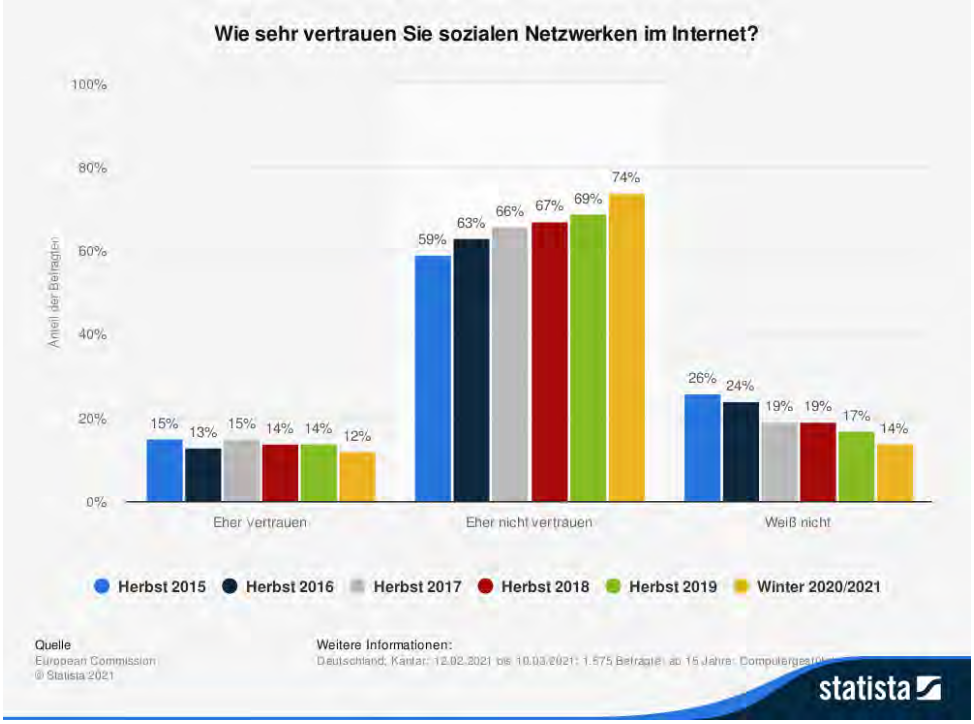


Abbildung 6.30: Vertrauen in soziale Netzwerke in Deutschland

Google und Co. im Jahr 2018 stark. Bezüglich der sozialen Netzwerke hat das Misstrauen in den vergangenen sechs Jahren sogar um gut 20% zugenommen (vgl. Abbildung 6.30). Bemerkenswert ist auch hier, dass sich dieses Misstrauen kaum explizit in konkreten Handlungen auf den Plattformen (Profil löschen, Datenschutzeinstellungen ändern) niederschlägt, wie PWC herausgefunden hat. Vielmehr gibt eine relative Mehrheit an, nur sparsam Daten preiszugeben und sieht darüber hinaus den Gesetzgeber gefordert, regulierend gegenzusteuern.

Ebenfalls auf der kritischen Seite zeigen sich die Deutschen im europäischen Vergleich bezüglich vertraulicher Daten in Online-Shops, wie Abbildung 6.31 für das Jahr 2015 veranschaulicht. Hier zeigen die angelsächsischen Länder ein um 50% höheres Vertrauen, was aber auch auf eine frühere und intensivere Nutzung der mehrheitlich im englischsprachigen Raum begonnenen Online-Shops zurückgeführt werden könnte.

Abbildung 6.32 stellt das differenzierte Verhalten bei der Vertrauensbildung in Deutschland dar: Mehrheitlich sorgen sich die Kunden um ihre Kontodaten und bewerten Shops, die abgesicherte Bezahlmechanismen wie PayPal verwenden, entsprechend höher. Neben persönlicher und öffentlicher Reputation spielen unabhängige Testberichte eine große Rolle. Instanzen wie Stiftung Warentest und auch die Verbraucherzentralen genießen in Deutschland eine herausragende Vertrauensstellung, was in unterschiedlichen Befragungen regelmäßig sichtbar wird.

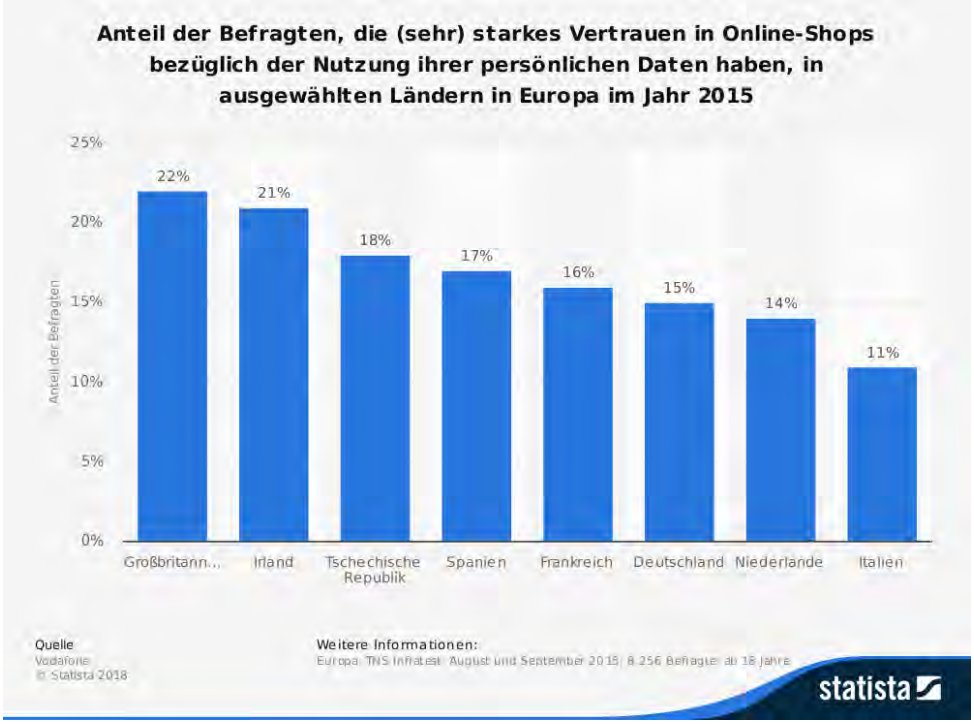


Abbildung 6.31: Vertrauen in der Nutzung privater Daten durch Online-Shops

Abbildung 6.32: Vertrauensbildung gegenüber Online-Shops in Deutschland

6.3 Vor- und Nachteile der Konsolidierung

In den vorangegangenen Abschnitten dieses Kapitels haben wir diskutiert, wie die Konsolidierung Großsysteme im Internet heranwachsen lässt, die Infrastrukturen, technische Funktionen und Informationen zentralisieren und teilweise monopolisieren. Wir haben wirtschaftliche und gesellschaftliche Entwicklungen und Konsequenzen dargelegt und an Fallstudien erläutert.

In diesem Abschnitt wollen wir nun die Kernaspekte der Konsolidierung im Internet aufgreifen und ihre Vor- und Nachteile summarisch gegenüberstellen.

6.3.1 Große Infrastrukturen

Vorteile

Versorgungsfähigkeit Der Auf- und Ausbau sowie der Unterhalt leistungsfähiger Netzinfrastrukturen wie etwa aktuelle Funknetze, große Unterseekabel oder Zugangs- und Backbone-Kabelinfrastrukturen erfordern erhebliche Investitionskraft und umfassende Kompetenzen. Diese Maßnahmen können naturgemäß von Großunternehmen leichter und schneller umgesetzt werden als von regionalen Akteuren.

Innovationspotential Die Einführung neuer Technologien und Protokolle (z.B. IPv6, QUIC) kann von sehr großen Akteuren wirksam initiiert bzw. beschleunigt werden, wohingegen viele, kleine Firmen schwerfälliger zu koordinieren sind.

Resilienz Große, professionell errichtete Infrastrukturen weisen i.d.R. höhere *interne* Redundanzen auf, welche im Störungsfall schnell aktiviert werden können.

Nachteile

Wettbewerb in der Fläche Die freie Anbieterwahl mit Konkurrenz in der Fläche hat sich in Deutschland (z.B. im Gegensatz zu den USA) als Hauptgrund für eine ausgeglichene Versorgung mit Netzzugängen erwiesen. Regionale Konsolidierungen können zu starken wirtschaftlichen Benachteiligungen, sozialen Ausgrenzungen bis hin zu gesellschaftlichen Verwerfungen führen.

Wettbewerb auf der Dienstebene Horizontal integrierende Netze beinhalten unterschiedliche Dienstebenen und erfordern Wettbewerb in jeder Ebene. Beispiele hierfür sind (submarine) Transitkabel, Internet Transitbeförderungen, aber auch der Einsatz von Transportprotokollen, welcher zu deutlichen Qualitätsverschiebungen zwischen Nutzergruppen führen kann, wie das Beispiel Google QUIC (BBR) vorgeführt hat.

Regionalität Oft können Synergien in der Region genutzt werden, welche zu einer preiswerteren Versorgung oder verbessertem Service führen. Beispiele hierfür sind Netze in Metropolregionen wie NetCologne, das Berliner Wissenschaftsnetz BRAIN oder

wilhelm.tel in Norderstedt (und Hamburg). Insbesondere gelten Regionalitätsvorteile für IXPs. Globale Akteure und zentralistische Großinfrastrukturen wie die überregionalen IXPs vergeben diese Synergien.

Resilienz Große, monolithische Systeme weisen oft Angriffspunkte in ihren zentralen Strukturen auf, welche bei konsolidierten Infrastrukturen große Auswirkungen haben. Als Beispiele hierfür sind kaskadierende Fehler in großen Infrastrukturen bekannt geworden, aber auch die massive Störung des Routings bei Tier-1 Providern oder der Location Registers bei Mobiltelefon-Providern. Sehr gleichmäßig eingesetzte Systemkomponenten können ebenfalls die Wirksamkeit von Angriffen erhöhen, wie etwa der TR-069-Bug bei den von der Telekom massiv eingesetzten Homegateways.

6.3.2 Technische Großsysteme

Vorteile

Skalierbarkeit Sehr große Systeme wie z.B. Cloud- und CDN-Serverinfrastrukturen erlauben es, Dienste mit einer entsprechend hohen Skalierbarkeit zu betreiben. Die Großsysteme ermöglichen ebenfalls die Realisierung von Informations-Großsystemen wie etwa den Google Such-Index etc. Beides ist ohne eine sehr große Systeminfrastruktur nicht möglich.

Effizienz Zentral gesteuerte Großsysteme können in der Errichtung und dem Betrieb nicht nur von der "Economy of Scale" profitieren, sondern auch dedizierte Sondervorteile ausnutzen. So können sehr große Cloud-Infrastrukturen im Betrieb in erheblichem Maße reskalieren und ihre Energiebedarfe an den aktuellen Betrieb und ggfs. die lokale Verfügbarkeit anpassen. CDNs profitieren von der Cache-Steuerung in *einer* Infrastruktur, die sehr viele Nutzer bedient.

Resilienz Sehr große Systeme verfügen naturgemäß über sehr umfangreiche Ressourcen, deren Last häufig auch dynamisch steuerbar ist, z.B. durch Load Sharing, Anycasting oder adaptives Routing. Die Systeme verfügen zwangsläufig auch über Redundanzen und Reserven. Damit wird es überproportional schwer, die Systeme z.B. durch DDoS wirksam anzugreifen.

Nachteile

Marktmonopolisierung Serverinfrastrukturen wachsen erfolgreich mit ihren Marktanteilen, so dass sehr große Systeme sehr große Marktanteile bedeuten. Für Konkurrenzunternehmen ist es dagegen wirtschaftlich schwer, sehr große Infrastrukturen zu replizieren und so den Zugang zu großen Kunden und Anwendungen zu gewinnen. Entsprechend kann die Konsolidierung im Bereich der Großsysteme als ein wesentlicher Schritt zur Monopolisierung in dem "Winner-takes-all" Markt verstanden werden.

Offene Innovationen und Standards Soweit Systeme homogen und geschlossen betrieben werden, etwa in konsolidierten Data Centers, sind offene Standards und mit der Fachwelt geteilte Innovationen nicht notwendig. Ein proprietäres Vorgehen von Großbetreibern beinhaltet so die Gefahr, dass Innovationen weniger zum Allgemeingut werden oder die Entwicklung offener Standards sogar torpediert wird, wie es z.B. teilweise bei der IETF Gruppe CDNI geschehen ist.

Resilienz Zentral betriebene Großsysteme sind ebenfalls anfällig für Betreiberfehler. Darüber hinaus weisen sie oft zentrale Schwachstellen auf, deren Angriff mit gewöhnlichen Ressourcen und Techniken möglich ist – z.B. der Angriff auf DynDNS mithilfe der Mirai Malware, welcher sich auf Großsysteme etwa von Amazon auswirkte. In beiden Fällen ist die Wirkung der Angriffe ungleich höher als bei pluralistischen Systemen mittlerer Größe.

6.3.3 Informations-Großsysteme

Vorteile

Anwendungslogik Im Internet sind Informationssysteme entstanden, deren Anwendungslogik inhärent auf Großsysteme gebaut ist; Suchmaschinen, welche einen möglichst vollständigen, aktuellen Index erfordern, bilden hier das Grundbeispiel. Diese Systeme werden nur sinnvoll dadurch nutzbar, dass sie sehr große Informationsräume überdecken.

Einheitlicher Zugang Insbesondere für technisch wenig erfahrene Anwender ist es einfacher und komfortabler, auf Informationen durch ein einheitliches Userinterface zuzugreifen. So ist es z.B. inzwischen üblich, auf die Fahrpläne des öffentlichen Nahverkehrs durch Google und nicht durch die jeweiligen lokalen Zugangsplattformen zuzugreifen. Der einheitliche Zugriff schließt oft Sprachlokalisierungen ein.

Informationstiefe Die Verbindung unterschiedlicher, orthogonaler Datenräume ermöglicht über statistische Korrelationsanalysen das Erkennen verdeckter Muster und verborgener Zusammenhänge. Hierdurch können Informationen nutzbar gemacht werden, die anderweitig nicht zur Verfügung stünden.

Nachteile

Informationsintegrität Informationsmonopole entziehen sich häufig der kritischen öffentlichen Überprüfung als Konsequenz der Informationsasymmetrie. So bleibt es für die Anwender und oft auch neutrale (staatliche) Instanzen unentscheidbar, ob die dargebotenen Informationen richtig und unverfälscht sind oder ob im Interesse des Anbieters oder Dritter Manipulationen vorgenommen wurden.

Privatsphärenschutz Der individuelle Gebrauch von Informationen, also z.B. Suchwörter, Aufrufe von Plattformangeboten, die Nutzung von Dialogdiensten wie Alexa o.ä.

kann umfangreiche persönliche Daten transportieren, welche über Fingerprinting-Techniken individuellen Nutzern zugeordnet werden können. Dies ist praktisch kaum zu kontrollieren und mit nationalem Recht schwer fassbar.

Gesellschaftliche Abhängigkeit Informationen und der omnipräsente Zugriff hierauf bilden inzwischen wichtige Funktionselemente der Gesellschaft. Dies gilt bereits für den Google Suchdienst, aber auch für viele spezialisierte Dienste diverser Anwendungsdomänen. Befinden sich diese Informationen und Dienste im exklusiven Besitz monopolartiger Dienstleister, so geraten Branchen, Wirtschaftsräume und ganze Gesellschaften in eine Abhängigkeit, die sie eventuell erpressbar macht.

6.3.4 Kommunikations-Großsysteme

Vorteile

Adaptivität Monolithische Kommunikationssysteme können schnell und ohne auf Interoperabilität Rücksicht nehmen zu müssen Anwenderanforderungen abbilden und sich aktuellen Nutzungstrends anpassen. Dies gilt insbesondere für die oft komplizierte Einbindung von diversen Medienformaten und damit verbundenen Kompatibilitätsproblemen.

Reaktivität Für zentralistisch organisierte Kommunikationssysteme sind aufwändige föderative Prozeduren etwa zur Authentifizierung verzichtbar. Sie können deshalb Kommunikationsabläufe oft schneller abwickeln und bleiben in ihren Nutzeroberflächen dadurch reaktiver.

Rohlfs' Effekt Konsolidierte Kommunikationssysteme profitieren von dem Skaleneffekt vieler Teilnehmer: Wer das System nutzt, kann viele Andere erreichen. Dieser Vorteil ist zwar auch mit offenen Standards erreichbar, erfordert aber Abstimmungsaufwand und oft höhere Anwendungskomplexität.

Nachteile

Privatsphärenschutz Persönliche Kommunikation erfordert den Schutz der Privatsphäre, welcher aber kaum sichergestellt werden kann, wenn Kommunikation über die Server eines proprietären Providers abgewickelt wird. Neben den ausgetauschten Inhalten sind auch die Kommunikationsbeziehungen zwischen den Teilnehmern schützenswert, welche vor dem Betreiber nicht verborgen werden können.

Pluralität und Standards Proprietäre Kommunikationsdienste wie WhatsApp oder Skype erzwingen die Nutzung herstellergebundener Software und nehmen den Anwendern die Wahl der Werkzeuge. Darüber hinaus behindern sie die Verbreitung von offenen Standards wie SIP oder XMPP, welche analoge Funktionalitäten in pluraler Weise ermöglichen.

Soziale Segmentierung Proprietäre Kommunikationsanwendungen schließen Nutzer anderer Anwendungen aus. Die Verbreitung dieser Anwendungen tendiert dabei dazu, sozialen oder territorialen Gruppen zu folgen. So ist der Gebrauch von Chat-Anwendungen inzwischen sehr stark segmentiert, was zur Folge hat, dass unterschiedliche gesellschaftliche Kreise oder Nutzer aus verschiedenen Ländern miteinander nicht mehr problemlos Kommunikationen initiieren können.

Resilienz Zentrale Kommunikationsplattformen beinhalten kritische Kernfunktionalitäten wie die Authentifizierung oder Teilnehmerlokalisierung, welche gezielt angegriffen werden können. Ein Ausfall dieser Funktionen bedeutet oft den Zusammenbruch des ganzen Dienstes. Dezentral betriebene Kommunikationsinfrastrukturen sind dagegen deutlich robuster gegen Totalausfälle.

6.3.5 Konsolidierung über die Handlungsfelder

Vorteile

Funktionalität Die konsolidierte Bereitstellung verschiedener Dienste, Infrastrukturen, Software, Systeme und Plattformen, wie ihn die großen Anbieter durchführen, ermöglicht zum einen eine abgestimmte Leistungsstruktur: Transportkapazitäten können passend zu Dienstanforderungen bereitgestellt werden und Infrastrukturdienste können die Anwendungen zuverlässig unterstützen. Darüber hinaus können einzelne Funktionen – etwa die Authentifizierung oder die Personenprofile – geteilt werden und machen so die Nutzung des Portfolios einfacher.

Strategische Entwicklung Leistungsanforderungen der Anwendungen können gemeinsam mit den Infrastrukturen und Basisdiensten entwickelt werden. So können Netzwerkinfrastrukturen im Gleichklang mit neuen Leistungsanforderungen, Cache-Populationen mit Software-Updates und Sicherheitslösungen mit Geschäftszielen entstehen. Eine strategisch abgestimmte Entwicklungsplanung kann so die Kundenzufriedenheit und gleichermaßen den Geschäftserfolg erhöhen.

Nachteile

Marktbeherrschung Wenn einzelne Akteure die wesentlichen Komponenten von der Basisinfrastruktur über die Systeme bis hin zu Anwendungssoftware und Anwendungsdaten beherrschen, entsteht eine Machtfülle am Markt, für welche kaum mehr entscheidbar ist, was technisch/inhaltlich noch sinnvoll und was bereits Missbrauch ist. Frühere Wettbewerbsverfahren gegen Microsoft zum Internet Explorer haben deshalb der Integration von Systemen, Anwendungen und Infrastrukturen enge Grenzen gesetzt.

Privatsphärenschutz Ein monolithischer Anbieter von Inhalten, Anwendungen, Systemen und Infrastruktur ist in der Lage, quasi jede Handlung seiner Kunden zu verfolgen und auszuwerten. Möglichkeiten, dieses Verhalten zu dokumentieren oder zu begrenzen, sind für die Kunden oder Dritte nur sehr begrenzt vorhanden.

Neutralität Ein Infrastrukturprovider, der in wesentlichen Geschäftsteilen sowohl seine eigenen Anwendungen und Dienste als auch Drittangebote unterstützt, befindet sich per se in dem Konflikt, die Dienste im eigenen Geschäftsinteresse zu bevorzugen oder durch Fairness seine Reputation zu stützen. Je wirkmächtiger Anwendungen, Infrastrukturen und Systeme verwoben sind, umso leichter wird es für den Akteur, diskriminierendes Verhalten gegen Dritte zu verbergen.

Kapitel 7

Ausblick auf zu erwartende Entwicklungen

In den vorangegangenen Kapiteln wurden auf der Basis umfangreicher Messungen und Analysen sowie empirischer Studien die vielfältigen Aspekte der Konsolidierung detailliert beleuchtet. Dieses Kapitel soll nun erwartete zentrale Entwicklungstrends in Gestalt von ausgewählten Thesen zusammenstellen, welche den Bezug zu den vorangehenden Darstellungen herstellen.

7.1 Entwicklungen der Protokolle und Dienste

These: Die IETF erarbeitet Protokolle, die eine Konsolidierung im Internet erschweren und die Offenheit der Internet-Infrastruktur gewahrleisten.

Wir haben gezeigt, dass führende Akteure im Markt erhebliche Änderungen in der Internet-Infrastruktur vornehmen können, ohne die Protokolle in der IETF zu standardisieren, wie z.B. bei QUIC offenbar wurde (vgl. Abschnitt 5.1.1). Sowohl die IETF als auch die IRTF sind sich der Probleme durch die zunehmende Konsolidierung bewusst und haben bereits mit der DINRG das Thema aktiv aufgegriffen.
Wir erwarten, dass künftige Standardisierungen der IETF sich in zentralen Bereichen des Internets aktiv gegen die Konsolidierungstendenzen stellen werden, um die Offenheit und Betreiberunabhängigkeit des Internet zu gewährleisten. Dabei sollten auch neue, kooperative Betreibermodelle für eine dezentralisierte Internet-Infrastruktur entstehen.

These: Neue Anwendungsprotokolle lassen authentifizierte und verschlusselte Daten frei in Caches der Provider replizierbar werden und brechen das geschlossene CDN-Modell auf.

Content Object Security auf der Transport Protokollschicht, wie sie etwa CoAP/ OSCORE oder informationszentrische Netze beinhalten, machen Datenauthentifizierung und -verschlüsselung transportunabhängig. Sie erlauben die freie Replikation von Inhalten zwischen verteilten Caches (vgl. Abschnitt 5.2.2, Abschnitt 5.2.3). Eine effiziente Cache-Infrastruktur, die nicht an die Transport-Endpunkte geknüpft ist, wird künftig von (Edge-) Providern zur Verbesserung ihrer Dienstqualität trans-

parent eingesetzt und macht den Betrieb geschlossener CDNs schrittweise überflüssig.

These: Verborgen hinter herstellerspezifischen APIs werden Internet Protokolle und Standarddienste schrittweise gegen proprietare Losungen aus getauscht.

Hersteller großer System- und Softwareplattformen kapseln bereits heute Zugriffsfunktionen auf Internet-Infrastruktur und -Anwendungen hinter eigenen, abstrakten APIs (vgl. Abschnitt 6.1.3), so dass Internet-Protokolle und Standarddienste ohne Änderung der Anwendungsprogramme austauschbar werden. Hierdurch können herstellerbezogene Vorteile zu Lasten der allgemeinen Internet-Nutzer weitgehend unbemerkt etabliert werden, wie am Beispiel Google-QUIC (vgl. Abschnitt 5.1.1) sichtbar wurde.
Eine zunehmende schichtenübergreifende Konsolidierung und Dominanz einzelner Betreiber wird die Möglichkeiten und Anreize erhöhen, Standarddienste und -funktionen zugunsten der eigenen Geschäftsmodelle auszutauschen, wobei Gegenmaßnahmen durch die benachteiligten Nutzergruppen ebenfalls wahrscheinlich sind. Es besteht die Gefahr, dass das Internet-Ökosystem fragmentiert und Interoperabilität abnimmt.

7.2 Entwicklungen der Deployment-Modelle

These: Großsysteme und professionelle, aber monolithische Infrastrukturen machen Infrastrukturausfalle seltener, aber schwerwiegender.

Professionell betriebene Großsysteme, aber auch globale (Anycast-addressierbare) Infrastrukturen haben sich im Betrieb als zuverlässiger und als gegen Angriffe robuster erwiesen. Ausfälle dieser großen Infrastrukturen mit internationalen Abhängigkeiten zeigen jedoch auch große Wirkungen (vgl. die realen Ausfälle [13, 66, 84] sowie Abschnitt 3.4).
Es ist insofern vorauszusehen, dass eine sich weiter konsolidierende Internet-Infrastruktur die Tendenz zu wenigen, aber sehr weitreichenden Ausfällen nach sich ziehen wird.

These: Rechen- und Speicherkapazitaten werden zunehmend am Rand des Internets verfugbar und Anwendungsdomanen zugeordnet.

Sehr niedrige Latenzanforderungen z.B. beim autonomen Fahren oder in industriellen Anfwendungen sowie hohe Datenbedarfe bedingen den Aufbau von Compute- und Speicherressourcen am Internet Edge (vgl. Abschnitt 5.4). Diese Infrastruk-

tur wird – teilweise virtualisiert als *Edge Clouds* – Anwendungsdomänen (in sog. Network Slices) zugeordnet. (Abschnitt 6.1.2).
Diese Entwicklung wird sich absehbar fortsetzen, da es aus technischen Gründen keine Einsatzalternativen gibt. Hierdurch werden die regionalen und nationalen Zugangsprovider gegenüber den globalen Akteuren gestärkt, wobei unklar bleibt, wer die Hoheit über das sogenannte Edge-Cloud-Deployment letztlich erhalten wird.

These: Die rasant wachsende Verbreitung von Sensor- und Aktorlosungen im Internet der Dinge wird zunehmend von großen Cloud-Anbietern und ihrem Technologie-Portfolie gesteuert. Diese IoT-Losungen nehmen dabei eine zunehmend kritische Rolle in der Internet-Sicherheit und dem Datenschutz ein.

Die IoT-Lösungen und die notwendige Zugangsinfrastruktur entwickeln sich überproportional stark (vgl. Abschnitt 6.1.2). Hyperscaler wie Amazon AWS und Microsoft Azure dominieren bereits den Markt, während sie integrierte IoT- und Edge-Cloud-Lösungen im Markt verstärkt verbreiten (s. (Abschnitt 5.2.2)). Komplementär wachsen die Bedrohungen auf die Internet-Infrastruktur durch Millionen schlecht gesicherter Kleinstgeräte mit veralteten Software-Ständen (s. die realen Ausfälle [84, 83] und Abschnitt 5.5.1) und der Schutzgrad der Privatsphäre von mit Sensorik ausgestatteten Personen und Haushalte wird immer schwerer zu bewerten (Abschnitt 6.2.5).
Die Verbreitung neuer Sensoren und Aktoren sowie die kontinuierlich zunehmende Vernetzung bestehender Systeme kann als unaufhaltsam vorausgesetzt werden. Dabei ist zu erwarten, dass sich viele Hersteller und Betreiber, etwa der Heimgeräte- oder Automobilindustrie, aber auch von profesionellen Produktions-, Überwachungs- und Sicherheitslösungen an den vorgefertigten Lösungen der großen Cloud-Provider orientieren. Damit werden die Hyperscaler Teil der technischen Lösung, des Betriebs und der Datenverarbeitung von sehr großen, weite Gesellschaftsbereiche durchdringenden IoT Systemlösungen.

7.3 Erwartete Topologische Anpassungen

These: Die Globalisierungstrends der großen IXPs lassen diese wirtschaftlich und technisch anfalliger werden.

Verteilte IXPs, die teilweise globale Transitaufgaben übernehmen, müssen risikobehaftete Kostenbindungen im Infrastrukturbereich eingehen (vgl. Abschnitt 6.1.1). Gleichzeitig steigt ihre technische Komplexität erheblich, was zu erhöhter technischer Störungsanfälligkeit führt (vgl. die realen Ausfälle [5, 22, 37, 67, 57] sowie den Abschnitt 3.5).

These: Die wachsende Monopolisierung wichtiger Transit-Kabelverbindungen hat das Potential, schwerwiegende wirtschaftliche Veranderungen und Konflikte zu bewirken.

Die Internet Hypergiants erwerben stark wachsende Weltmarktanteile an den internationalen Transit-Kabeln (vgl. Abschnitt 6.1.1), was ihre dominante Rolle im Betrieb der Internet-Infrastruktur weiter verstärkt. Hierdurch geraten die traditionellen Telekommunikationsunternehmen in eine Sandwichposition gegenüber Unternehmen, die sowohl die physische Infrastruktur als auch die Nutzung also die Inhalte des Internets dominieren. Ausfälle internationaler Kabelverbindungen z.B. als Folge wirtschafltlicher Dispute können erhebliche Auswirkungen auf den Transitverkehr haben (s. Abschnitte 3.2 und 4).
Wir erwarten größere Marktveränderungen in den kommenden Jahren. Der Ausgang dieser Verschiebungen wird allerdings von vielen Faktoren abhängen, u.a. von der Entwicklung der Nachfrage und vom Verhalten der Marktregulierer.

7.4 Potentielle Regulatorische Maßnahmen

These: Die universelle Breitbandversorgung sowohl in der Flache als auch in allen sozialen Gesellschaftsschichten hat ein hohes nationales Entwicklungs potential und wird deshalb verstarkt vorangetrieben.

Sowohl die wirtschaftlich-technische Entwicklung im ländlichen Raum, als auch die Realwirtschaft, als auch die persönliche Bildungsentwicklung von Kindern und Jugendlichen ist wesentlich mit der einfachen und preiswerten Verfügbarkeit von Breitband-Internetanschlüssen verbunden (vgl. Abschnitte 6.1.2, 6.1.5 und 6.2.1).
Es ist deshalb im gemeinsamen Interesse sowohl der regionalen wie der nationalen Entscheidungsträger, die Netzversorgung voranzutreiben, um eine leistungsfähige Netzinfrastruktur in der Fläche zu entwickeln.

These: Die dienstubergreifende Konsolidierung von Internet-Grundfunktionen und Anwendungen in den Handen weniger Akteure fuhrt die Informationsgesellschaft in eine praktisch und kartellrechtlich bedenktliche Abhangigkeit.

Wenige große Anwendungsprovider betreiben (i) quasi monopolartig Alltagsanwendungen und (ii) gleichzeitig ein vertikal integriertes Portfolio von Internet-Basisdiensten (vgl. Abschnitt 6.1.3). Zusammen betrachtet finden wir bereits heute große Bereiche des Internet-Betriebs in den Händen einer kleinen Gruppe unregulierter Unternehmen.
Eine weitere Fortführung des schichtenübergreifenden Konsolidierungsprozesses wird diese Schieflage weiter verschärfen, so daß die Internet-Infrastruktur in kritischer Weise von einzelnen oder wenigen sehr wenigen Akteuren abhängig wird. Aus dieser Entwicklung entsteht ein Regulationsbedarf ähnlich wie bei der Auflö-

sung der staatlichen Telekommunikationsmonopole.

7.5 Gesellschaftliche Reaktionen und Prozesse

These: Anwender gewohnen sich an ein stabilisiertes Anwendungsportfolio der konsolidierten Anbieter und verlieren an kritischer Distanz.

Anwender nehmen dominierende, proprietäre Anwendungen zunehmend als Standarddienste wahr und "vergessen" die zugrundeliegenden Geschäftsmodelle der Anbieter (vgl. Abschnitte 6.2.5 und 6.2.6).
Die Konsolidierung der Anwendungsanbieter führt zu einer abnehmenden Entwicklungsdynamik und einer sich verfestigenden Anwendungslandschaft. Konsumenten verlieren das Gefühl für Alternativen und nutzen die Dienste mehr und mehr distanzlos.

These: Der Einfluss sozialer Medien und Content-Plattformen kann infolge ihrer Verbreitung und steuerbaren Kontextualisierung so groß werden, dass eine staatliche (Medien-)Aufsicht unumganglich wird.

Die Verknüpfung von Inhalten in (sozialen) Plattformen beeinflusst möglicherweise viele Konsumenten stark und wirkt prägend auf persönliche Perspektiven (siehe Abschnitt 6.2.3). Die gleichzeitige Dominanz einzelner Großsysteme und Anbieter (vgl. Abschnitt 6.1.3) eröffnet den Wenigen dann ein bisher unbekanntes Manipulationspotential.

These: Die potentiell breite Manipulationswirkung durch Internet-Anwendungsplattformen macht diese fur staatlichen Mißbrauch attraktiv.

Angesichts der messbaren Erfolge in der Meinungsmanipulation durch (soziale) Internet-Plattformen (vgl. Abschnitt 6.2.3) liegt es nahe, dass meinungsbildende Interessen von (inländischen wie ausländischen) Regierungsorganisationen mittels staatlich gelenktem Mißbrauch bzw. Zensur forciert werden.

Kapitel 8

Zusammenfassung

Die Internet-Infrastruktur, ihre Dienste und Anwendungen sind das Rückgrat für die Digitalisierung in Staat, Wirtschaft und Gesellschaft. Obgleich die zugrundeliegenden Prinzipien und Technologien erst in den letzten 30 Jahren eine massive Verbreitung fanden, erleben wir momentan einen erheblichen Paradigmenwechsel weg von Offenheit und Dezentralisierung hin zu Bestrebungen nach Geschlossenheit und Konsolidierung. Das Internet, das Innovationen und Teilhabe für kleine und große, etablierte und nicht etablierte Akteure ermöglicht, hat nicht nur global agierende, sektorübergreifende Unternehmen mit enormer Marktmacht hervorgebracht, sondern auch Staaten Möglichkeiten einer bisher nicht vorhandenen Überwachung bereitgestellt.

In dieser Studie haben wir die Verletzlichkeit der Internet-Infrastruktur basierend auf realen und fiktiven Vorkommnissen beleuchtet, Abhängigkeiten der regionalen Internet-Infrastruktur von internationalen Kabelverbindungen analysiert, aktuelle Änderungen in der Internet-Infrastruktur diskutiert und gesellschaftliche und wirtschaftliche Konsequenzen aufgezeigt.

Die in dieser Studie gewonnenen Messergebnisse sind interaktiv auf folgender Webseite abrufbar: `https://zwiback.leitwert.net/`

Kapitel 2 stellte weitreichende Internet-Störungen der Vergangenheit vor. 107 reale Vorfälle wurden (*i*) in einem Vorfallskatalog kategorisiert und (*ii*) fünf im Detail unter Anwendung zusätzlicher Messungen und Recherchen post-mortem analysiert.

1. Isolierte, technisch bedingte Ausfälle weisen eine hohe Eintrittserwartung[1] auf. Die daraus resultierenden Schäden sind jedoch meist begrenzt.

2. Unerwünschte Verkehrsumleitungen bergen ein hohes Schadenspotential, treten aber in der Praxis weniger häufig auf.

3. Das größte Risiko im Internet geht sowohl in Bezug auf die Eintrittserwartung als auch auf mögliche Schäden von gezielten Angriffen aus.

Kapitel 3 stellte vier fiktive Ausfallszenien vor. Basierend auf realen Daten wurde (*i*) der Totalausfall des Überseekabels TAT-14, (*ii*) der Ausfall aller Transitverbindungen

[1] Dies bezeichnet die erwartete Wahrscheinlich für den Eintritt eines Ereignisses der genannten Fehlerkategorie.

durch Russland, (*iii*) der DDoS-Angriff auf einen populären DNS-Dienstleister und (*iv*) der Totalausfall des Internetaustauschpunkts DE-CIX (Frankfurt) untersucht. Die einzelne Ausfälle wurden durch konkrete Ausfallszenarien untermauert.

1. Alle vier Ausfälle sind durch die Betroffenen mitigierbar.
2. Die Mitigation der Störung verlangt u.U. eine sehr hohe fachliche Kompetenz.
3. Ein schichtenübergreifendes Verständnis hilft auch Endnutzern mit globalen Vorfällen umzugehen.
4. Der Ausfall des DE-CIX schränkt die Erreichbarkeit nicht ein, verlangt aber höhere Transitkapazitäten und führt zu höheren Latenzen.

Kapitel 4 stellte Abhängigkeiten von internationalen Kabelverbindungen vor. Bestandteile der Untersuchungen waren (*i*) eine Charakterisierung der Abhängigkeiten für das deutsche Internet und (*ii*) eine Bewertung zur Verbesserung der Widerstandsfähigkeit auf Basis der realen Vorfälle und zusätzlicher empirischer Messungen.

1. Aus den technisch und ökonomisch gegensätzlichen Ausrichtungen der Deutschen Telekom (ISP) und des DE-CIX (IXP) ergeben sich vorteilhafte Synergien für den Internet-Standort Deutschland bzgl. Dienstgüte und Ausfallsicherheit.
2. Infrastrukturelle Risiken ergeben sich aus den grundlegenden Veränderungen des weltweiten Internet-Marktes.
3. Populäre Content Delivery Networks und Over-The-Top-Anbieter verfügen über einen überraschend hohen Anteil an internationalen Kabelverbindungen.
4. Die Sicherstellung weltweiter Konnektivität tritt zunehmend hinter die prioritäre Bereitstellung kommerzieller Masseninhalte zurück.

Kapitel 5 gab eine Übersicht zu den Begrifflichkeiten, Grundprinzipien und Trends bezüglich der aktuellen Änderungen in der Internet-Infrastruktur. Basierend hierauf wurden Auswirkungen, teilweise belegt durch erweiterte Messungen, auf (*i*) Content Distribution Networks, (*ii*) OTTs und Content-Anbieter, (*iii*) Endgeräte und den Internet-Edge, (*iv*) verteilte Denial-of-Service-Angriffe und (*v*) Regierungsaktivitäten diskutiert.

1. Viele bestehende Aktivitäten und staatliche Vorgaben gegen die Konsolidierung im Internet können missbraucht werden, da sie entweder nur die Gewichte zwischen großen Firmen verschieben oder Zensur und Überwachgung begünstigen.
2. Grundsätzlich neue Internet-Architekturen, die dem Problemen von Konsolidierung und Überwachung entgegenwirken, werden in der Fachgemeinschaft diskutiert. Wieweit sie die Probleme *vollständig* inhärent lösen, ist offen.

3. Die erfolgreiche, globale Verbreitung einer neuen Lösung hängt maßgeblich von den potentiellen Marktperspektiven ab. Lösungen werden nicht primär deswegen eingesetzt, weil sie technisch gut sind, sondern weil sie gegenüber bestehenden Lösungen einen ökonomischen Mehrwert bieten.

4. Vorschläge für eine neue Internet-Architektur und neue Infrastruktur-Dienste sollten im Zusammenhang mit möglichen Betreiberkonzepten diskutiert werden, um mögliche Abhängigkeiten frühzeitig zu identifizieren.

Kapitel 6 diskutierte die Konsolidierungstrends aus den Perspektiven der Internet-Ökonomie sowie ihrer Rückwirkungen in die Gesellschaft. Wirtschaftlich wurden sowohl die Perspektiven der verschiedenen Ebenen in der Infrastrukturversorgung und den zugehörigen Ressourcen, als auch die Wechselwirkungen mit der Realwirtschaft betrachtet. Die Rollen der dominanten Akteure und insbesondere ihrer Anwendungsplattformen standen im Vordergrund der gesellschaftlichen Betrachtungen genauso wie die Bedeutung der gleichmäßigen Versorgung mit Internet-Breitbanddiensten und Alarmfunktionen im Katastrophenfall. Besondere Berücksichtigung fanden Datenschutz und Aspekte der Netzneutralität.

1. Die Regulierung in der Fläche, wie sie in Deutschland beim Netzwerkzugang stattfindet, ist nicht nur richtig, sondern das Beispiel USA zeigt auch, dass ohne sie regionale Monopole mit ungünstigen Versorgungsstrukturen zu befürchten wären. Dennoch bedarf die gleichmäßige Versorgung in der Fläche noch intensiver Anstrengungen.

2. Die Konsolidierung im Internet Core, d.h. sowohl auf den Ebenen der physischen Transitinfrastrukturen, wie auf der Ebene der großen Provider, wie auf der Ebene der großen Content- und Plattformanbieter ist z.T. sehr weit vorangeschritten und bedarf aus Sicht einer sich ungehindert fortentwickelnden Informationsgesellschaft einer intensiven regulatorischen Begleitung.

3. Der gesellschaftliche Einfluss der großen (sozialen) Plattformanbieter – insbesondere im steuerbaren Bereich der Kontextbildung zwischen Inhalten – hat einen teilweise bedenklichen Wirkungsgrad erreicht und erfordert neue Verfahren in der Medieninterpretation und -bewertung, welche über die Betrachtung singulärer Inhalte hinausgehen.

4. Netzneutralität und die zuverlässige Wahrung der Persönlichkeitsrechte aller Internet-Nutzer bleiben kritische Handlungsfelder, die ein tiefes Verständnis der Detailaspekte erfordern und teilweise neue Methoden der Messung und Bewertung für das praktische Handeln der Akteure erfordern.

Kapitel 7 stellt Ausblicke auf die zu erwartenden Entwicklungen zusammen. Dabei besteht vorherrschend die Erwartung, dass sich die Konsolidierung insbesondere in den bereits fortgeschrittenen Bereichen weiter fortsetzen wird, auch wenn die IETF und einzelne Staaten Anstrengungen unternehmen, diese Entwicklung zu begrenzen und sogar in Teilbereichen umzukehren.

Verzeichnis der Internet-Vorfälle

Technischer Defekt

[I1] Vodafone: Störung im Netz von Vodafone führt zu Internet-Ausfällen bei 13,000 Kunden, 13. Nov. 2019. [Online]. Abrufbar: https://www1.wdr.de/nachrichten/stoerung-bei-online-diensten-100.html

[I2] Südamerika: Großflächiger Stromausfall in Argentinien und Uruguay mit weiten Internet-Störungen, 16. Jun. 2019. [Online]. Abrufbar: https://www.heise.de/tp/features/Blackout-in-Suedamerika-Ursache-noch-unbekannt-4447533.html

[I3] Korea Telecom: Brand in Kabelschacht führt zu städteweitem Telekommunikationsausfall in Süd Korea, 24. Nov. 2018. [Online]. Abrufbar: http://english.hani.co.kr/arti/english_edition/e_national/871848.html

[I4] Microsoft: Blitzeinschlag in Rechenzentrum führt zu Ausfall von Azure-Diensten im Süden der USA, 4. Sep. 2018. [Online]. Abrufbar: https://www.theregister.co.uk/2018/09/17/azure_outage_report/

[I5] Interxion: Stromausfall in Frankfurter Rechenzentrum führt zu starken Störungen am DE-CIX, 9. Apr. 2018. [Online]. Abrufbar: https://www.capacitymedia.com/articles/3799671/DE-CIX-down-at-Frankfurt-after-power-failure-at-Interxion

[I6] Microsoft: Azure-Dienste durch fälschlicherweise ausgelöstes Löschsystem in Nordeuropa offline, 29. Sep. 2017. [Online]. Abrufbar: https://www.theregister.co.uk/2017/10/03/faulty_fire_systems_take_down_azure_across_northern_europe

[I7] British Airways: Defekte Notstromversorgung führt nach Wartungsfehler zu weltweiten Flugausfällen, 27. Mai 2017. [Online]. Abrufbar: https://www.theregister.co.uk/2017/06/02/british_airways_data_centre_configuration

[I8] Amazon: Stromausfall und defekte USV führen zu Ausfällen der AWS Services in Australien, 4. Jun. 2016. [Online]. Abrufbar: https://aws.amazon.com/message/4372T8

[I9] Vodafone UK: Ausfall eines Rechenzentrums nach Überschwemmung stört Internetanschlüsse, 28. Dez. 2015. [Online]. Abrufbar: https://www.datacenterdynamics.com/news/vodafone-uk-data-center-suffers-outage-due-to-floods

[I10] GitHub.com: Kurze Stromunterbrechung in Rechenzentrum führt zu mehrstündigem Ausfall, 28. Jan. 2016. [Online]. Abrufbar: https://github.blog/2016-02-03-january-28th-incident-report

[I11] JetBlue: Stromausfall in Verizon-Rechenzentrum führt zu landesweitem Ausfall von Flügen, 14. Jan. 2016. [Online]. Abrufbar: https://bobsullivan.net/cybercrime/verizon-grounds-jetblue-how-could-that-happen-another-plan-b-gone-bad

[I12] Delta Telecom: Internet-Anbindung von Aserbaidschan nach Feuer auf Landkabel zu 94% eingeschränkt, 16. Nov. 2015. [Online]. Abrufbar: https://www.bgpmon.net/country-wide-outage-in-azerbaijan/

Menschliche Fehler

[I13] Cloudflare: Fehlerhafte Firewall-Regel auf Proxy führt zu weltweitem Ausfall aller CDN-Dienste, 2. Jul. 2019. [Online]. Abrufbar: https://blog.cloudflare.com/details-of-the-cloudflare-outage-on-july-2-2019

[I14] Quadriga CX: Crypto-Wallets im Wert von $190 Millionen nach Tod des Firmengründers unzugänglich, 9. Dez. 2018. [Online]. Abrufbar: https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem

[I15] Cloudflare: Fehlkonfigurierter DDoS-Schutz blockiert Zugang zu eigenem DNS-Server 1.1.1.1, 31. Mai 2018. [Online]. Abrufbar: https://blog.cloudflare.com/today-we-mitigated-1-1-1-1

[I16] Google: Fehlerhafte VM-Netzwerkkonfiguration führt zu Ausfällen in Compute Engine Instanzen, 29. Aug. 2017. [Online]. Abrufbar: https://status.cloud.google.com/incident/cloud-networking/17002

[I17] Telia: Konfigurationsfehler führt zu Transatlantik-Ausfall und weltweiten Cloud-Störungen, 2. Mai 2017. [Online]. Abrufbar: https://www.theregister.co.uk/2017/05/02/telia_hiccups_cloudflare_falls_over

[I18] Amazon: Tippfehler führt zu Backend-Neustart und S3/AWS-Ausfall an der US-Ostküste, 28. Feb. 2017. [Online]. Abrufbar: https://aws.amazon.com/message/41926

[I19] Telia: Router-Fehlkonfiguration führt zu Routing von europäischem Verkehr über Hong Kong, 20. Jun. 2016. [Online]. Abrufbar: https://www.theregister.co.uk/2016/06/20/telia_engineer_blamed_massive_net_outage

[I20] 123-reg: Fehlerhaftes Cleanup-Script löscht zahlreiche Kunden-Webseiten auf VPS-Instanzen, 16. Apr. 2016. [Online]. Abrufbar: https://arstechnica.com/information-technology/2016/04/123-reg-deletes-sites-in-massive-clean-up-script-blunder-as-customers-let-rip

[I21] Telstra: Wartungsfehler führt zu landesweitem Ausfall aller Kommunikationsdienste, 9. Feb. 2016. [Online]. Abrufbar: https://www.businessinsider.com.au/telstra-is-having-huge-national-outages-across-australia-2016-2

[I22] AMS-IX: Fehlkommunikation bei Wartungsarbeiten führt zu Ausfall von 500 Peering-Sessions, 13. Mai 2015. [Online]. Abrufbar: https://atnog.at/pipermail/atnog/2015-May/000039.html

[I23] Joyent: Versehentlicher Neustart aller VMs führt zu Überlast in Netboot-Infrastruktur, 27. Mai 2014. [Online]. Abrufbar: https://www.joyent.com/blog/postmortem-for-outage-of-us-east-1-may-27-2014

Software-Fehler

[I24] China Telecom: Router-Störungen führen zu Verbindungsausfällen zwischen Asien und Nordamerika, 13. Mai 2019. [Online]. Abrufbar: https://blog.thousandeyes.com/internet-outage-reveals-reach-of-chinas-connectivity

[I25] Ericsson UK: Abgelaufenes Software-Zertifikat führt zu landesweitem Ausfall des Mobilfunknetzes, 6. Dez. 2018. [Online]. Abrufbar: https://www.theregister.co.uk/2018/12/06/ericsson_o2_telefonica_uk_outage

[I26] Ecobee: Ausfall eines internen Web-Dienstes führt zu Unnutzbarkeit aller Smart-Home-Produkte, 4. Okt. 2018. [Online]. Abrufbar: https://www.digitaltrends.com/home/ecobee-outage

[I27] Fortnite: BGP Route Flapping bei italienischem Hoster führt zu regionalem Dienstausfall, 18. Mär. 2018. [Online]. Abrufbar: https://blog.thousandeyes.com/kill-shot-all-of-us-anatomy-fortnite-outage

[I28] MYNIC: Abgelaufenes DNSSEC-Zertifikat führt zu Totalausfall der .my Top-Level-Domain, 15. Jun. 2018. [Online]. Abrufbar: https://www.lowyat.net/2018/164585/mynic-services-experiencing-disruption-all-my-domain-names-affected/

[I29] Google: Störung bei DoubleClick-Werbung führt zu eingeschränkter Nutzbarkeit von Webseiten, 13. Mär. 2018. [Online]. Abrufbar: http://blog.catchpoint.com/2018/03/14/doubleclick-outage-another-lesson-third-party-optimization

[I30] Adobe Marketo: Fehler in automatisierter Domain-Erneuerung führt zu Domain-Parking und Dienstausfall, 25. Jul. 2017. [Online]. Abrufbar: https://blog.thousandeyes.com/what-happened-when-marketos-domain-name-expired

[I31] Rackspace: Abgelaufene Software-Lizenz einer Cloud-Lösung führt zu weltweitem Dienstausfall, 29. Jun. 2017. [Online]. Abrufbar: https://www.theregister.co.uk/2017/06/29/rackspace_hit_with_global_outage

[I32] GoDaddy: Fehlerhafter Domain-Validierungsprozess führt zur Revokierung von 6,100 Zertifikaten, 10. Jan. 2017. [Online]. Abrufbar: https://www.theregister.co.uk/2017/01/11/godaddy_pulls_unvalidated_digital_certs/

[I33] GlobalSign: Produktiveinsatz eines revokierten Schulungszertifikats führt zu HTTPS-Fehlern, 13. Okt. 2016. [Online]. Abrufbar: https://downloads.globalsign.com/acton/attachment/2674/f-06d2/1/-/-/-/-/globalsign-incident-report-13-oct-2016.pdf

[I34] NIC.IO: Fehlerhafte Name Server liefern NXDOMAIN für alle Zonen der .io Top-Level-Domain, 28. Okt. 2016. [Online]. Abrufbar: https://news.ycombinator.com/item?id=12813065

[I35] Tesla: Datennetzwerk der Fahrzeugflotte nach 3G-Ausfall bei AT&T landesweit offline, 15. Aug. 2016. [Online]. Abrufbar: https://electrek.co/2016/08/15/teslas-car-data-network-down-in-the-us-its-a-top-priority-currently-being-fixed/

[I36] Seacom: Seekabelverbindung für australischen ISP Syrex nach Router-Upgrade unterbrochen, 3. Jul. 2016. [Online]. Abrufbar: https://www.itweb.co.za/content/KwbrpOqgNmQMDLZn

[I37] AMS-IX: Ausfall von BGP Sessions beider Route Server durch nicht unterstützte BGP-Nachricht, 28. Jun. 2016. [Online]. Abrufbar: https://lists.ams-ix.net/mailman/private/tech-l/2016-June/015956.html

[I38] Cisco: Router-Ausfälle nach Überschreiten des 512K-Limits in der globalen Routing-Tabelle, 12. Aug. 2014. [Online]. Abrufbar: https://www.bgpmon.net/what-caused-todays-internet-hiccup/

Kabelbeschädigung

[I39] Comcast: Kabelbrüche bei Level3 und Zayo führen zu landesweitem Telekommunikationsausfall, 29. Jun. 2018. [Online]. Abrufbar: https://blog.thousandeyes.com/comcast-fiber-outage-rips-the-internet

[I40] ACE: Kabelbeschädigung führt zu massiven Internet-Ausfällen in zehn afrikanischen Ländern, 30. Mär. 2018. [Online]. Abrufbar: https://blogs.oracle.com/internetintelligence/ace-submarine-cable-cut-impacts-ten-countries

[I41] SMW-4: Paketverlust in Südamerika durch SEA-ME-WE4-Störung zwischen Europa und Asien, 17. Mai 2016. [Online]. Abrufbar: https://blog.thousandeyes.com/smw-4-cable-fault-ripple-effects-across-networks

[I42] PPC-1: Kabelbeschädigung zwischen Sydney und Guam führt zu Ausweich-Routen hoher Latenz, 5. Feb. 2016. [Online]. Abrufbar: https://www.zdnet.com/article/tpg-submarine-cable-outage-expected-to-last-a-month

[I43] Seacom: Kabelbeschädigung bei Bauarbeiten in Ägypten führt zu Internet-Ausfällen in ganz Afrika, 21. Jan. 2016. [Online]. Abrufbar: https://techerati.com/the-stack-archive/world/2016/01/22/civil-construction-wipes-out-internet-connectivity-across-africa

[I44] SMW-4: SEA-ME-WE4-Sabotage trennt Ägypten und Pakistan von westlichem Internet, 27. Mär. 2013. [Online]. Abrufbar: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests

[I45] I-ME-WE: Totalausfall der libanesischen Internet-Anbindung durch Kabelbeschädigung, 4. Jul. 2012. [Online]. Abrufbar: https://www.bgpmon.net/internet-outage-in-lebanon-continues-for-days/

[I46] SMW-4: Singapore Telecom in Südostasien durch SEA-ME-WE4-Beschädigung nicht erreichbar, 6. Jun. 2012. [Online]. Abrufbar: https://dyn.com/blog/smw4-break-on-south-asia/

[I47] Armenien: Ältere Frau beschädigt georgisches Landkabel und trennt Armenien vom Internet, 28. Mär. 2011. [Online]. Abrufbar: https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access

Peering Dispute

[I48] DTAG: Cogent verklagt Deutsche Telekom wegen Nichteinhaltung von Peering-Verträgen, 8. Dez. 2015. [Online]. Abrufbar: https://policyreview.info/articles/news/cogent-v-deutsche-telekom-classy-conflict/393

[I49] Netflix: Verizon nimmt Paketverlust bei Netflix über Level3-Peering in Kauf, 22. Jun. 2014. [Online]. Abrufbar: https://www.techdirt.com/articles/20140718/06533327927/level3-proves-that-verizon-is-absolutely-to-blame-netflix-congestion-using-verizons-own-data.shtml

[I50] Netflix: Verizon nimmt Paketverlust bei Netflix über Cogent-Peering in Kauf, 19. Jun. 2013. [Online]. Abrufbar: https://www.telecompetitor.com/verizon-netflix-dispute-not-just-over-peering-servers-are-new-battlefield

[I51] YouTube: France Telecom blockiert YouTube regulierungskonform im Peering-Streit mit Cogent, 22. Nov. 2012. [Online]. Abrufbar: https://www.techdirt.com/articles/20130102/02113921537/france-telecom-accused-holding-youtube-videos-hostage-unless-it-gets-more-money.shtml

[I52] Telstra: Upstream-ISPs beenden BGP-Sessions aufgrund eines vorangehenden Route Leaks, 23. Feb. 2012. [Online]. Abrufbar: https://www.bgpmon.net/how-the-internet-in-australia-went-down-under/

[I53] Netflix: Comcast fordert Paid-Peering mit Level3 aufgrund einseitigem Netflix-Verkehr, 29. Nov. 2010. [Online]. Abrufbar: https://www.telecompetitor.com/level-3comcast-dispute-revives-eyeball-vs-content-debate

[I54] Hurricane: Peering-Streit zwischen Hurricane Electric und Cogent führt zu Teilung des IPv6-Internets, 12. Okt. 2009. [Online]. Abrufbar: https://www.datacenterknowledge.com/archives/2009/10/22/peering-disputes-migrate-to-ipv6

[I55] Cogent: Sprint beendet Peering mit Cogent als Reaktion auf eskalierenden Peering-Streit, 30. Okt. 2008. [Online]. Abrufbar: https://dyn.com/blog/wrestling-with-the-zombie-spri

[I56] Telia: Cogent beendet Peering mit Telia wegen Nichteinhaltung von Peering-Vereinbarungen, 13. Mär. 2008. [Online]. Abrufbar: https://archive.nanog.org/meetings/nanog43/presentations/Zmij_Brown_peeringwars_N43.pdf

Route Leak

[I57] AMS-IX: Durch DDoS-Schutz deaggregiertes Peering-LAN-Präfix propagiert über Telia und führt zum Ausfall zahlreicher BGP Sessions, 24. Jul. 2019. [Online]. Abrufbar: https://lists.ams-ix.net/mailman/private/tech-l/2019-July/018172.html

[I58] Verizon: Akzeptanz von 20,000 more-specific Präfixen deaggregiert durch BGP Optimizer führt zu nicht erreichbaren OTT-Diensten, 24. Jun. 2019. [Online]. Abrufbar: https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today

[I59] China Telecom: Akzeptanz von 70,000 same-specific Präfixen eines Schweizer Cloud-Anbieters führt zu weltweiten Beeinträchtigungen im Internet, 6. Jun. 2019. [Online]. Abrufbar: https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china

[I60] Google: Less-specific Cloud Network Präfixe propagieren über IXP in Nigeria und China Telecom und führen zu weltweiten Dienststörungen, 12. Nov. 2018. [Online]. Abrufbar: https://www.manrs.org/2018/11/route-leak-causes-major-google-outage

[I61] Comcast: Reannoncierung von same-specific Kunden-Präfixen durch Level3 führt zu landesweitem Dienstausfall aufgrund überlasteter Router, 6. Nov. 2017. [Online]. Abrufbar: https://blog.thousandeyes.com/comcast-outage-level-3-route-leak

[I62] Verizon: Akzeptanz von 135,000 Präfixen (teils more-specific) annonciert durch Google führt zu Internet-Ausfällen insbesondere in Japan, 25. Aug. 2017. [Online]. Abrufbar: https://www.bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

[I63] Hurricane: Akzeptanz von 3,500 more-specific Präfixen deaggregiert durch BGP Optimizer eines Schweizer Hosters führt zu weltweiten Störungen, 22. Apr. 2016. [Online]. Abrufbar: https://www.bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/

[I64] Cogent: Akzeptanz von 16,000 same-specific Präfixen des indischen ISP Bharti Airtel führt zu weltweiten Beeinträchtigungen im Internet, 6. Nov. 2015. [Online]. Abrufbar: https://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/

[I65] Level3: Akzeptanz von 176,000 same-specific Präfixen über Telekom Malaysia führt zu weltweiten Beeinträchtigungen im Internet, 12. Jun. 2015. [Online]. Abrufbar: https://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/

[I66] Google: Same-specific Präfixe aller Google-ASe annonciert durch indischen ISP führen zu Dienstausfällen in Europa und Asien, 12. Mär. 2015. [Online]. Abrufbar: https://www.bgpmon.net/what-caused-the-google-service-interruption/

[I67] Los Angeles IXP: Akzeptanz von 7,000 more-specific Präfixen deaggregiert durch BGP Optimizer eines US-Hosters führt zu weltweiten Störungen, 27. Mär. 2015. [Online]. Abrufbar: https://www.bgpmon.net/bgp-optimizer-causes-thousands-of-fake-routes/

[I68] Hurricane: Akzeptanz von 415,000 same-specific Präfixen des indonesischen ISPs Indosat führt zu weltweiten Beeinträchtigungen im Internet, 2. Apr. 2014. [Online]. Abrufbar: https://www.bgpmon.net/hijack-event-today-by-indosat/

[I69] Bell: Akzeptanz von 105,000 same-specific Präfixen eines kanadischen ISPs führt zu weltweiten Beeinträchtigungen im Internet, 8. Aug. 2012. [Online]. Abrufbar: https://www.bgpmon.net/a-bgp-leak-made-in-canada/

BGP-Hijacking

[I70] TWNIC: ISP in Brasilien übernimmt kurzzeitig Privacy-fokussierten DNS-Dienst Quad-101, 8. Mai 2019. [Online]. Abrufbar: https://www.manrs.org/2019/05/public-dns-in-taiwan-the-latest-victim-to-bgp-hijack

[I71] Telegram: Iran Telecommunication übernimmt spezifischere Präfixe des Messenger-Dienstes, 30. Jul. 2018. [Online]. Abrufbar: https://www.theregister.co.uk/2018/08/01/bgp_route_leak_telegram_iran

[I72] Amazon: US-ansässiger ISP übernimmt DNS-Dienst und leitet Bitcoin-Wallets nach Russland um, 24. Apr. 2018. [Online]. Abrufbar: https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency

[I73] OTTs: Russisches Schläfer-AS übernimmt 80 Präfixe populärer Dienste für wenige Minuten, 12. Dez. 2017. [Online]. Abrufbar: https://www.bgpmon.net/popular-destinations-rerouted-to-russia/

[I74] Finanzsektor: Rostelecom übernimmt 50 Präfixe populärer Bezahldienstleister für wenige Minuten, 26. Apr. 2017. [Online]. Abrufbar: https://www.bgpmon.net/bgpstream-and-the-curious-case-of-as12389/

[I75] Amazon: Kanadischer ISP fängt mehrfach Bitcoin Mining-Verkehr im Wert von $83,000 ab, 3. Feb. 2014. [Online]. Abrufbar: https://www.bgpmon.net/the-canadian-bitcoin-hijack/

[I76] Santrex: Hacking Team unterstützt italienischen Geheimdienst bei Angriff auf eigenen Server, 16. Aug. 2013. [Online]. Abrufbar: https://www.bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/

[I77] Spamhaus: Übernahme des DNSBL-Dienstes führt zu weitreichender Spam-Markierung von Emails, 21. Mär. 2013. [Online]. Abrufbar: https://greenhost.nl/2013/03/21/spam-not-spam-tracking-hijacked-spamhaus-ip/

Denial-of-Service

[I78] servers.com: 139 Gbps TCP SYN/ACK Amplification-Angriff mit wechselnden Angriffsvektoren, 18. Aug. 2019. [Online]. Abrufbar: https://www.prnewswire.com/news-releases/root-cause-analysis-and-incident-report-on-the-august-ddos-attack-300905405.html

[I79] Wikimedia: Gezielter DDoS-Angriff führt zu europaweitem Ausfall von Wikimedia-Diensten, 6. Sep. 2019. [Online]. Abrufbar: https://blog.thousandeyes.com/analyzing-the-wikipedia-ddos-attack

[I80] Arbor: 1.7 Tbps memcached Amplification-Angriff mitigiert ohne Ausfall von Diensten, 5. Mär. 2019. [Online]. Abrufbar: https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era

[I81] GitHub.com: 1.3 Tbps memcached Amplification-Angriff mit mehrstufiger Cloudflare-Mitigierung, 28. Feb. 2018. [Online]. Abrufbar: https://github.blog/2018-03-01-ddos-incident-report

[I82] GoDaddy: DDos-Angriff auf DNS-Infrastruktur mit minimaler Kommunikation und Datenlage, 2. Mär. 2017. [Online]. Abrufbar: https://www.theregister.co.uk/2017/03/02/godaddy_dns_has_gone_diddy

[I83] Liberia: DDoS-Angriff mit Mirai-Botnet führt zu landesweitem Ausfall der Internet-Infrastruktur, 3. Nov. 2016. [Online]. Abrufbar: https://www.telegraph.co.uk/technology/2016/11/04/unprecedented-cyber-attack-takes-liberias-entire-internet-down

[I84] Dyn: 1.2 Tbps DDoS-Angriff mit Mirai-Botnet auf DNS-Server mit hohen Kollateralschäden, 21. Okt. 2016. [Online]. Abrufbar: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack

[I85] rootops: 17 Gbps TCP SYN Flooding-Angriff gleichzeitig auf alle DNS Root Server, 25. Jun. 2016. [Online]. Abrufbar: https://root-servers.org/news/events-of-20160625.txt

[I86] NS1: DDoS-Angriff auf DNS-Infrastruktur über mehrere unterschiedliche Angriffsvektoren, 16. Mai 2016. [Online]. Abrufbar: https://ns1.com/blog/how-we-responded-to-last-weeks-major-multi-faceted-ddos-attacks

[I87] DigitalOcean: DDoS-Angriff auf DNS-Infrastruktur basierend auf ausschließlich gültigen Anfragen, 24. Mär. 2016. [Online]. Abrufbar: https://blog.digitalocean.com/update-on-the-march-24-2016-dns-outage

[I88] GoDaddy: Vermeintlicher DDos-Angriff von Anonymous-Mitglied entpuppt sich als Netzausfall, 10. Sep. 2012. [Online]. Abrufbar: https://techcrunch.com/2012/09/10/godaddy-outage-takes-down-millions-of-sites/

Hacking-Angriff

[I89] Pitney Bowes: Ransomware-Angriff legt britische Online-Plattform des Versanddienstleisters lahm, 19. Okt. 2019. [Online]. Abrufbar: https://www.teiss.co.uk/pitney-bowes-ransomware-attack

[I90] iNSYNQ: Ransomware-Angriff verhindert Zugang zum Buchhaltungsdienst des Cloud-Anbieteres, 16. Jul. 2019. [Online]. Abrufbar: https://blog.insynq.com/blog/company-update-concerning-the-megacortex-ransomware-attack

[I91] Naher Osten: Malware-basierter DNS Redirection-Angriff auf staatliche und kommerzielle Dienste, 13. Sep. 2018. [Online]. Abrufbar: https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

[I92] MikroTik: Weltweiter Cryptomining-Angriff durch Web-Injection über infizierte ISP-Router, 1. Aug. 2018. [Online]. Abrufbar: https://threatpost.com/huge-cryptomining-attack-on-isp-grade-routers-spreads-globally/134667

[I93] OpenSRS: Komplexer DNS-Angriff führt zu massiver Störung von Mail- und DNS-Diensten, 28. Sep. 2017. [Online]. Abrufbar: https://opensrs.com/blog/2017/09/intermittent-degraded-performance-resolved

[I94] PTCL: Vermutete Sabotage bei Pakistan Telecom führt zu landesweitem Internet-Ausfall, 26. Dez. 2016. [Online]. Abrufbar: https://www.pakistantoday.com.pk/2016/12/27/what-is-the-real-reason-behind-pakistans-massive-internet-outage

[I95] Telstra: Mutwillige Kabelbeschädigung führt zu Internet-Ausfall an Nordküste Australiens, 18. Mai 2016. [Online]. Abrufbar: https://www.echo.net.au/2016/05/tarree-vandals-cause-north-coast-internet-outage

[I96] Pa Online: Sabotage durch ehemaligen Administrator führt zu Totalausfall des regionalen ISPs, 1. Mär. 2016. [Online]. Abrufbar: https://news.softpedia.com/news/network-admin-sabotages-isp-s-network-after-getting-fired-now-faces-jail-501933.shtml

[I97] MYNIC: Sabotage an Name Servern führt zu Umleitung aller Zonen der .my Top-Level-Domain, 1. Jul. 2013. [Online]. Abrufbar: https://www.lowyat.net/2013/9986/google-dns-poisoned-numerous-my-sites-redirected/

[I98] Vodafone UK: Totalausfall von Internet-Anschlüssen nach Hardware-Diebstahl in Rechenzentrum, 28. Feb. 2011. [Online]. Abrufbar: https://www.datacenterknowledge.com/archives/2011/02/28/data-center-theft-kos-vodafone-network

Staatliche Aktion

[I99] Yandex: Vermutete staatliche Choke-Point-Filterung bei populärer russischer Suchmaschine, 2. Apr. 2019. [Online]. Abrufbar: https://blog.thousandeyes.com/yandex-packet-loss-ddos-or-russian-firewall

[I100] Blue Content: Iran leitet asiatischen Verkehr zu Erwachsenenseiten durch BGP-Zensurversuch um, 5. Jan. 2017. [Online]. Abrufbar: https://www.theverge.com/2017/1/7/14195118/iran-porn-block-censorship-overflow-bgp-hijack

[I101] Irak: Irakische Regierung trennt landesweite Internet-Verbindung als Reaktion auf Proteste, 15. Jul. 2016. [Online]. Abrufbar: https://www.silicon.co.uk/cloud/iraq-shuts-down-internet-195163

[I102] Irak: Irakische Regierung trennt landesweite Internet-Verbindung vor Schulprüfungen, 27. Jun. 2015. [Online]. Abrufbar: https://www.theguardian.com/technology/2016/may/18/iraq-shuts-down-internet-to-stop-pupils-cheating-in-exams

[I103] Neuseeland: Vollständige Verkehrsausleitung am Southern Cross Cable zur Überwachung durch USA, 20. Mai 2014. [Online]. Abrufbar: https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11222413

[I104] Türkei: Türkische Regierung leitet Anfragen an populäre DNS-Resolver zu eigenen Servern um, 29. Mär. 2014. [Online]. Abrufbar: https://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/

[I105] Syrien: USA trennen syrische Internet-Verbindung bei mutmaßlicher Infiltrierung im Bürgerkrieg, 29. Nov. 2012. [Online]. Abrufbar: https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war

[I106] Syrien: Syrische Regierung trennt landesweite Internet-Verbindung als Reaktion auf Aufstände, 3. Jun. 2011. [Online]. Abrufbar: https://www.bgpmon.net/internet-syria-offline/

[I107] Ägypten: Ägyptische Regierung trennt landesweite Internet-Verbindung während Protesten, 27. Jan. 2011. [Online]. Abrufbar: https://www.bgpmon.net/egypt-offline/

Literaturverzeichnis

[1] A. Markkanen and D. Shey, "Edge Analytics in IoT," ABI Research, Tech. Rep., April 8 2015.

[2] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

[3] L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.

[4] A. Nordrum, "Transmission Failure Causes Nationwide Blackout in Argentina," IEEE Spectrum, Technical Review, Jun. 2019. [Online]. Available: https://spectrum.ieee.org/energywise/energy/the-smarter-grid/transmission-failure-causes-nationwide-blackout-in-argentina

[5] D. Belson, "Internet Disruption Report," Oracle, Technical Review, Jul. 2019. [Online]. Available: https://internetdisruption.report/2019/07/12/internet-disruption-report-june-2019/

[6] J. H. Cowie, A. T. Ogielski, B. Premore, E. A. Smith, and T. Underwood, "Impact of the 2003 blackouts on internet communications," *Preliminary Report, Renesys Corporation (updated March 1, 2004)*, 2003.

[7] Z. Wu, E. Purpus, and J. Li, "Bgp behavior analysis during the august 2003 blackout," *Proceedings of IEEE IM*, 2005.

[8] G. Aceto, A. Botta, P. Marchetta, V. Persico, and A. Pescapé, "A comprehensive survey on internet outages," *Journal of Network and Computer Applications*, vol. 113, pp. 36–63, 2018.

[9] J. Li and S. Brooks, "I-seismograph: Observing and measuring internet earthquakes," in *2011 Proceedings IEEE INFOCOM*, Apr. 2011, pp. 2624–2632.

[10] C. W. Johnson, "Analysing the causes of the italian and swiss blackout, 28th september 2003," in *Proceedings of the 12th Australian Workshop on Safety Critical Systems and Software-Related Programmable Systems, Adelaide, Australia*, 2007, pp. 21–30.

[11] E. Van der Vleuten and V. Lagendijk, "Transnational infrastructure vulnerability: The historical shaping of the 2006 european "blackout"," *Energy Policy*, vol. 38, no. 4, pp. 2042–2052, 2010.

[12] O. P. Veloza and F. Santamaria, "Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes," *The Electricity Journal*, vol. 29, no. 7, pp. 42–49, 2016.

[13] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, no. 8, pp. 1245–1265, 2010.

[14] S. Erjongmanee and C. Ji, "Large-scale network-service disruption: Dependencies and external factors," *IEEE Transactions on Network and Service Management*, vol. 8, no. 4, pp. 375–386, 2011.

[15] Y. Liu, X. Luo, R. K. Chang, and J. Su, "Characterizing inter-domain rerouting by betweenness centrality after disruptive events," *IEEE Journal on Selected areas in communications*, vol. 31, no. 6, pp. 1147–1157, 2013.

[16] A. Mauthe, D. Hutchison, E. K. Cetinkaya, I. Ganchev, J. Rak, J. P. Sterbenz, M. Gunkelk, P. Smith, and T. Gomes, "Disaster-resilient communication networks: Principles and best practices," in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2016, pp. 1–10.

[17] "Emergency Notice: This KT fire caused serious server loss," Technical Review, Nov 2018. [Online]. Available: https://mania.kr/g2/bbs/board.php?bo_table=notice&wr_id=5862

[18] K. Liang, X. Hao, W. An, Y. Tang, and Y. Cong, "Study on cable fire spread and smoke temperature distribution in t-shaped utility tunnel," *Case Studies in Thermal Engineering*, vol. 14, p. 100433, 2019.

[19] K. Ye, X. Zhou, L. Yang, X. Tang, Y. Zheng, B. Cao, Y. Peng, H. Liu, and Y. Ni, "A multi-scale analysis of the fire problems in an urban utility tunnel," *Energies*, vol. 12, no. 10, p. 1976, 2019.

[20] G. Ke, L. Zimeng, J. Jinzhang, L. Zeyi, A. Yisimayili, Q. Zhipeng, W. Yaju, and L. Shengnan, "Study on flame spread characteristics of flame-retardant cables in mine," *Advances in Polymer Technology*, vol. 2020, 2020.

[21] D. Guo, G. Zhang, G. Zhu, B. Jia, and P. Zhang, "Applicability of liquid nitrogen fire extinguishing in urban underground utility tunnel," *Case Studies in Thermal Engineering*, p. 100657, 2020.

[22] W. Zhou, W. Nie, X. Liu, C. Zhou, C. Wei, C. Liu, Q. Liu, and S. Yin, "Optimization of dust removal performance of ventilation system in tunnel constructed using shield tunneling machine," *Building and Environment*, vol. 173, p. 106745, 2020.

[23] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding bgp misconfiguration," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 4, pp. 3–16, 2002.

[24] M. S. Siddiqui, D. Montero, M. Yannuzzi, R. Serral-Gracià, and X. Masip-Bruin, "Route leak identification: A step toward making inter-domain routing more reliable," in *2014 10th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2014, pp. 1–8.

[25] M. Siddiqui, D. Montero, M. Yannuzzi, R. Serral-Gracià, X. Masip-Bruin, and W. Ramírez, "Route leak detection using real-time analytics on local bgp information," in *2014 IEEE Global Communications Conference*. IEEE, 2014, pp. 1942–1948.

[26] L. Cheng, P. Zhang, and Y. Ma, "Route leakage detection algorithm based on new feature discovery," in *Proceedings of the 4th International Conference on Communication and Information Processing*, 2018, pp. 222–226.

[27] M. Cosovic, S. Obradovic, and E. Junuz, "Deep learning for detection of bgp anomalies," in *International Work-Conference on Time Series Analysis*. Springer, 2017, pp. 95–113.

[28] M. F. Galmés, R. C. Aumatell, A. Cabellos-Aparicio, S. Ren, X. Wei, and B. Liu, "Preventing route leaks using a decentralized approach," in *2020 IFIP Networking Conference (Networking)*. IEEE, 2020, pp. 509–513.

[29] J. Jin, "Bgp route leak prevention based on bgpsec," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–6.

[30] M. S. Siddiqui, D. Montero, M. Yannuzzi, R. Serral-Gracià, and X. Masip-Bruin, "Diagnosis of route leaks among autonomous systems in the internet," in *2014 International Conference on Smart Communications in Network Technologies (SaCoNeT)*. IEEE, 2014, pp. 1–6.

[31] C. Wang, Z. Lu, Z. Wu, J. Wu, and S. Huang, "Optimizing multi-cloud cdn deployment and scheduling strategies using big data analysis," in *2017 IEEE International Conference on Services Computing (SCC)*. IEEE, 2017, pp. 273–280.

[32] H. H. Liu, Y. Wang, Y. R. Yang, H. Wang, and C. Tian, "Optimizing cost and performance for content multihoming," in *Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication*, 2012, pp. 371–382.

[33] H. Wang, G. Tang, K. Wu, and J. Fan, "Speeding up multi-cdn content delivery via traffic demand reshaping," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018, pp. 422–433.

[34] W. Dang, H. Wang, J. Wang, H. Wang *et al.*, "Evaluating performance and inefficient routing of an anycast cdn," in *2019 IEEE/ACM 27th International Symposium on Quality of Service (IWQoS)*. IEEE, 2019, pp. 1–10.

[35] A. Tekerek, C. Gemci, and O. F. Bay, "Development of a hybrid web application firewall to prevent web based attacks," in *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*. IEEE, 2014, pp. 1–4.

[36] K. Nagendran, S. Balaji, B. A. Raj, P. Chanthrika, and R. Amirthaa, "Web application firewall evasion techniques," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2020, pp. 194–199.

[37] H. Chang, S. Jamin, and W. Willinger, "To peer or not to peer: Modeling the evolution of the internet's as-level topology," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*. IEEE, 2006, pp. 1–12.

[38] A. Lodhi, A. Dhamdhere, and C. Dovrolis, "Open peering by internet transit providers: Peer preference or peer pressure?" in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 2562–2570.

[39] C. Courcoubetis, K. Sdrolias, and R. Weber, "Network neutrality [paid peering: Pricing and adoption incentives]," *Journal of Communications and Networks*, vol. 18, no. 6, pp. 975–988, 2016.

[40] L. Shi, X. Wang, and M. R. TB, "On optimal hybrid premium peering and caching purchasing strategy of internet content providers," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 2107–2115.

[41] T. Böttger, F. Cuadrado, G. Tyson, I. Castro, and S. Uhlig, "Open connect everywhere: A glimpse at the internet ecosystem through the lens of the netflix cdn," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 1, pp. 28–34, 2018.

[42] R. T. Ma, J. Wang, and D. M. Chiu, "Paid prioritization and its impact on net neutrality," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 367–379, 2017.

[43] H. K. Cheng, S. Bandyopadhyay, and H. Guo, "The debate on net neutrality: A policy perspective," *Information systems research*, vol. 22, no. 1, pp. 60–82, 2011.

[44] J. Crowcroft, "Net neutrality: the technical side of the debate: a white paper," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 1, pp. 49–56, 2007.

[45] T. Rudl. (2017) Netzneutralität: Jahresbericht deckt verstöße gegen das offene internet auf. [Online]. Available: https://netzpolitik.org/2017/netzneutralitaet-jahresbericht-deckt-verstoesse-gegen-das-offene-internet-auf/

[46] Q. Scheitle, O. Hohlfeld, J. Gamba, J. Jelten, T. Zimmermann, S. D. Strowes, and N. Vallina-Rodriguez, "A Long Way to the Top: Significance, Structure, and Stability of Internet Top Lists," in *Proceedings of the Internet Measurement Conference (IMC '18)*. New York, NY, USA: ACM, 2018, pp. 478–493.

[47] S. A. Jyothi, "Solar Superstorms: Planning for an Internet Apocalypse," in *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, ser. SIGCOMM '21. New York, NY, USA: ACM, 2021, pp. 692–704.

[48] B. für Sicherheit in der Informationstechnik, "It-grundschutz-kompendium," 2020. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

[49] G. Nomikos, V. Kotronis, P. Sermpezis, P. Gigis, L. Manassakis, C. Dietzel, S. Konstantaras, X. Dimitropoulos, and V. Giotsas, "O Peer, Where Art Thou? Uncovering Remote Peering Interconnections at IXPs," in *Proceedings of the Internet Measurement Conference (IMC) 2018*. New York, NY, USA: ACM, 2018, pp. 265–278. [Online]. Available: https://doi.org/10.1145/3278532.3278556

[50] T. Böttger, G. Antichi, E. L. Fernandes, R. di Lallo, M. Bruyere, S. Uhlig, G. Tyson, and I. Castro, "Shaping the internet: 10 years of ixp growth," Open Archive: arXiv.org, Tech Report 1810.10963, July 2019.

[51] V. Giotsas, C. Dietzel, G. Smaragdakis, A. Feldmann, A. Berger, and E. Aben, "Detecting peering infrastructure outages in the wild," in *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, ser. SIGCOMM '17. New York, NY, USA: ACM, 2017, p. 446–459.

[52] T. King, C. Dietzel, J. Snijders, G. Doering, and G. Hankins, "BLACKHOLE Community," IETF, RFC 7999, October 2016.

[53] M. Nawrocki, J. Blendin, C. Dietzel, T. C. Schmidt, and M. Wählisch, "Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs," in *Proc. of ACM Internet Measurement Conference (IMC)*. New York: ACM, 2019, pp. 435–448. [Online]. Available: https://doi.org/10.1145/3355369.3355593

[54] G. Antichi, I. Castro, M. Chiesa, E. L. Fernandes, R. Lapeyrade, D. Kopp, J. H. Han, M. Bruyere, C. Dietzel, M. Gusat, A. W. Moore, P. Owezarski, S. Uhlig, and M. Canini, "ENDEAVOUR: A Scalable SDN Architecture For Real-World IXPs," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2553–2562, 2017.

[55] C. Dietzel, M. Wichtlhuber, G. Smaragdakis, and A. Feldmann, "Stellar: Network Attack Mitigation Using Advanced Blackholing," in *Proc. of ACM CoNEXT*. New York, NY, USA: ACM, 2018, pp. 152–164.

[56] S. Carl-Mitchell and J. Quarterman, "Using ARP to implement transparent subnet gateways," IETF, RFC 1027, October 1987.

[57] M. Calder, A. Flavel, E. Katz-Bassett, R. Mahajan, and J. Padhye, "Analyzing the performance of an anycast cdn," in *ACM Internet Measurement Conference (IMC)*, ser. IMC '15. New York, NY, USA: ACM, 2015, p. 531–537.

[58] M. Omer, R. Nilchiani, and A. Mostashari, "Measuring the resilience of the trans-oceanic telecommunication cable system," *IEEE Systems Journal*, vol. 3, no. 3, pp. 295–303, 2009.

[59] T. Bilski, "Disaster's impact on internet performance–case study," in *International Conference on Computer Networks*, 2009, pp. 210–217.

[60] M. Kobayashi, "Experience of infrastructure damage caused by the great east japan earthquake and countermeasures against future disasters," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 23–29, 2014.

[61] R. Fanou, B. Huffaker, R. Mok, and K. Claffy, "Unintended consequences: Effects of submarine cable deployment on internet routing," in *International Conference on Passive and Active Network Measurement (PAM)*, Mar. 2020, pp. 211–227.

[62] D. L. Msongaleli, F. Dikbiyik, M. Zukerman, and B. Mukherjee, "Disaster-aware submarine fiber-optic cable deployment," in *2015 International Conference on Optical Network Design and Modeling (ONDM)*, May 2015, pp. 245–250.

[63] ——, "Disaster-aware submarine fiber-optic cable deployment for mesh networks," *Journal of Lightwave Technology*, vol. 34, no. 18, pp. 4293–4303, 2016.

[64] Z. Wang, Q. Wang, M. Zukerman, J. Guo, Y. Wang, G. Wang, J. Yang, and B. Moran, "Multiobjective path optimization for critical infrastructure links with consideration to seismic resilience," *Computer-Aided Civil and Infrastructure Engineering*, vol. 32, no. 10, pp. 836–855, 2017.

[65] Z. Wang, Q. Wang, M. Zukerman, and B. Moran, "A seismic resistant design algorithm for laying and shielding of optical fiber cables," *Journal of Lightwave Technology*, vol. 35, no. 14, pp. 3060–3074, 2017.

[66] A. Agrawal, V. Bhatia, and S. Prakash, "Network and risk modeling for disaster survivability analysis of backbone optical communication networks," *Journal of Lightwave Technology*, vol. 37, no. 10, pp. 2352–2362, 2019.

[67] A. Agrawal, P. Sharma, V. Bhatia, and S. Prakash, "Survivability enhancement of backbone optical networks leveraging seismic zone information," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec. 2017, pp. 1–6.

[68] Z. Wang, Q. Wang, B. Moran, and M. Zukerman, "Terrain constrained path planning for long-haul cables," *Optics express*, vol. 27, no. 6, pp. 8221–8235, 2019.

[69] ——, "Optimal submarine cable path planning and trunk-and-branch tree network topology design," *IEEE/ACM Transactions on Networking*, 2020.

[70] B. Mukherjee, M. F. Habib, and F. Dikbiyik, "Network adaptability from disaster disruptions and cascading failures," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 230–238, 2014.

[71] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska, "Recodis: Resilient communication services protecting end-user applications from disaster-based failures," in *2016 18th International Conference on Transparent Optical Networks (ICTON)*, Jul. 2016, pp. 1–4.

[72] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. De Sousa, A. Iossifides, R. Travanca, J. André *et al.*, "A survey of strategies for communication networks to protect against large-scale natural disasters," in *2016 8th international workshop on resilient networks design and modeling (RNDM)*, Sep. 2016, pp. 11–22.

[73] P. N. Tran and H. Saito, "Enhancing physical network robustness against earthquake disasters with additional links," *Journal of Lightwave Technology*, vol. 34, no. 22, pp. 5226–5238, 2016.

[74] M. W. Ashraf, S. M. Idrus, F. Iqbal, R. A. Butt, and M. Faheem, "Disaster-resilient optical network survivability: a comprehensive survey," in *Photonics*, vol. 5, no. 4, Dec. 2018, p. 35.

[75] S. Ferdousi, M. Tornatore, M. F. Habib, and B. Mukherjee, "Rapid data evacuation for large-scale disasters in optical cloud networks," *Journal of Optical Communications and Networking*, vol. 7, no. 12, pp. B163–B172, 2015.

[76] X. Xie, Q. Ling, P. Lu, W. Xu, and Z. Zhu, "Evacuate before too late: distributed backup in inter-dc networks with progressive disasters," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 5, pp. 1058–1074, 2017.

[77] R. B. Lourenço, G. B. Figueiredo, M. Tornatore, and B. Mukherjee, "Data evacuation from data centers in disaster-affected regions through software-defined satellite networks," *Computer Networks*, vol. 148, pp. 88–100, 2019.

[78] S. Ferdousi, F. Dikbiyik, M. Tornatore, and B. Mukherjee, "Progressive datacenter recovery over optical core networks after a large-scale disaster," in *2016 12th International Conference on the Design of Reliable Communication Networks (DRCN)*, Mar. 2016, pp. 47–54.

[79] ——, "Joint progressive recovery of optical network and datacenters after large-scale disasters," in *2017 Optical Fiber Communications Conference and Exhibition (OFC)*, Mar. 2017, pp. 1–3.

[80] R. Gour, J. Kong, G. Ishigaki, A. Yousefpour, S. Hong, and J. P. Jue, "Finding survivable routes in multi-domain optical networks with geographically correlated failures," *Journal of Optical Communications and Networking*, vol. 10, no. 8, pp. C39–C49, 2018.

[81] M. W. Ashraf, S. M. Idrus, R. A. Butt, and F. Iqbal, "Post-disaster least loaded lightpath routing in elastic optical networks," *International Journal of Communication Systems*, vol. 32, no. 8, p. e3920, 2019.

[82] Q. Mao and N. Li, "Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems," *Natural hazards*, vol. 93, no. 1, pp. 315–337, 2018.

[83] J. Arkko, "Centralised Architectures in Internet Infrastructure," IETF, Internet-Draft – work in progress 00, November 2019.

[84] B. Carpenter, "Architectural Principles of the Internet," IETF, RFC 1958, June 1996.

[85] Caida.org, "Caida as relationships dataset," 2020. [Online]. Available: http://www.caida.org/data/as-relationships/

[86] T. P. Peixoto, "Hierarchical block structures and high-resolution model selection in large networks," *Phys. Rev. X*, vol. 4, p. 011047, Mar 2014.

[87] P. F. Tehrani, E. Osterweil, J. Schiller, T. C. Schmidt, and M. Wählisch, "The Missing Piece: On Namespace Management in NDN and How DNSSEC Might Help," in *Proc. of 6th ACM Conference on Information-Centric Networking (ICN)*. New York: ACM, 2019, pp. 37–43. [Online]. Available: https://doi.org/10.1145/3357150.3357401

[88] G. Huston, "DNS Trends," *The Internet Protocol Journal*, vol. 24, no. 1, pp. 2–17, Mär. 2021.

[89] "On Firefox moving DNS to a third party)," PowerDNS, Technical Blog, September 2018. [Online]. Available: https://blog.powerdns.com/2018/09/04/on-firefox-moving-dns-to-a-third-party/

[90] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a Large European IXP," in *Proc. of the ACM SIGCOMM*. New York, NY, USA: ACM, 2012, pp. 163–174.

[91] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF, RFC 7252, June 2014.

[92] A. Banks and R. G. (Eds.), "MQTT Version 3.1.1," OASIS, OASIS Standard, October 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

[93] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. Schmidt, and M. Waehlisch, "Information-Centric Networking (ICN) Research Challenges," IETF, RFC 7927, July 2016.

[94] M. Strong, "Think Global, Peer Local. Peer with CloudFlare at 100 Internet Exchange Points," Cloudflare, The Cloudflare Blog, January 2016. [Online]. Available: https://blog.cloudflare.com/think-global-peer-local-peer-with-cloudflare-at-100-internet-exchange-points/

[95] E. Savitz, "Netflix Shifts Traffic To Its Own CDN; Akamai, Limelight Shrs Hit," Forbes, Blog Post, Jun. 2012. [Online]. Available: https://www.forbes.com/sites/ericsavitz/2012/06/05/netflix-shifts-traffic-to-its-own-cdn-akamai-limelight-shrs-hit/

[96] T. Böttger, F. Cuadrado, G. Tyson, I. Castro, and S. Uhlig, "Open Connect Everywhere: A Glimpse at the Internet Ecosystem through the Lens of the Netflix CDN," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 48, no. 1, pp. 28–34, Apr. 2018.

[97] Telxius, "Telxius and Amazon Web Services reach agreement on transatlantic subsea cable MAREA," Telxius, Press Release, January 2019. [Online]. Available: https://telxius.com/en/telxius-and-amazon-web-services-reach-agreement-on-transatlantic-subsea-cable-marea/

[98] D. Bach, "Microsoft, Facebook and Telxius complete the highest-capacity subsea cable to cross the Atlantic," Microsoft, Press Release, September 2017. [Online]. Available: https://news.microsoft.com/features/microsoft-facebook-telxius-complete-highest-capacity-subsea-cable-cross-atlantic/

[99] C. of Commerce, "Google Fiber Internet Review – 2021 (Source: https://www.chamberofcommerce.org/review/google-fiber-internet)," Chamber of Commerce, Website, 2021. [Online]. Available: https://www.chamberofcommerce.org/review/google-fiber-internet

[100] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained-Node Networks," IETF, RFC 7228, May 2014.

[101] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute, Technical Report, June 2015.

[102] M. Nawrocki, T. C. Schmidt, and M. Wählisch, "Uncovering Vulnerable Industrial Control Systems from the Internet Core," in *Proc. of IEEE/IFIP Network Operations and Management Symposium (NOMS)*. Piscataway, NJ, USA: IEEE Press, April 2020, pp. 1–9. [Online]. Available: https://arxiv.org/abs/1901.04411

[103] ——, "Industrial control protocols in the Internet core: Dismantling operational practices," *International Journal of Network Management*, 2021. [Online]. Available: https://doi.org/10.1002/nem.2158

[104] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach," in *Proceedings of the Internet Measurement Conference*. New York, NY, USA: ACM, 2019, pp. 267–279.

[105] B. Collier, D. R. Thomas, R. Clayton, and A. Hutchings, "Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks," in *Proceedings of the Internet Measurement Conference*, ser. IMC '19. New York, NY, USA: ACM, 2019, pp. 50–64.

[106] F. J. Ryba, M. Orlinski, M. Wählisch, C. Rossow, and T. C. Schmidt, "Amplification and DRDoS Attack Defense – A Survey and New Perspectives," Open Archive: arXiv.org, Technical Report arXiv:1505.07892, June 2015. [Online]. Available: http://arxiv.org/abs/1505.07892

[107] R. Hiesgen, M. Nawrocki, A. King, A. Dainotti, T. C. Schmidt, and M. Wählisch, "Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope," 2021, under submission.

[108] Z. Durumeric, E. Wustrow, and J. Halderman, "ZMap: Fast Internet-Wide Scanning and its Security Applications," in *In Proceedings of the 22nd USENIX Security Symposium*, 08 2013, pp. 605–620.

[109] D. Madory, "The Mystery of AS8003," Kentik, Kentik Blog, April 2021. [Online]. Available: https://www.kentik.com/blog/the-mystery-of-as8003/

[110] V. Jacobson, D. K. Smetters, J. D. Thornton, and M. F. Plass, "Networking Named Content," in *5th Int. Conf. on emerging Networking Experiments and Technologies (ACM CoNEXT'09)*. New York, NY, USA: ACM, Dez. 2009, pp. 1–12.

[111] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named Data Networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014.

[112] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, July 2012.

[113] J.-P. Kleinhans, "Internet of Insecure Things. Can Security Assessment Cure Market Failures?" Stiftung Neue Verantwortung, Tech. Rep., September 2017.

[114] ——, "Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit," Stiftung Neue Verantwortung, Tech. Rep., April 2018.

[115] E. Lear, R. Droms, and D. Romascanu, "Manufacturer Usage Description Specification," IETF, RFC 8520, March 2019.

[116] R. Dobbins, D. Migault, R. Moskowitz, N. Teague, L. Xia, and K. Nishizuka, "Use Cases for DDoS Open Threat Signaling," IETF, RFC 8903, May 2021.

[117] "Freedom on the Net," Freedom House, Annual Survey, 2021. [Online]. Available: https://freedomhouse.org/report/freedom-net

[118] J. Nicas, "Apple Reaches $2 Trillion, Punctuating Big Tech's Grip," New York Times, Article, September 2020. [Online]. Available: https://www.nytimes.com/2020/08/19/technology/apple-2-trillion.html

[119] "Consolidation in the Internet Economy," Internet Society, Internet Society Global Internet Report, 2019. [Online]. Available: https://future.internetsociety.org/2019/

[120] "Russia: Freedom on the Net 2020 Country Report," Freedom House, Annual Survey, 2020. [Online]. Available: https://freedomhouse.org/country/russia/freedom-net/2020

[121] "Indonesia: Freedom on the Net 2020 Country Report," Freedom House, Annual Survey, 2020. [Online]. Available: https://freedomhouse.org/country/indonesia/freedom-net/2020

[122] T. Allard and J. Stubbs, "Indonesian army wields internet 'news' as a weapon in Papua," Reuters, Press Release, January 2020. [Online]. Available: https://www.reuters.com/article/us-indonesia-military-websites-insight/indonesian-army-wields-internet-news-as-a-weapon-in-papua-idUSKBN1Z7001

[123] Pew Research Center, "Internet Fact Sheets," Washington, DC, 2020. [Online]. Available: https://www.pewresearch.org/internet/

[124] S. Greenstein, "The Basic Economics of Internet Infrastructure," *Journal of Economic Perspectives*, vol. 34, no. 2, pp. 192–214, Spring 2020.

[125] M. Moore and D. Tambini, *Digital Dominance – The Power of Google, Amazon, Facebook, and Apple.* Oxford University Press, 2018.

[126] Caida.org, "Caida as rank," 2020. [Online]. Available: https://www.caida.org/data/as-classification/

[127] E. Mededovic, V. G. Douros, and P. Mähönen, "Node centrality metrics for hotspots analysis in telecom big data," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* IEEE, 2019, pp. 417–422.

[128] T. Böttger, G. Antichi, E. L. Fernandes, R. di Lallo, M. Bruyere, S. Uhlig, and I. Castro, "Shaping the internet: 10 years of IXP growth," *CoRR*, vol. abs/1810.10963, 2019. [Online]. Available: http://arxiv.org/abs/1810.10963

[129] H. Trostle and C. Mitchel, "Profiles of Monopoly: Big Cable and Telecom," The Institute for Local Self-Reliance (ILSR), Tech. Rep., August 2020. [Online]. Available: https://cdn.ilsr.org/wp-content/uploads/2020/08/2020_08_Profiles-of-Monopoly.pdf

[130] J. Brodkin, "Jared Mauch didn't have good broadband—so he built his own fiber ISP," ars Technica, Tech. Rep., January 12 2021. [Online]. Available: https://arstechnica.com/information-technology/2021/01/jared-mauch-didnt-have-good-broadband-so-he-built-his-own-fiber-isp/

[131] "Der Breitbandatlas," Bundesministerium für Verkehr und digitale Infrastruktur, Tech. Rep., 2020. [Online]. Available: https://www.breitbandatlas.de

[132] J. Rohlfs, "A Theory of Interdependent Demand for a Communications Service," *The Bell Journal of Economics and Management Science*, vol. 5, no. 1, pp. 16–37, 1974. [Online]. Available: http://www.jstor.org/stable/3003090

[133] OECD, "Measuring the Internet Economy," OECD Publishing, Paris, FR, Digital Economy Papers 226, 2013. [Online]. Available: https://doi.org/10.1787/5k43gjg6r8jf-en

[134] C. Wernick, "Ökonomie und Kostenstrukturen des Glasfaserausbaus," WIK - Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Tech. Rep., 2016. [Online]. Available: https://www.wik.org/fileadmin/Studien/2016/Studie_OEkonomie_Glasfaserausbau.pdf

[135] C. Ilgmann, "Breitbandausbau in Deutschland: eine strategische Analyse," *Wirtschaftsdienst - Zeitschrift für Wirtschaftspolitik*, vol. 99, no. 2, pp. 119–125, 2019.

[136] L. Taurines and et al., "The Great Digital Divide," Capgemini Research Institute, Technical Report, 2020. [Online]. Available: https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2020/05/Digital-Divide-3.pdf

[137] D. Schmidt and S. A. Power, "Offline World: the Internet as Social Infrastructure among the Unconnected in Quasi-Rural Illinois," *Integr. psych. behav.*, August 2020. [Online]. Available: https://doi.org/10.1007/s12124-020-09574-9

[138] W. Briglauer, N. Dürr, and K. Gugler, "A retrospective study on the regional benefits and spillover effects of high-speed broadband networks: Evidence from German counties," *International Journal of Industrial Organization*, vol. 74, p. 102677, 2021. [Online]. Available: https://doi.org/10.1016/j.ijindorg.2020.102677

[139] L. Townsend, A. Sathiaseelan, G. Fairhurst, and C. Wallace, "Enhanced broadband access as a solution to the social and economic problems of the rural digital divide," *Local Economy*, vol. 28, no. 6, pp. 580–595, 2013. [Online]. Available: https://doi.org/10.1177/0269094213496974

[140] M. Horkheimer and T. W. Adorno, "DIALEKTIK DER AUFKLÄRUNG. PHILOSOPHISCHE FRAGMENTE (1944/1947)," *Horkheimer, Max, Gesammelte Schriften Bd*, vol. 5, 1969.

[141] L. de Dominicis, L. Dijkstra, and N. Pontarollo, "Social, demographic and economic factors affecting the vote for parties opposed to European integration," EU Directorate-General for Regional and Urban Policy, WORKING PAPER WP 05/2020, 2020. [Online]. Available: https://ec.europa.eu/regional_policy/sources/docgener/work/2020_05_discontent_en.pdf

[142] H. Schulzrinne, "Location-to-URL Mapping Architecture and Framework," IETF, RFC 5582, September 2009.

[143] T. Hardie, A. Newton, H. Schulzrinne, and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," IETF, RFC 5222, August 2008.

[144] H. Tschofening, " A Secure and Privacy-Friendly IP-based Emergency Services Architecture," Ph.D. dissertation, Georg-August-Universität Göttingen, 2019.

[145] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," IETF, RFC 4033, March 2005.

[146] ——, "Resource Records for the DNS Security Extensions," IETF, RFC 4034, March 2005.

[147] ——, "Protocol Modifications for the DNS Security Extensions," IETF, RFC 4035, March 2005.

[148] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.

[149] P. F. Tehrani, E. Osterweil, J. Schiller, T. C. Schmidt, and M. Wählisch, "Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI," in *30th The Web Conference (WWW'21)*. New York, USA: ACM, April 2021.

[150] D. O'Callaghan, D. Greene, M. Conway, J. Carthy, and P. Cunningham, "Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems," *Social Science Computer Review*, vol. 33, no. 4, pp. 459–478, 2015. [Online]. Available: https://doi.org/10.1177/0894439314555329

[151] ——, "Uncovering the Wider Structure of Extreme Right Communities Spanning Popular Online Networks," in *Proceedings of the 5th Annual ACM Web Science Conference*, ser. WebSci '13. New York, NY, USA: Association for Computing Machinery, 2013, pp. 276–285. [Online]. Available: https://doi.org/10.1145/2464464.2464495

[152] M. H. Ribeiro, R. Ottoni, R. West, V. A. F. Almeida, and W. Meira, "Auditing Radicalization Pathways on YouTube," Open Archive: arXiv.org, Technical Report abs/1908.08313, 2019. [Online]. Available: https://arxiv.org/abs/1908.08313

[153] M. Ledwich and A. Zaitsev, "Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization," *First Monday*, vol. 25, no. 3, February 2020. [Online]. Available: https://dx.doi.org/10.5210/fm.v25i3.10419

[154] T. Wu, "Network Neutrality, Broadband Discrimination," *Journal on Telecom and High Tech Law*, vol. 2, pp. 141–176, 2003.

[155] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-End Arguments in System Design," *ACM Trans. Comput. Syst.*, vol. 2, no. 4, pp. 277–288, Nov 1984.

[156] F. Li, A. M. Kakhki, D. Choffnes, P. Gill, and A. Mislove, "Classifiers Unclassified: An Efficient Approach to Revealing IP Traffic Classification Rules," in *Proceedings of the 2016 Internet Measurement Conference*, ser. IMC '16. New York, NY, USA: ACM, 2016, pp. 239–245. [Online]. Available: https://doi.org/10.1145/2987443.2987464

[157] C. Contavalli, W. van der Gaast, D. Lawrence, and W. Kumari, "Client Subnet in DNS Queries," IETF, RFC 7871, May 2016.

[158] "The Internet of Things: An Overview," Internet Society, Internet Society Global Internet Report, 2015. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[159] A. Nassehi, *Muster*. München: C.H.Beck, 2019.

[160] Z. Bauman, *Liquid Modernity*. Cambridge, UK: Polity Press, 2000.

[161] C. Daase and N. Deitelhoff, "Privatisierung der Sicherheit – Eine sozialwissenschaftliche Studie," Tech. Rep. 11, September 2013.

[162] S. Krasmann, R. Kreissl, S. Kühne, B. Paul, and C. Schlepper, “Die gesellschaftliche Konstruktion von Sicherheit – Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung,” Tech. Rep. 13, Maärz 2014.