Bundesamt für Sicherheit in der Informationstechnik

leitwert

link-lab

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

TECHNISCHE UNIVERSITÄT DRESDEN

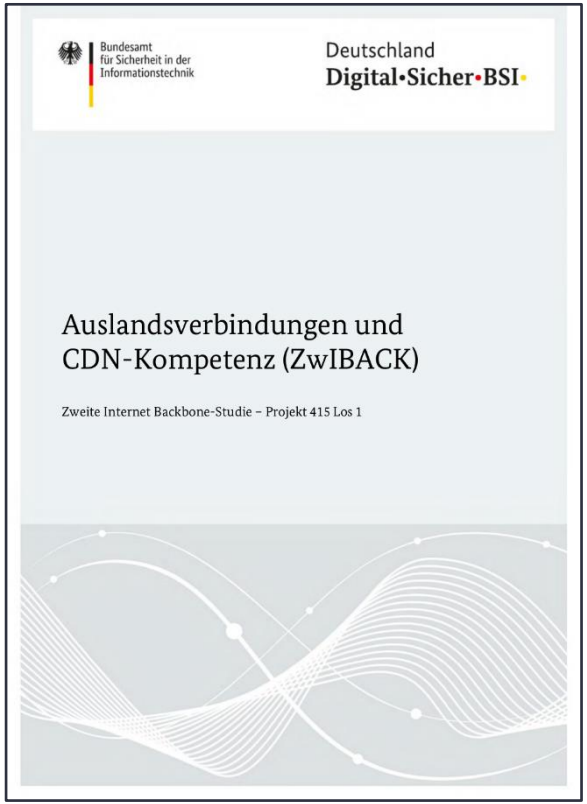
Second Internet Backbone Study

Johann Schlamp, Thomas C. Schmidt, Matthias Wählisch
schlamp@leitwert.net | {schmidt, mw}@link-lab.net

Anders Kölligan, Markus de Brün
{anders.koelligan, markus.debruen}@bsi.bund.de

Why?

- Ongoing consolidation
  - central service providers
  - consequences of outages
- Changing Internet landscape
  - role of content providers
  - open standards vs. proprietary systems



Overview

Chapter 1
Introduction and Motivation

Chapter 2
Real Internet Outages

Chapter 3
Virtual Internet Outages

Chapter 4
International Cable Connections

Chapter 5
Changes of the Internet Infrastructure

Chapter 6
Social and Economical Implications

Chapter 7
Outlook & Anticipated Developments

Chapter 8
Conclusion

Overview – Chapter 2

Chapter 1 **Introduction and Motivation**	Chapter 2 **Real Internet Outages**	Chapter 3 **Virtual Internet Outages**	Chapter 4 **International Cable Connections**
Chapter 5 **Changes of the Internet Infrastructure**	Chapter 6 **Social and Economical Implications**	Chapter 7 **Outlook & Anticipated Developments**	Chapter 8 **Conclusion**

Catalogue of 107 Internet incidents (2008-2019)

Category
SERVICE OUTAGE
RANDOM

Physical damage
[I1], [I2], [I3], [I4], [I5], [I6], [I7], [I8], [I9], [I10], [I11], [I12]

Human error
[I13], [I14], [I15], [I16], [I17], [I18], [I19], [I20], [I21], [I22], [I23]

Software bug
[I24], [I25], [I26], [I27], [I28], [I29], [I30], [I31], [I32], [I33], [I34], [I35], [I36], [I37], [I38]

Number of incidents	38
Damage potential	MEDIUM
Likelihood of event	HIGH

Category
REROUTING
NEGLIGENT

Fibre cut
[I39], [I40], [I41], [I42], [I43], [I44], [I45], [I46], [I47]

Peering dispute
[I48], [I49], [I50], [I51], [I52], [I53], [I54], [I55], [I56]

Route leak
[I57], [I58], [I59], [I60], [I61], [I62], [I63], [I64], [I65], [I66], [I67], [I68], [I69]

Number of incidents	31
Damage potential	HIGH
Likelihood of event	MEDIUM

Category
ATTACK
INTENTIONAL

BGP hijacking
[I70], [I71], [I72], [I73], [I74], [I75], [I76], [I77]

Denial-of-service
[I78], [I79], [I80], [I81], [I82], [I83], [I84], [I85], [I86], [I87], [I88]

Hacking attack
[I89], [I90], [I91], [I92], [I93], [I94], [I95], [I96], [I97], [I98]

Nation-state action
[I99], [I100], [I101], [I102], [I103], [I104], [I105], [I106], [I107]

Number of incidents	38
Damage potential	HIGH
Likelihood of event	HIGH

Assessment of each incident

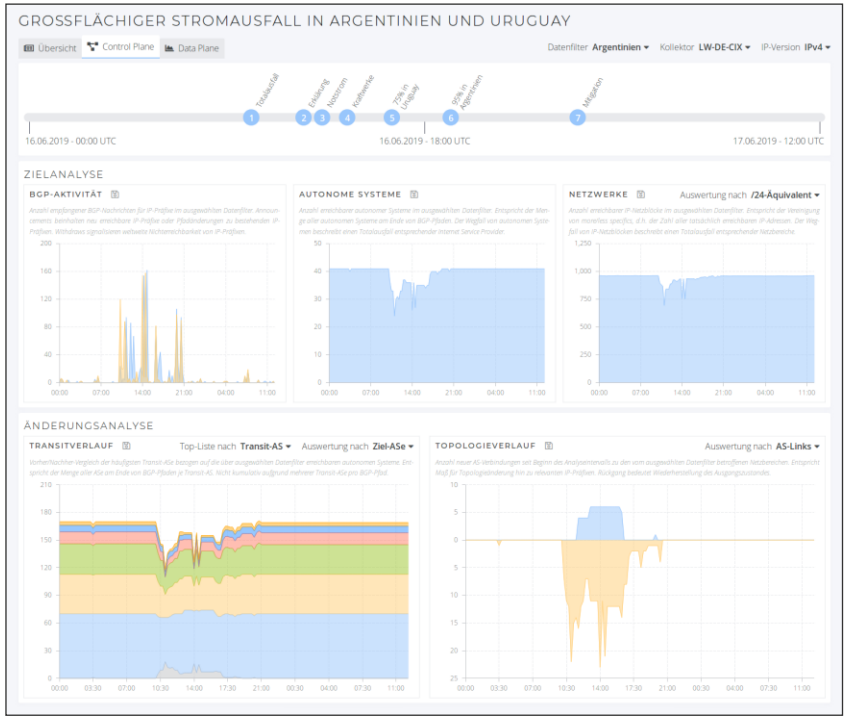
ÜBERSICHT

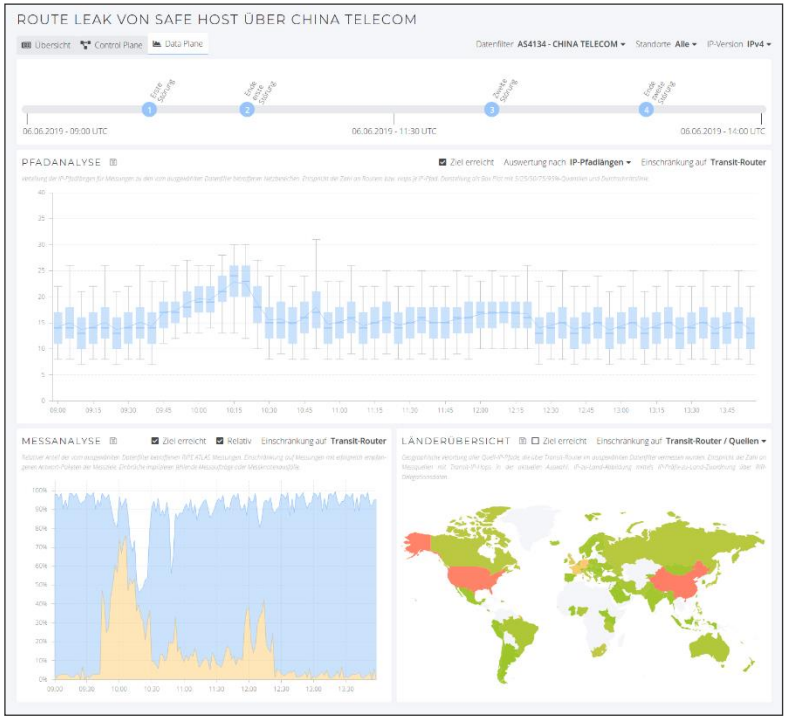
☐ Mit Detailanalyse Kategorien **1 von 10** Richtung **Aufsteigend** Sortieren nach **Datum** Bewerten nach **Reihenfolge**

Datum	Kategorie	Dienst	Betroffener	Vorfall	Dauer	Reichweite	Auswirkung	Komplexität	Post-Mortem	Datenlage
21.03.2013	BGP-Hijacking	Enterprise	Spamhaus	Übernahme des DNSBL-Dienstes führt zu weitreichender Spam-Markierung von Emails	3	2	3	3	2	3
16.08.2013	BGP-Hijacking	Cloud	Santrex	Hacking Team unterstützt italienischen Geheimdienst bei Angriff auf eigenen Server	3	1	1	1	2	3
03.02.2014	BGP-Hijacking	Cloud	Amazon	Kanadischer ISP fängt mehrfach Bitcoin Mining-Verkehr im Wert von $83,000 ab	3	2	2	3	1	3
26.04.2017	BGP-Hijacking	Enterprise	Finanzsektor	Rostelecom übernimmt 50 Präfixe populärer Bezahldienstleister für wenige Minuten	1	3	2	1	1	3
12.12.2017	BGP-Hijacking	Content	OTTs	Russisches Schläfer-AS übernimmt 80 Präfixe populärer Dienste für wenige Minuten	1	3	2	1	1	3
24.04.2018	BGP-Hijacking	DNS	Amazon	US-ansässiger ISP übernimmt DNS-Dienst und leitet Bitcoin-Wallets nach Russland um	2	2	3	3	1	3
30.07.2018	BGP-Hijacking	Content	Telegram	Iran Telecommunication übernimmt spezifischere Präfixe des Messenger-Dienstes	1	2	3	1	1	3
08.05.2019	BGP-Hijacking	DNS	TWNIC	ISP in Brasilien übernimmt kurzzeitig Privacy-fokussierten DNS-Dienst Quad-101	1	2	2	2	1	3

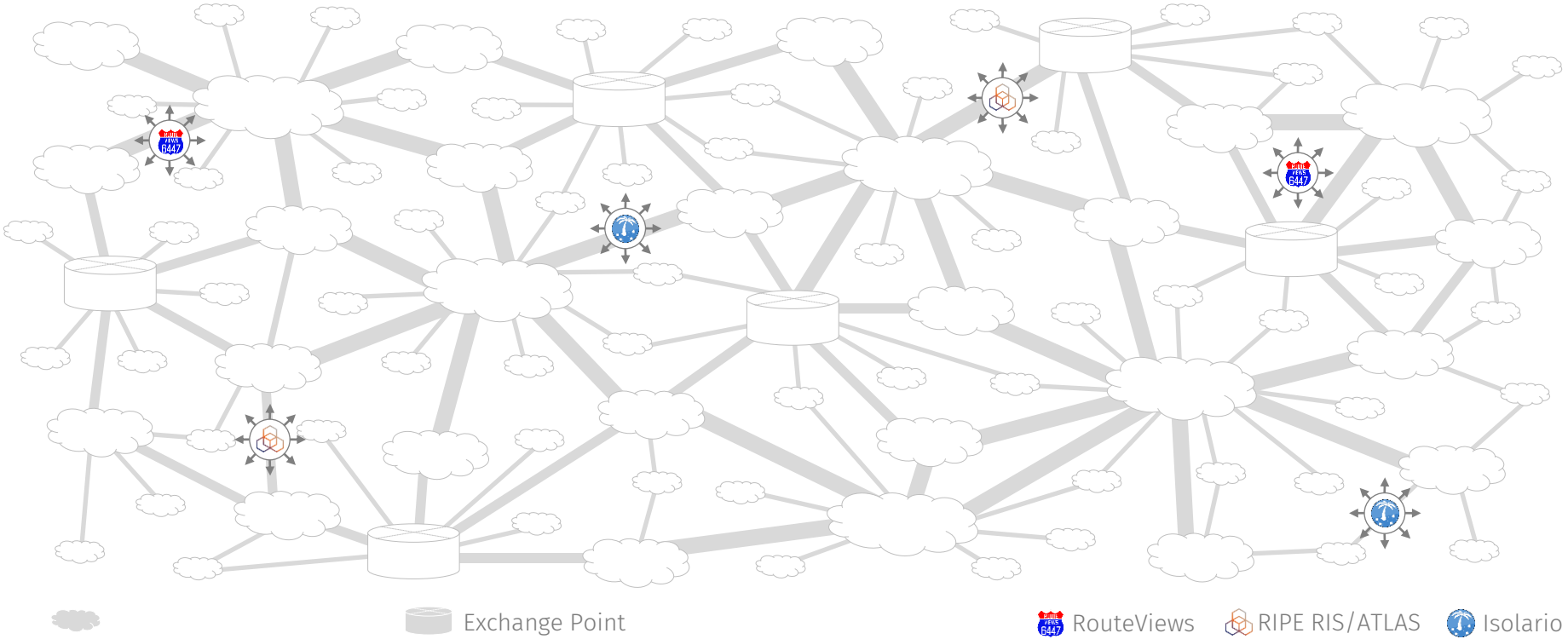
« ‹ 1 › »

Detailed analysis of 5 selected incidents

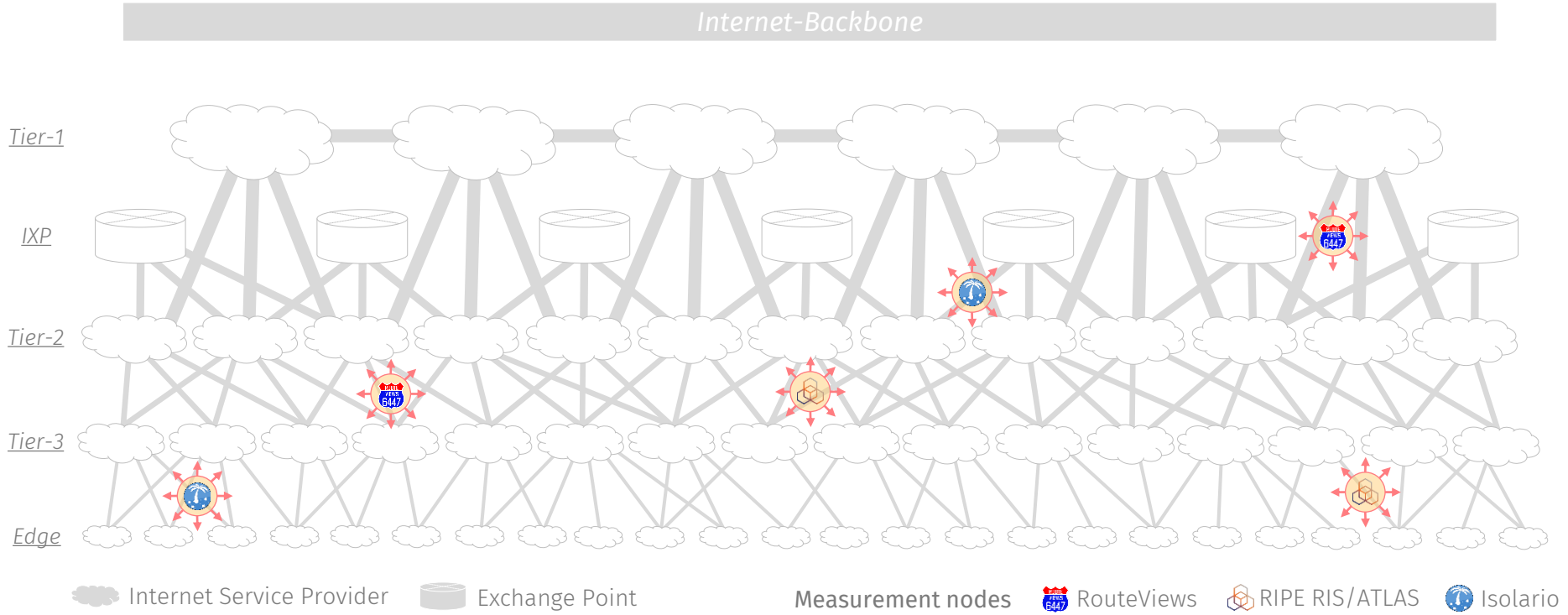




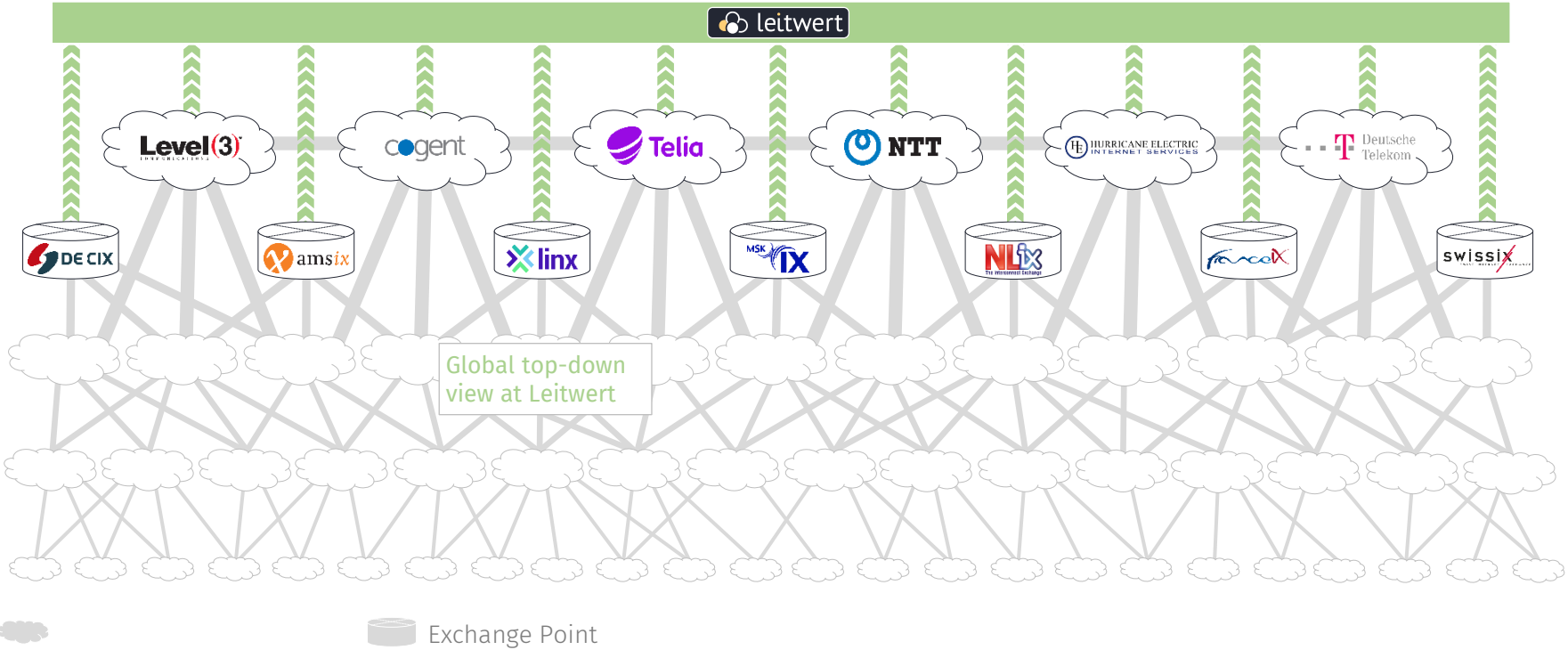
Excursus: Internet measurements (1/3)



Excursus: Internet measurements (2/3)



Excursus: Internet measurements (3/3)



Overview – Chapter 3

Chapter 1 **Introduction and Motivation**	Chapter 2 **Real Internet Outages**	Chapter 3 **Virtual Internet Outages**	Chapter 4 **International Cable Connections**
Chapter 5 **Changes of the Internet Infrastructure**	Chapter 6 **Social and Economical Implications**	Chapter 7 **Outlook & Anticipated Developments**	Chapter 8 **Conclusion**

Fictitious incidents

Outage of international cable connections

- Virtual incident: TAT-14 outage

Blackout of transit connections via a country

- Virtual incident: Russia black

DDoS attack on a central Internet service

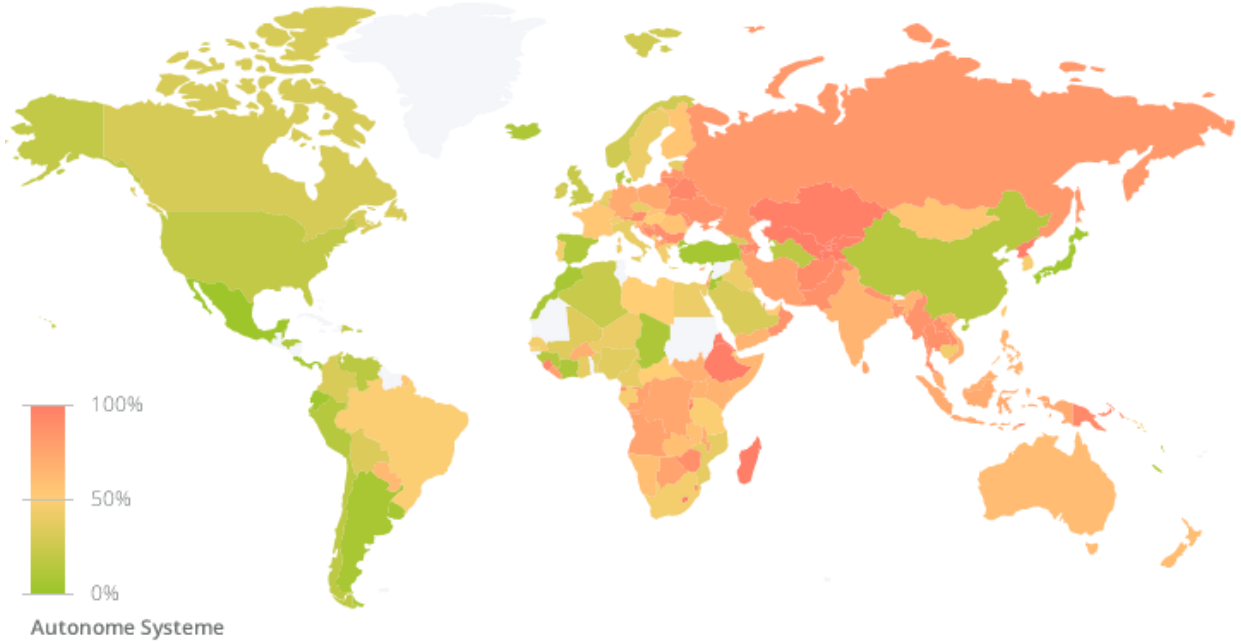
- Virtual incident: IONOS DNS attack

Outage of a popular Internet Exchange point

- Virtual incident: DE-CIX outage

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	+

DE-CIX outage (fictitious)



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 | Anwender | 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

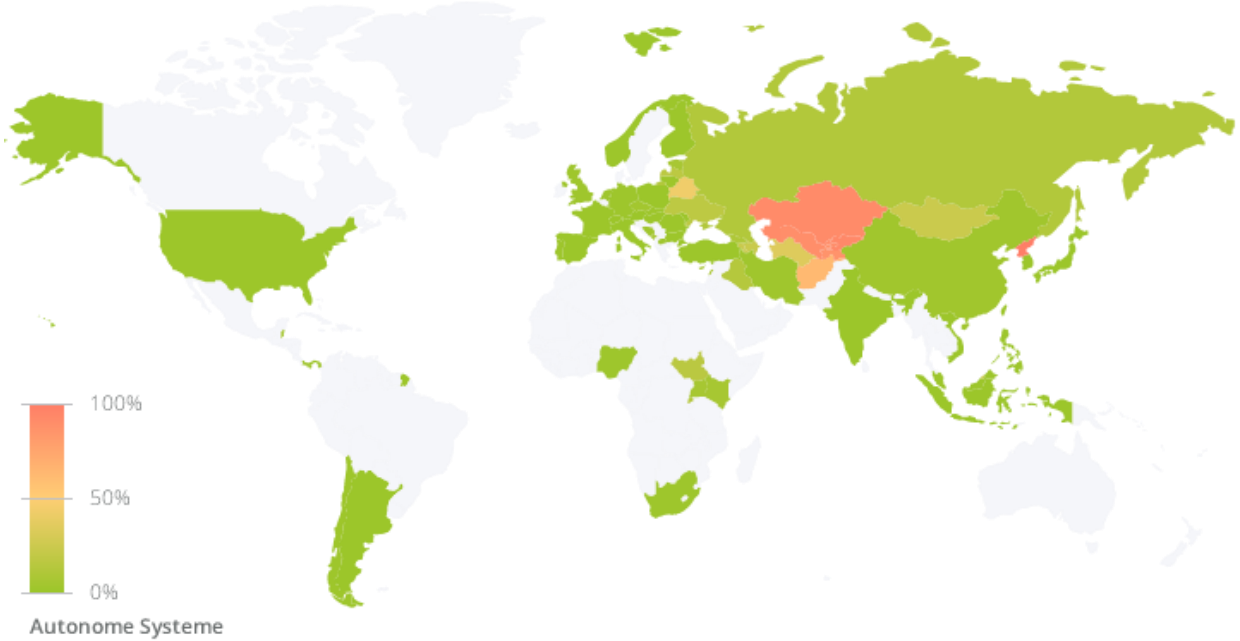
Durch Betroffene mitigierbar: ja | nein

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

Russia transit outage (fictitious)



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
Naturkatastrophe			
Menschlicher Fehler	1	●	h
Peering-Dispute			
Route Leak	0	●	d
Software-Fehler	1	●	h
Staatliche Aktion	1	●	∞
Technischer Defekt	1	●	h

Overview – Chapter 5

Chapter 1 **Introduction and Motivation**	Chapter 2 **Real Internet Outages**	Chapter 3 **Virtual Internet Outages**	Chapter 4 **International Cable Connections**
Chapter 5 **Changes of the Internet Infrastructure**	Chapter 6 **Social and Economical Implications**	Chapter 7 **Outlook & Anticipated Developments**	Chapter 8 **Conclusion**

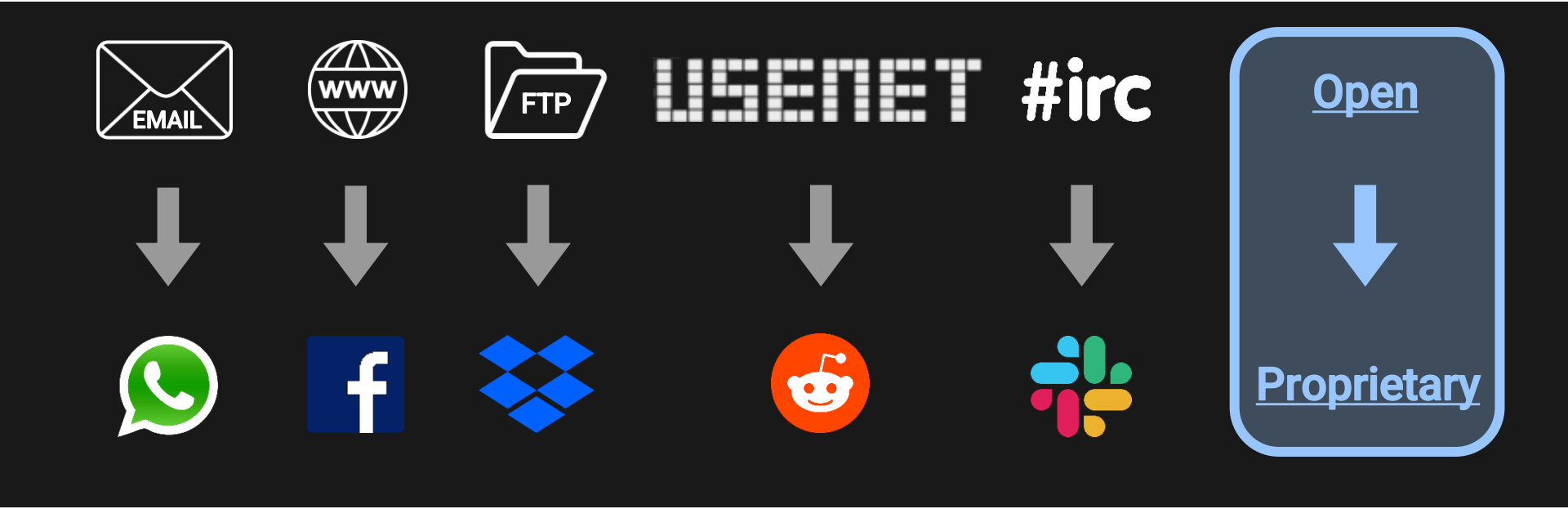
Two fundamental changes, unfortunately

Chapter 5
Changes of the Internet Infrastructure

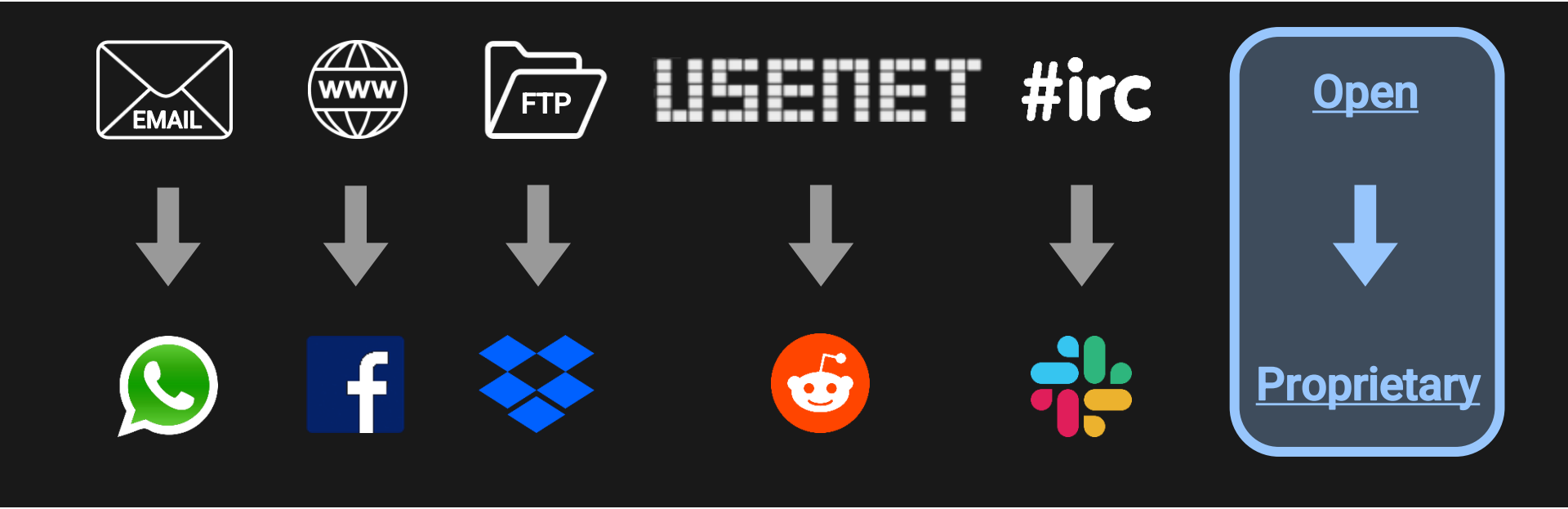
Consolidation

Splinternet

We see consolidation everywhere

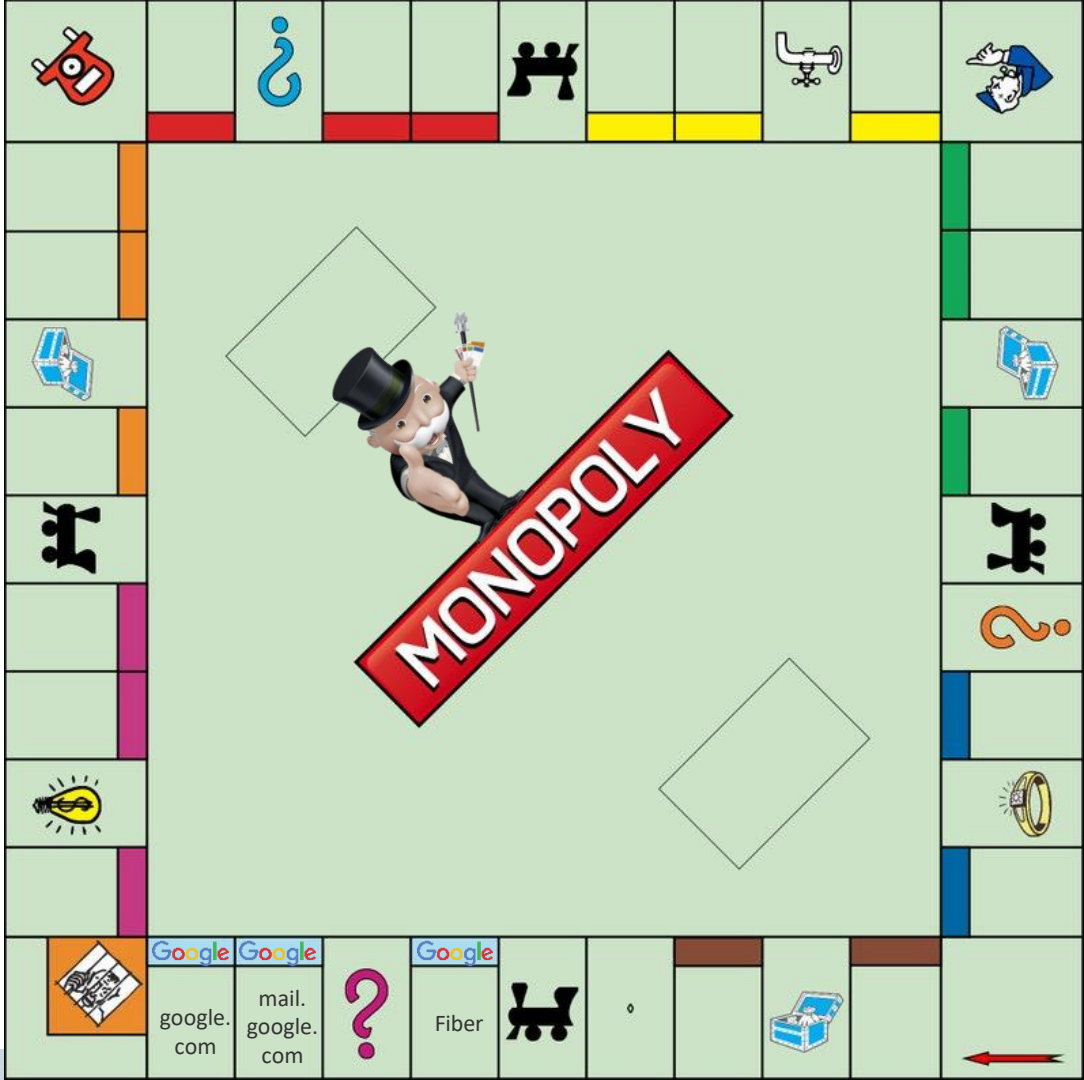


We see consolidation everywhere across layers

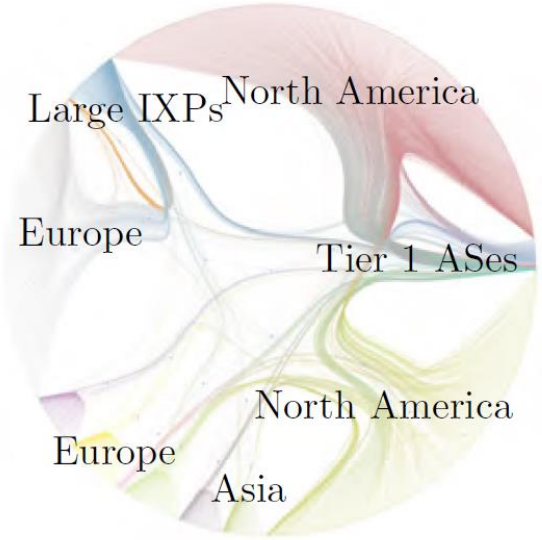


Who owns transatlantic fiber cables?

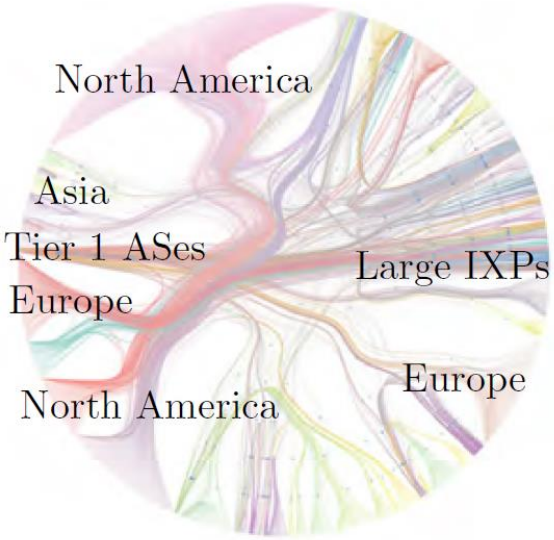
Consolidation is a friendly word for monopolization.



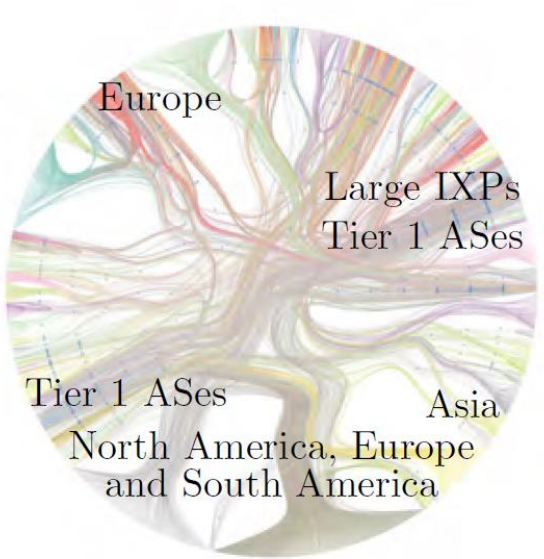
Internet routing relations over the last two decades



(a) 2000

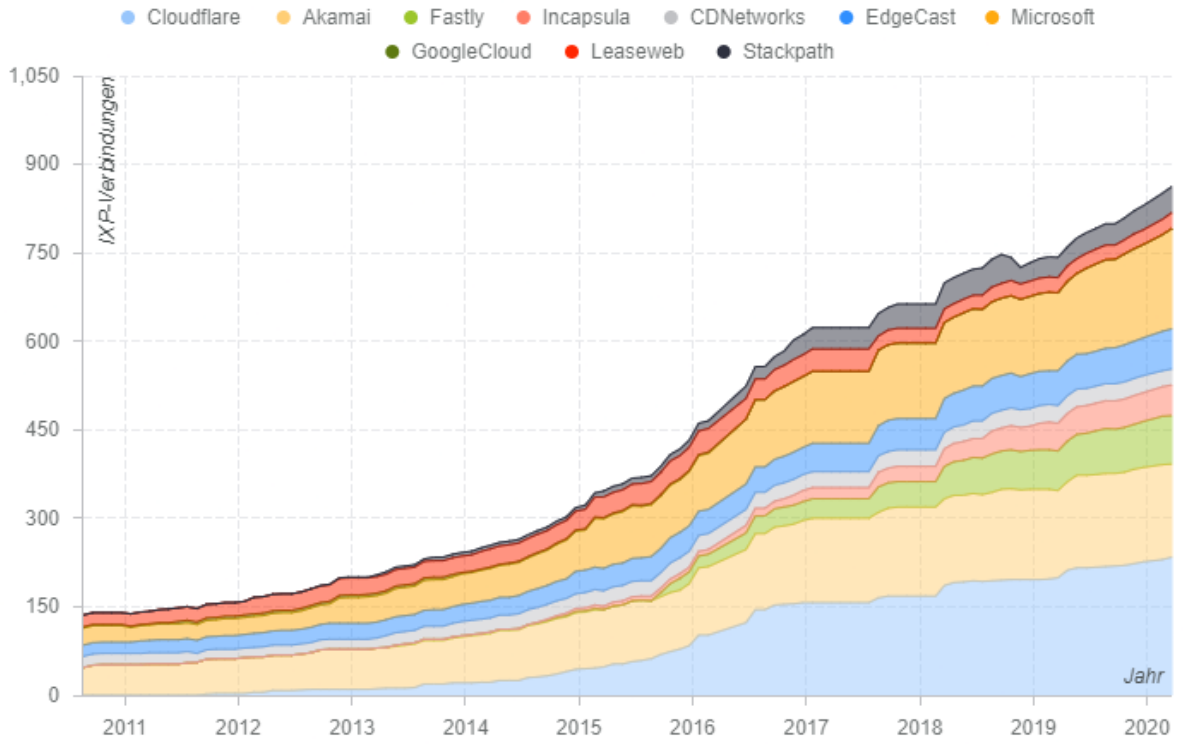


(b) 2010

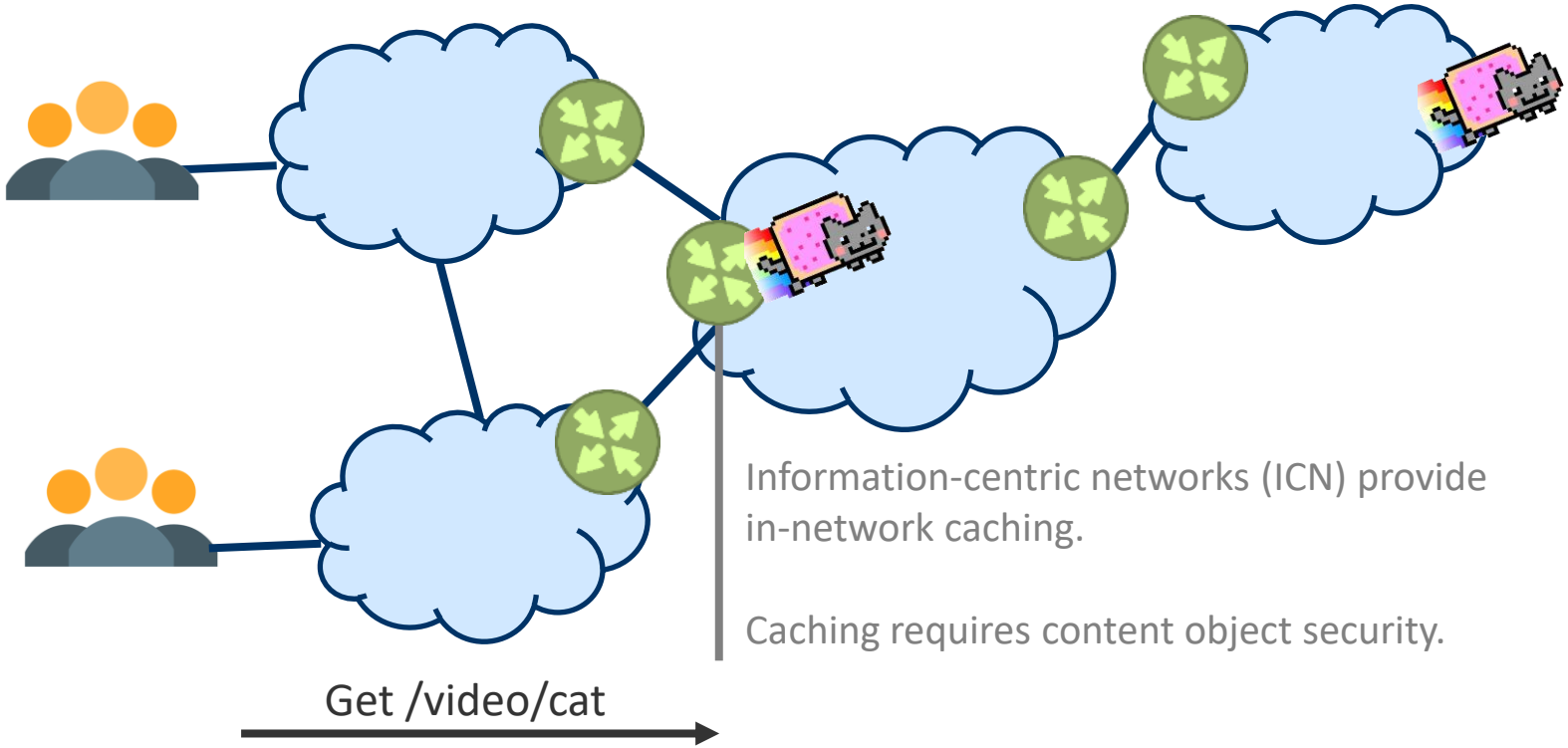


(c) 2020

Development of IXP connections for large CDNs



Prevent monopolization of content delivery by new network architectures, e.g., ICN + edge data centers



Information-centric networks (ICN) provide in-network caching.

Caching requires content object security.

Two OTT case studies: Disney+ and Netflix

NETFLIX

Originally using Akamai and Limelight
Since 2012 operating own CDN
Uses AWS to store and code movies

Started in USA in November 2019
Distributes Disney movies exclusively
No own CDN but Akamai, Lumen, Limelight, Edgecast, CloudFront, and Fastly
Did not change the global data volume or peering

Two OTT case studies: Disney+ and Netflix

An example where de-consolidation is not beneficial – fragmentation for end users increases.

Many states introduce Internet regulations to improve cyber sovereignty – for the good but also for the bad.

The **Splinternet**.

> The Internet is not open anymore.
> Free flow of information is restricted or suppressed.
> Even if you receive information under well-known names, you cannot rely on them.

We should raise awareness and be vocal.

The **Splinternet**.

> The Internet is not open anymore.
> Free flow of information is restricted or suppressed.
> Even if you receive information under well-known names, you cannot rely on them.

Overview – Chapter 5

Chapter 1 **Introduction and Motivation**	Chapter 2 **Real Internet Outages**	Chapter 3 **Virtual Internet Outages**	Chapter 4 **International Cable Connections**
Chapter 5 **Changes of the Internet Infrastructure**	Chapter 6 **Social and Economical Implications**	Chapter 7 **Outlook & Anticipated Developments**	Chapter 8 **Conclusion**

Lessons from the past. Network access.

Provisioning of network access infrastructure is a challenging business outside metropolitan areas

Traditionally, public telephone monopolies were split up in the western countries

Network infrastructure w/ last mile coverage remains monolithic

How to organize a provider market that

- continuously invests into state-of-the-art access technologies?
- maintains and develops network coverage also in rural areas?
- allows for plurality in the last mile without replicating infrastructure?

The US case

The US telephone monopolist AT&T was split up in 1984

- Seven independent regional Bell Operating Companies (Baby Bells)
- AT&T remained as long distance telephone company

Geographic split without competition at consumers

Since then

- Southwestern Bell bought three other Baby Bells and later AT&T
- Atlantic Bell bought the remainders and formed Verizon

Two large companies monopolize area-wise most of the US

Today, 50M households (40 %) only have a single provider choice

The German case

Deutsche Telekom (DTAG) lost the network monopoly in 1996

Per law, the access to cable infrastructure was regulated

- DTAG kept its cables but had to open access at regulated prices
- DTAG had to sell the TV cable network (CATV)

Horizontal split across all last miles, competition at consumers

Since then

- Pluralistic network access at nation-wide prices
- TV cable network partly monopolized with Vodafone

Diverse ecosystem of (partly regional) providers, relevant newcomers

Conclusion and a (positive) outlook

If we continue with the changes of the last ten years, the Internet will be doomed*.

*There is some hope, though.

Your turn. Three questions, your opinion. Thanks!

https://tudvote.tu-dresden.de/42071

Measurement data and interactive incident catalog

https://zwiback.leitwert.net